aws

用户指南

AWS 资源探索器

AWS 资源探索器: 用户指南

Table of Contents

什么是 AWS 资源探索器？

AWS 资源探索器 是一项资源搜索和发现服务。借助资源管理器，您可以使用类似互联网搜索引擎的体验来浏览您的资源，例如 Amazon Elastic Compute Cloud 实例、Amazon Kinesis 流或 Amazon DynamoDB 表。您可以使用资源元数据（如名称、标签和 ID）来搜索资源。资源管理器可在您的账户中跨 AWS 区域 运行，以简化您的跨区域工作负载。

资源管理器使用由 AWS 资源探索器 服务创建和维护的索引来快速响应您的搜索查询。资源管理器使用各种数据来源来收集有关您的 AWS 账户 中的资源的信息。资源管理器将这些信息存储在索引中，供资源管理器搜索。

> **我们想听听您对本文档的反馈**
>
> 我们的目标是帮助您从资源管理器中获得所有可能的资源。如果本指南可以帮助您做到这一点，请告诉我们。如果本指南对您没有帮助，则我们希望收到您的反馈，以便我们解决问题。请使用每页右上角的反馈链接。这会将您的评论直接发送给本指南的作者。我们会查看每份提交的内容，寻找改进文档的机会。提前感谢您的帮助！

主题

您是第一次使用资源管理器吗？

如果您是首次使用资源管理器的用户，建议您先阅读入门部分中的以下主题：

- 资源管理器的术语和概念
- 使用快速设置功能设置资源管理器

资源管理器的功能

资源管理器提供以下功能：

- 用户可以在自己的 AWS 区域 中或在其 AWS 账户 中跨区域搜索资源。
- 用户可以使用关键字、搜索运算符和标签等属性筛选搜索结果以仅匹配的资源。
- 当用户在搜索结果中找到资源时，他们可以立即前往该资源的本机控制台使用该资源。
- 管理员可以创建视图来定义搜索结果中哪些资源可用。管理员可以根据其任务为不同的用户组创建不同的视图，并仅向需要视图的用户授予视图权限。
- 与许多其他 AWS 服务 一样，资源管理器一样最终是一致的。资源管理器通过复制 Amazon 在全球的数据中心内多个服务器上的数据实现高可用性。如果成功请求更改某些数据，则更改会提交并安全存储。不过，更改必须跨资源管理器复制，这需要时间。举例来说，这包括资源管理器在一个区域中查找资源，然后将其复制到包含该账户聚合器索引的区域。

相关 AWS 服务

以下是其他以帮助您管理 AWS 资源为主要目的的 AWS 服务：

AWS Resource Access Manager (AWS RAM)

将一个 AWS 账户 中的资源与其他 AWS 账户 共享。如果您的账户由 AWS Organizations 管理，则可以使用 AWS RAM 与组织单位中的账户或组织中的所有账户共享资源。共享资源适用于这些账户中的用户，就像在本地账户中创建它们一样。

AWS Resource Groups

为您的 AWS 资源创建组。然后，您可以将每个组作为一个单元来使用和管理，而不必单独引用每个资源。您的组可以由属于同一 AWS CloudFormation 堆栈的资源或使用相同标签标记的资源组成。某些资源类型还支持将配置应用于资源组以影响该组中的所有相关资源。

标签编辑器和 AWS Resource Groups Tagging API

标签是客户定义的元数据，您可以将其附加到您的资源。您可以出于成本分配和基于属性的访问控制等目的对资源进行分类。

访问资源管理器

您可以通过以下方式与资源管理器交互：

资源管理器控制台

资源管理器提供基于 Web 的用户界面，即资源管理器控制台。如果您已注册 AWS 账户，则可通过登录 AWS Management Console 并从控制台主页中选择资源管理器来访问资源管理器控制台。

您也可以在浏览器中直接导航到资源管理器控制对面板页面或资源搜索页面。如果您尚未登录，则系统会要求您在控制台出现之前登录。

> **Note**
>
> 资源管理器控制台是一个全局控制台，这意味着您不必选择 AWS 区域 即可使用。但是，使用资源管理器创建索引或视图时，您需要指定索引或视图存储在哪个区域。使用资源管理器进行搜索时，可以选择您有权访问的任何视图。结果自动来自与所选视图关联的区域。如果视图来自包含聚合器索引的区域，则结果将包括您创建资源管理器索引所在的所有区域的资源。

AWS Management Console 统一搜索

AWS Management Console 中每个页面的顶部都有一个搜索栏。您可以将资源管理器配置为参与统一搜索。然后，您的用户可以在统一搜索文本框中使用资源管理器安装搜索查询语法，并在这些搜索结果中查看匹配的资源。开启此功能后，用户可以从任何 AWS 服务 的控制台搜索资源，而无需先切换到资源管理器控制台。

> **Important**
>
> 统一搜索始终使用包含聚合器索引的 AWS 区域 中的默认视图进行搜索。

中的资源管理器命令AWS CLI和适用于 Windows 的工具 PowerShell

AWS CLI和工具 PowerShell 提供对资源管理器公共 API 操作的直接访问权限。这些工具可在 Windows、macOS 和 Linux 上运行。有关入门的更多信息，请参阅《AWS Command Line Interface 用户指南》https://docs.aws.amazon.com/cli/latest/userguide/或《AWS Tools for Windows PowerShell 用户指南》https://docs.aws.amazon.com/powershell/latest/userguide/。有关资源管理器命令的更多信息，请参阅《AWS CLI 命令参考》https://docs.aws.amazon.com/cli/latest/reference/resource-explorer-2或《AWS Tools for Windows PowerShell Cmdlet 参考》https://docs.aws.amazon.com/powershell/latest/reference/index.html?page=ResourceExplorer2_cmdlets.html。

AWS SDK 中的资源管理器操作

AWS 为大量编程语言提供 API 命令。有关入门的更多信息，请参阅AWS 资源探索器 与 AWS SDK 一起使用。

查询 API

如果您不使用支持的编程语言之一，则资源管理器 HTTPS 查询 API 可让您以编程方式访问资源管理器。使用资源管理器 API，您可以直接向服务发布 HTTPS 请求。当您使用资源管理器 API 时，必须添加代码，才能使用您的 AWS 凭证对请求进行数字化签名。有关更多信息，请参阅 AWS 资源探索器 API 参考。

定价

使用 AWS 资源探索器 搜索资源（包括创建视图、开启区域或搜索资源）不收取任何费用。在创建资源清单的过程中，资源管理器会代表您调用 API，这可能会产生费用。与您在搜索结果中找到的资源进行交互可能会产生不同的使用费，具体取决于资源类型及其类型AWS 服务。有关 AWS 如何为特定资源类型的正常使用计费的更多信息，请参阅该资源类型所属服务的文档。

资源管理器入门

使用本部分中的主题对 AWS 资源探索器 使用的概念和术语进行基本的了解。了解成功使用资源管理器必须满足的先决条件，以及如何在 AWS 账户 中开启资源管理器。

主题

- 资源管理器的术语和概念
- 使用资源管理器的先决条件
- 设置和配置资源管理器

资源管理器的术语和概念

AWS 资源探索器 是一项资源搜索和发现服务。借助资源管理器，您可以通过使用类似互联网搜索引擎的体验来探索您的资源。您可以使用类似名称、标签和 ID 的资源元数据来搜索您的资源，例如 Amazon Elastic Compute Cloud 表、Amazon Kinesis 流或 Amazon DynamoDB 表。资源管理器可在您的账户中跨 AWS 区域 运行，以简化您的跨区域工作负载。

资源管理器使用由 AWS 资源探索器 服务创建和维护的索引来快速响应您的搜索查询。资源管理器使用各种数据来源来收集有关您的 AWS 账户 中的资源的信息。资源管理器将这些信息存储在索引中，供资源管理器搜索。

要想为用户成功管理和配置 AWS 资源探索器，您应该了解以下概念。

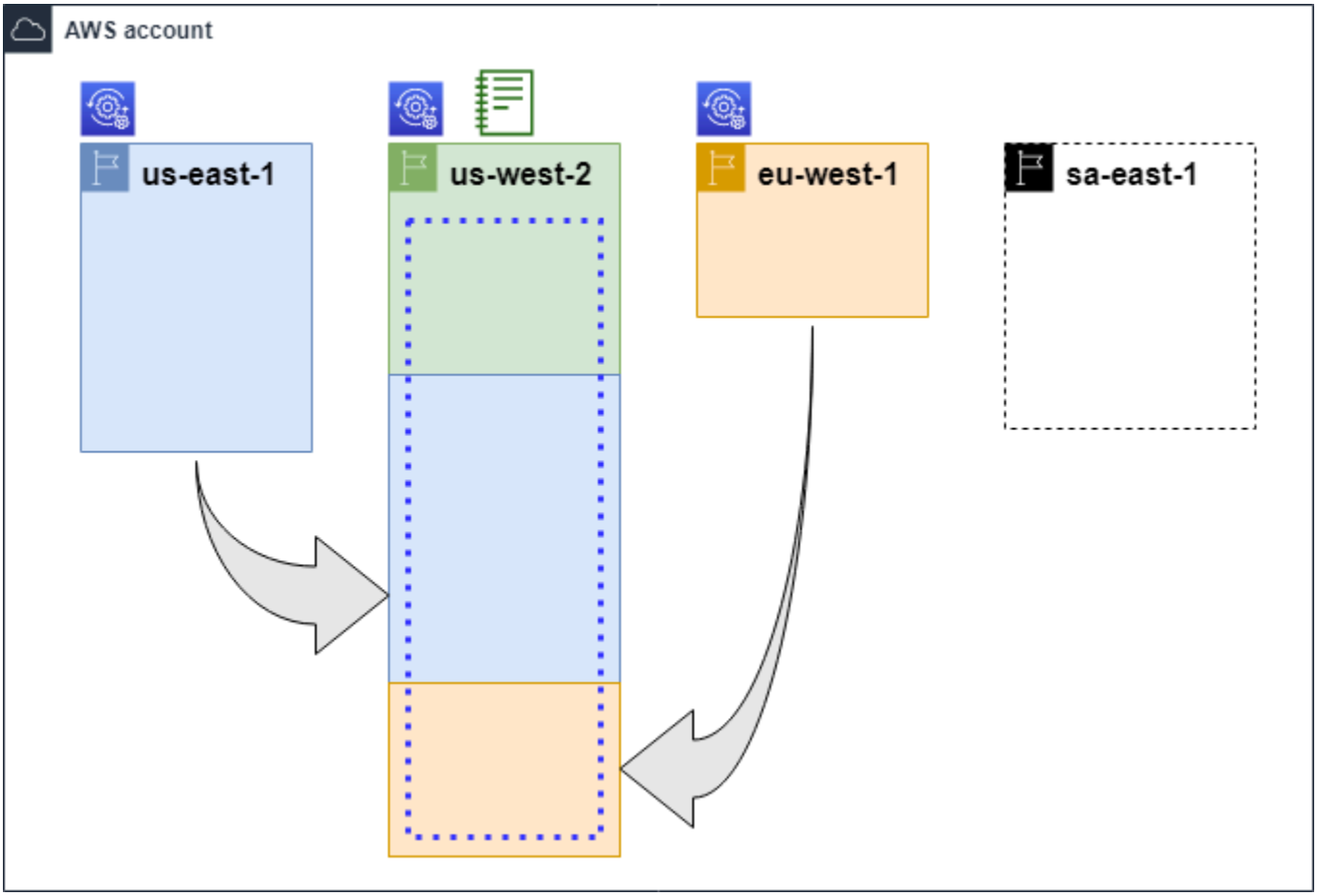
概念

- 资源管理器管理员
- 资源管理器用户
- 索引
- 查看
- 资源
- AWS Management Console 中的统一搜索
- 多账户搜索

下图显示了管理员在其中开启资源管理器的三个 AWS 区域，以及管理员选择不开启的一个区域。未开启资源管理器的区域没有索引。因此，资源管理器查询无法搜索其资源。

在此示例场景中，管理员选择了美国西部（俄勒冈州）区域（us-west-2）来包含该账户的聚合器索引。您开启的所有区域都将其本地索引复制到包含聚合器索引的区域。

资源管理器创建的默认视图没有任何筛选条件。因此，使用此视图进行搜索的结果可以包括开启资源管理器的账户中所有区域中的任何类型的资源。



图例	
	此 AWS 区域 中已开启资源管理器，有关该区域资源的信息存储在该区域的本地索引中。每个区域的本地索引（由箭头指示）也被复制到包含聚合器索引的区域中。
	AWS 区域 中的索引被配置为账户的聚合器索引。资源管理器将在已开启资源管理器的所有其他区域中的本地索引中收集的信息复制到该区域中的聚合器索引。在该区域进行的搜索可以包括账户中所有区域的结果。
	快速设置功能创建的默认视图包含所有 AWS 区域 中的所有资源。

资源管理器管理员

资源管理器管理员是一个 AWS Identity and Access Management（IAM）主体，该主体有权管理资源管理器及其在 AWS 账户 或。资源管理器管理员可以配置以下功能：

- 通过在这些区域中创建索引，为 AWS 账户 中的各个 AWS 区域 开启资源管理器。这样，资源管理器就可以发现资源并在索引中填充有关这些资源的信息，以便用户可以在该区域中搜索资源。
- 更新一个 AWS 区域 中的索引类型，使其成为其 AWS 账户 的聚合器索引。该区域中的聚合器索引会接收资源信息的复制副本，资料信息来自已开启资源管理器的账户中所有其他区域。
- 创建视图，定义用户可以在资源管理器中搜索和发现的索引信息子集。
- 虽然不是资源管理器操作的一部分，但资源管理器管理员还必须能够向账户中的主体授予搜索权限。管理员可以通过向现有 IAM 权限策略添加相关权限，或使用资源管理器只读 AWS 托管策略，向主体授予这些权限。

  要提供访问权限，请为您的用户、群组或角色添加权限：

  - AWS IAM Identity Center 中的用户和群组：

    创建权限集。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。
  - 通过身份提供商在 IAM 中托管的用户：

    创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
  - IAM 用户：
    - 创建您的用户可以代入的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
    - （不推荐使用）将策略直接附加到用户或将用户添加到用户群组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

管理员通常拥有所有资源管理器资源（包括索引和视图）的所有资源管理器权限（`resource-explorer-2:*`）。可以使用资源管理器完全访问 AWS 托管策略来授予这些权限。

资源管理器用户

资源管理器用户是有权执行以下一项或多项任务的 IAM 主体：

- 通过使用视图查询资源管理器来搜索资源。资源管理器用户想要发现和查找 AWS 资源，通常使用资源管理器控制台或 AWS SDK 或 AWS CLI 提供的资源管理器 `Search` 操作。

角色或用户可以使用 IAM 获取通过以下两种方法之一进行搜索的权限：

- 资源管理器对 IAM 角色、组或用户的只读 AWS 托管策略。
- 一个 IAM 权限策略，其语句包含对 IAM 角色、组或用户的以下最低权限。

```
{
    "Effect": "Allow",
    "Action": [
        "resource-explorer-2:Search",
        "resource-explorer-2:GetView",
    "Resource": "<ARN of the view>"
}
```

- 您可以将定义创建视图的权限委托给受信任的用户，尽管这通常被视为管理员任务。为此，管理员可以在附加到相关角色、组或用户的 IAM 权限策略中授予调用 `resource-explorer-2:CreateView` 操作的权限。如果视图需要特定权限，则必须为相关用户提供添加或修改 IAM policy 的配置。

有关如何使用资源管理器搜索资源的信息，请参阅 使用 AWS 资源探索器 搜索资源。

索引

索引是有关 AWS 账户 中的一个 AWS 区域 中所有 AWS 资源的信息集合，由资源管理器维护。资源管理器在您开启资源管理器的每个区域中维护一个索引。当您在 AWS 账户 中创建和删除资源时，资源管理器会自动更新索引。在前面的图表中，AWS 区域 名称下方的方框表示每个 AWS 区域 中维护的资源管理器索引。某个区域中的索引是在该区域中创建的任何视图的信息来源。用户不能直接查询索引。反之，他们必须始终使用视图进行查询。

有两种类型的索引：

本地索引

开启资源管理器的每个 AWS 区域 中都有一个本地索引。本地索引仅包含有关同一区域中的资源的信息。

聚合器索引

资源管理器管理员还可以将一个 AWS 区域 中的索引指定为 AWS 账户 的聚合器索引。聚合器索引接收并存储账户中所有其他开启资源管理器的区域的索引副本。聚合器索引还接收和存储有关其自己区域中的资源的信息。在前面的图表中，区域 `us-west-2` 包含账户的聚合器索引。为账户指定

聚合器索引的主要原因是，您可以创建包含账户中所有区域的资源的视图。一个 AWS 账户 中只能有一个聚合器索引。

开启资源管理器后，您可以指定哪个 AWS 区域 将包含聚合器索引。您也可以稍后更改聚合器索引所用的 AWS 区域。有关如何提升本地索引以使其成为其 AWS 账户 的聚合器索引的信息，请参阅通过创建聚合器索引开启跨区域搜索。

索引是具有 Amazon 资源名称（ARN）的资源。但是，您只能在权限策略中使用此 ARN 来授予对直接与索引交互的操作的访问权限。通过这些操作，您可以创建视图并将其设置为区域中的默认视图，在区域中开启或关闭资源管理器，并为该账户创建聚合器索引。索引的 ARN 与以下示例类似：

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd11111111
```

查看

视图是用于查询索引中列出的资源的机制。该视图用于定义索引中哪些信息可见，哪些信息可用于搜索和发现。用户从不直接查询资源管理器索引。相反，查询必须始终通过视图进行，该视图允许视图创建者限制用户可以在搜索结果中看到哪些资源。

创建视图时，您可以指定筛选条件来限制搜索结果中包含哪些资源。例如，您可以选择仅包含少数指定资源类型的资源，这些资源由您向其授予该视图访问权限的用户使用。始终会自动筛选用户使用视图进行查询的结果，以仅包括与视图标准相匹配的资源。

要授予使用视图的访问权限，您可以使用以下方法之一分配权限。

要提供访问权限，请为您的用户、群组或角色添加权限：

- AWS IAM Identity Center 中的用户和群组：

  创建权限集。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。
- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以代入的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户群组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

授予权限，以允许您的角色、组或用户对由 Amazon 资源名称（ARN）标识的视图调用 `resource-explorer-2:GetView` 和 `resource-explorer-2:Search` 操作。或者，您可以对所有需要使用该视图进行搜索的主体使用资源管理器只读 AWS 托管策略。您可以创建具有不同筛选条件和范围的多个视图，从而返回资源信息的不同子集。然后，您可以向用户授予对每个视图的权限，这些用户需要查看该视图的结果中包含的信息。

要使用资源管理器进行搜索，每个用户都必须拥有至少使用一个视图的权限。如果不使用视图，您就无法在资源管理器中执行搜索。

视图基于每个区域进行存储。视图只能访问该 AWS 区域 中的资源管理器索引。要访问账户范围内的搜索结果，您必须使用包含该账户的聚合器索引的区域中的视图。快速设置功能选项在 AWS 区域 中创建默认视图，其中包含聚合器索引和和包含账户在所有 AWS 区域 中使用的所有资源的筛选条件。

有关如何创建视图的信息，请参阅 管理资源管理器视图以提供搜索访问权限。有关如何在查询中使用视图的信息，请参阅 使用 AWS 资源探索器 搜索资源。

每个视图都有一个 Amazon 资源名称（ARN），您可以在权限策略中引用该名称来授予对单个视图的访问权限。您还可以将某个视图的 ARN 作为参数传递给与视图交互的任何 API 或 AWS CLI 操作。视图的 ARN 与以下示例类似。

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View-
Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> 每个视图 ARN 的末尾都包含一个由 AWS 生成的 UUID。这有助于确保用户无法自动访问使用相同名称创建的新视图，而这些用户可能有权使用已删除的特定名称对视图进行访问。

资源

资源是您可以使用的 AWS 中的实体。资源由 AWS 服务 在您使用服务的功能时创建。示例包括 Amazon EC2 实例、Amazon S3 存储桶或 AWS CloudFormation 堆栈。某些资源类型可能包含客户数据。所有资源类型都有描述资源的属性或元数据，包括名称、描述和您用来唯一引用资源的 Amazon 资源名称（ARN）。大多数资源类型还支持标签。标签是您可以出于各种目的附加到资源的自定义元数据，例如账单中的成本分配、使用基于属性的访问控制进行安全授权，或者支持您的其他分类需求。

资源管理器的主要目的是帮助您找到您的 AWS 账户 中存在的资源。资源管理器使用各种技术来发现您的所有资源，并将有关这些资源的信息放在索引中。然后，您可以通过管理员为您提供的任何视图来查询索引。

> **Important**
>
> 资源管理器故意排除那些包含会暴露客户数据的资源类型。以下资源类型不会被资源管理器编入索引，因此搜索结果中不会返回这些资源类型。
>
> - 存储桶内包含的 Amazon S3 对象
> - Amazon DynamoDB 表项目
> - DynamoDB 属性值

AWS Management Console 中的统一搜索

在每个 AWS 服务 中的 AWS Management Console 顶部都有一个搜索栏，您可以用它来搜索与 AWS 相关的各种内容。您可以搜索服务和功能，并在该服务的控制台中获得直接到相关页面的链接。您还可以搜索与您的搜索词相关的文档和博客文章。

开启资源管理器并创建聚合器索引和默认视图后，统一搜索还可以在搜索结果中包含您账户的资源。统一搜索会自动使用包含账户聚合器索引的 AWS 区域 中的默认视图。这使您可以从 AWS Management Console 中的任何页面搜索资源，而不必先打开资源管理器。如果您没有将本地索引提升为账户的聚合器索引，或者您没有在聚合器索引区域中创建默认视图，则统一搜索的搜索结果中不会包含资源。此外，任何执行搜索的主体必须有权使用包含聚合器索引的区域中的默认视图，否则统一搜索的搜索结果中不包含资源。

> **Important**
>
> 统一搜索会自动在字符串中第一个关键字的末尾插入通配符（*）运算符。这意味着统一的搜索结果包括与任何以指定关键字开头的字符串相匹配的资源。
> 通过查询文本框，在资源管理器控制台的资源搜索页面上执行的搜索，不会自动附加通配符。您可以在搜索字符串中的任何术语后面手动插入 *。

有关统一搜索及其与资源管理器集成的更多信息，请参阅 在 AWS Management Console 中使用统一搜索。

多账户搜索

通过多账户搜索，您可以通过单个关键字搜索跨 AWS Organizations 和 AWS 区域 搜索和发现资源。

有关多账户搜索以及如何为资源管理器启用多账户搜索的更多信息，请参阅 开启多账户搜索。

使用资源管理器的先决条件

在 AWS 资源探索器 首次使用之前，请根据需要完成以下任务。

任务

- 注册获取 AWS 账户
- 创建具有管理访问权限的用户

注册获取 AWS 账户

如果您没有 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/signup。
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。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

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

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的以根用户身份登录。
2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center

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

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

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

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加组。

设置和配置资源管理器

在设置和配置之前 AWS 资源探索器，请先确保满足先决条件。之后，以 IAM 角色或拥有执行以下过程资源管理器操作所需权限的用户身份登录。

您可以使用此设置和配置过程在现有帐户以及添加到组织中的任何新帐户中设置资源浏览器。

有以下两种方法可设置资源管理器：

- 快速设置
- 高级设置

> **Important**
>
> 如果您选择使用任何显示 AWS 区域 “全部” 的选项来设置资源浏览器，则它只 AWS 区域 会激活在您执行该过程时存在且已启用的资源浏览器。 AWS 账户在任何将来 AWS 添加的资源管理器中 AWS 区域 ，资源浏览器都不会自动开启。 AWS 引入新区域时，您可以选择在资源管理器控制台的 “设置” 页面中显示该区域时手动打开该区域中的资源浏览器，也可以通过调用CreateIndex操作来选择将其打开。

> **Note**
>
> 设置资源管理器还可以启用资源搜索功能，通过使用 AWS Management Console 上的统一搜索栏进行搜索。要让用户在统一搜索结果中看到资源，您必须为资源管理器配置跨区域聚合器索引和默认视图。有关详细信息，请参阅以下过程。您还必须确保您的搜索用户有权使用包含聚合器索引 AWS 区域 的默认视图。有关更多信息，请参阅在 AWS Management Console 中使用统一搜索。

使用快速设置功能设置资源管理器

如果选择“快速设置功能”选项，则资源管理器将执行以下操作：

- 在你的每 AWS 区域 一个中创建一个索引 AWS 账户。
- 更新您指定为账户聚合器索引的区域中的索引。
- 在聚合器索引区域中创建一个默认视图。此视图没有筛选条件，因此它会返回在索引中找到的所有资源。

最小权限

要执行下列程序中的步骤，您必须具有以下权限：

- 操作：`resource-explorer-2:*` – 资源：无特定资源（*）
- 操作：`iam:CreateServiceLinkedRole` – 资源：无特定资源（*）

AWS Management Console

要使用快速设置功能来设置资源管理器

1. 在 https://console.aws.amazon.com/resource-explorer 处打开 AWS 资源探索器 控制台。
2. 选择开启资源管理器。
3. 在开启资源管理器页面上，选择快速设置功能。
4. 选择 AWS 区域 要包含聚合器索引的聚合器索引。您应该选择适合用户地理位置的区域。
5. 在页面底部，选择开启资源管理器。
6. 在进度页面上，您可以在资源管理器创建其索引时监控每个 AWS 区域 。该页面显示创建聚合器索引和创建默认视图的状态。

当所有步骤都显示已成功完成之后，您和您的用户就可以导航到资源搜索页面并开始搜索资源。

> **Note**
>
> 索引本地的已标记资源会在几分钟内出现在搜索结果中。未标记的资源通常需要不到两个小时的时间便可以显示，但在需求旺盛时可能需要更长的时间。完成从所有现有本地索引向新聚合器索引的初始复制过程，也可能需要长达一个小时。

后续步骤：在您的用户可以使用您刚刚创建的默认视图进行搜索之前，您必须向他们授予使用该视图进行搜索的权限。有关更多信息，请参阅授予对资源管理器视图的访问权限以进行搜索。

AWS CLI

顾名思义，使用等同于 “ AWS CLI 高级设置” 选项在中设置资源管理器。 AWS 账户 这是因为资源管理器 CLI 操作不会像资源管理器控制台那样自动为您执行任何步骤。请参阅上的 AWS CLI 选项卡使用高级设置功能设置资源管理器 ，了解哪些命令等同于使用控制台。

使用高级设置功能设置资源管理器

如果您选择“高级设置”选项，则可以执行以下操作：

- 选择要 AWS 区域 在其中打开 “资源浏览器” 的。
- 选择是否为一个区域配置聚合器索引。如果这样做，则可以指定 AWS 区域 将其放置在其中。此索引允许您创建可包含账户中所有区域资源的视图。有关更多信息，请参阅通过创建聚合器索引开启跨区域搜索。
- 选择是否创建默认视图。该视图允许在您打开 AWS 资源浏览器的区域中自动搜索任何资源。您必须确保，需要使用默认视图在资源管理器中进行搜索的任何主体，均拥有该视图的权限。有关更多信息，请参阅授予对资源管理器视图的访问权限以进行搜索。

> **Note**
>
> 您可以将资源管理器配置为将您的资源包含在 AWS Management Console 上的统一搜索功能提供的搜索结果中。要开启此功能，您必须为资源管理器配置聚合器索引和默认视图，所有角色和用户均可使用该索引和视图进行搜索。快速设置功能选项可创建聚合器索引和默认视图，建议您使用该选项打开资源管理器。

最小权限

要执行下列程序中的步骤，您必须具有以下权限：

- 操作：`resource-explorer-2:*` – 资源：无特定资源（ * ）
- 操作：`iam:CreateServiceLinkedRole` – 资源：无特定资源（ * ）

AWS Management Console

要使用高级设置功能设置资源管理器

1. 在 https://console.aws.amazon.com/resource-explorer 处打开 AWS 资源探索器 控制台。
2. 选择开启资源管理器。
3. 在开启资源管理器页面上，选择高级设置功能。
4. 在 “区域” 下的AWS 区域框中，选择是要在所有区域中打开资源浏览器 AWS 区域，还是仅在特定区域中打开资源浏览器。

如果您选择仅在此账户中指定的 AWS 区域 区域中开启资源管理器，则请选择要在搜索结果中包含其资源的每个区域。

5. 对于聚合器索引，选择是否要创建聚合器索引。如果您选择创建聚合器索引，则所有其他索引都会将其索引 AWS 区域 复制到该区域。这允许用户在中搜索所有选定区域的资源 AWS 账户。选择 AWS 区域 包含聚合器索引的。建议您指定用户花费大部分时间的区域，或者至少指定您期望他们进行大部分资源搜索的区域。
6. 在默认视图框的视图创建下，选择是否创建默认视图。仅当您选择创建聚合器索引时，此选项才可用。如果您选择创建默认视图，资源管理器会将此视图放置在与聚合器索引 AWS 区域 相同的位置中。这样，默认视图就可以包含您在其中注册资源管理器的所有 AWS 区域 结果。每当用户使用默认视图在区域中执行搜索但未明确指定视图时，搜索将使用该区域的默认视图。

> **Note**
>
> 您必须先向用户授予使用该视图的权限，然后他们才能使用该视图。有关更多信息，请参阅授予对资源管理器视图的访问权限以进行搜索。

7. 选择激活资源管理器。

> **Note**
>
> 索引本地的已标记资源会在几分钟内出现在搜索结果中。未标记的资源通常需要不到两个小时的时间便可以显示，但在需求旺盛时可能需要更长的时间。完成从所有现有本地索引向新聚合器索引的初始复制过程，也可能需要长达一个小时。

AWS CLI

要使用高级设置功能来设置资源管理器

资源管理器控制台根据您所做的选择代表您执行许多 API 操作调用。以下示例 AWS CLI 命令说明了如何使用在控制台之外执行相同的基本过程 AWS CLI。

Example 步骤 1：通过在所需的 AWS 区域 中创建索引来开启资源管理器

在要激活资源浏览器的每个命令 AWS 区域 中运行以下命令。以下示例命令在 AWS 区域 中开启资源管理器，这是 AWS CLI 的默认设置。

```
$ aws resource-explorer-2 create-index
```

```
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-27T16:17:12.130000+00:00",
    "State": "CREATING"
}
```

Example 第 2 步：将索引合 AWS 区域 并为账户的聚合索引

在中运行以下命令， AWS 区域 您希望资源管理器将本地索引更新为该帐户的聚合器索引。以下示例命令更新美国东部（弗吉尼亚州北部）（us-east-1）中的聚合器索引。

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt": "2022-07-27T16:29:49.231000+00:00",
    "State": "UPDATING",
    "Type": "AGGREGATOR"
}
```

Example 步骤 3：在中创建 AWS 区域 包含聚合器索引的视图

在创建聚合器索引的 AWS 区域 中运行以下命令。以下示例命令创建的视图，与资源管理器控制台设置过程创建的视图相同。这个新视图包括作为索引信息的一部分附加到资源的标签，并支持按标签键或值搜索资源。

```
$ aws resource-explorer-2 create-view \
    --view-name My-New-View \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
```

```
        ],
        "LastUpdatedAt": "2022-07-27T16:34:14.960000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222"
    }
}
```

Example 第 4 步：将新视图设置为其默认视图 AWS 区域

以下示例将您在上一步创建的视图设置为区域的默认视图。必须使用与创建默认视图相同的 AWS 区域 命令运行以下命令。

```
$ aws resource-explorer-2 associate-default-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

您必须先向用户授予使用该视图的权限，然后他们才能使用该视图。有关更多信息，请参阅授予对资源管理器视图的访问权限以进行搜索。

运行这些命令后，资源管理器将在 AWS 账户 中的指定区域中运行。资源管理器每个区域中构建和维护一个索引，其中包含位于该区域的资源的详细信息。资源管理器将每个单独的区域索引复制到指定区域中的聚合器索引中。该区域还包含一个视图，该视图允许账户中的任何 IAM 角色或用户在所有已编入索引的区域中搜索资源。

> **Note**
>
> 索引本地的已标记资源会在几分钟内出现在搜索结果中。未标记的资源通常需要不到两个小时的时间便可以显示，但在需求旺盛时可能需要更长的时间。完成从所有现有本地索引向新聚合器索引的初始复制过程，也可能需要长达一个小时。

管理资源管理器以支持搜索资源

在您最初在您的 AWS 账户 中的至少一个 AWS 区域 中开启 AWS 资源探索器 之后，您可能需要偶尔执行一些管理任务。本部分介绍维护和配置任务，这些任务可帮助您随着 AWS 账户 和资源使用量的变化使资源管理器按您想要的方式工作。

主题

检查哪些 AWS 区域 开启了资源管理器

您可以通过查看哪些区域包含资源管理器的索引来找出哪些 AWS 区域 已开启 AWS 资源探索器。要查看哪些区域有索引，请使用本页上的步骤。

> **Important**
>
> 用户只能在已开启资源管理器的区域中搜索资源。您还可以在一个区域中创建聚合器索引，以支持在所有区域中搜索资源。资源管理器会将资源信息从包含资源管理器索引的所有其他区域复制到带有聚合器索引的区域。用户无法使用资源管理器来发现没有索引的区域中的资源。

检查区域中的资源管理器状态

您可以使用 AWS Management Console、使用 AWS Command Line Interface（AWS CLI）中的命令或在 AWS SDK 中使用 API 操作来检查哪些区域具有资源管理器的索引。

AWS Management Console

要查看哪些区域有资源管理器的索引

1. 在资源管理器控制台中打开设置页面。
2. 索引部分的列表仅包括那些包含资源管理器索引的区域。类型列中的值表示该索引是其区域的本地索引，还是 AWS 账户 的聚合器索引。
3. 要查看哪些区域不包含资源管理器，请选择创建索引。如果某个区域没有列出，则该区域不包含资源管理器。

AWS CLI

要查看哪些区域有资源管理器的索引

运行以下命令以查看哪些 AWS 区域 具有资源管理器的索引。

```
$ aws resource-explorer-2 list-indexes
{
    "Indexes": [
        {
            "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Region": "us-east-1",
            "Type": "AGGREGATOR"
        },
        {
            "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
            "Region":"us-west-2",
            "Type":"LOCAL"
        }
    ]
}
```

开启多账户搜索

通过多账户搜索，您可以跨账户搜索在您 AWS Organizations 或组织单位 (OU) 中具有活动索引的账户。

主题

先决条件

要为您的组织开启多账户搜索功能，请完成以下操作：

- 对于选择加入的区域，请确认您的管理账户是否也已选择加入，同时您正在开启多账户搜索。
- 创建管理用户。
- 使用 `aws iam create-service-linked-role --aws-service-name resource-explorer-2.amazonaws.com` 在管理员账户中创建服务相关角色。
- 在中@@ 启用可信访问 AWS Organizations。这样可与资源管理器完全集成，从而列出组织中的所有账户中的资源。
- 分配委派的管理员（推荐）。有关更多信息，请参阅《AWS Organizations 用户指南》中的与 Organizations 配合使用的 AWS 服务的委派管理员。
  - 资源管理器仅支持 1 位执行与管理账户类似操作的委派管理员。
  - 移除或更改组织的委派管理员会导致在其账户中创建的所有多账户视图被移除。

启用多账户搜索

要在组织中的账户间搜索和发现资源，必须完成以下步骤：

1. AWS 资源探索器 在您的一个或多个帐户中激活 AWS Organizations。
2. 注册一个区域以包含聚合器索引。
3. 选择要在其中创建聚合器索引的区域。该区域必须与您的区域保持一致 AWS Organizations。
4. 创建限定于您 AWS Organizations 或组织单位的资源浏览器视图。在上一步中的聚合区域中创建此视图。
5. 与您组织中的账户共享视图。

多账户快速设置功能

使用快速设置功能在组织中的多个账户中启用资源管理器。

> **Note**
>
> 此过程不会在管理账户中部署任何资源。如果您使用的是管理账户，并且想要在账户中加入索引，则必须使用资源管理器引导流程手动添加索引。

1. 在 Systems Manager 控制台中导航到资源管理器的快速设置功能。
2. 选择您的聚合器索引区域。这样，您就可以搜索位于所选目标账户中所有区域的资源。如果任何选定的目标账户已经在其他区域配置了聚合器索引，则现有的聚合器索引将自动替换为这个新区域。
3. 选择您的账户目标。您可以为整个组织或特定组织单位（OU）启用资源管理器。

   > **Note**
   >
   > 您一次最多可以部署到 50,000 个 AWS CloudFormation 堆栈。如果您的大型组织跨越多个区域，则应在 OU 级别进行小批量部署。

4. 在选择创建之前，请仔细阅读确认摘要。

在 AWS 区域 中启用资源管理器以索引您的资源

最初在 AWS 账户 中开启 AWS 资源探索器 时，您在一个或多个 AWS 区域 中为服务创建了索引。如果您使用了快速设置功能选项，则资源管理器会自动在已在您的 AWS 账户 中开启的 AWS 区域 中创建索引。资源管理器服务还已将指定区域中的索引提升为账户的聚合器索引。如果您使用高级设置功能选项，则指定了要在其中创建索引的区域。

要在其他区域开启资源管理器，请使用本主题中的过程。

在 AWS 区域 中打开资源管理器时，该服务将执行以下操作：

- 在 AWS 账户 中的第一个区域中启动资源管理器时，资源管理器会在名为 AWSServiceRoleForResourceExplorer 的账户中创建一个服务相关角色。此角色授予资源管理器使用诸如 AWS CloudTrail 和标记服务等服务的权限，以发现和索引您账户中的资源。只有当您在账户中注册第一个 AWS 区域 时，才会创建服务相关角色。资源管理器对您稍后添加的所有其他区域使用同一个服务相关角色。
- 资源管理器在指定区域创建索引，以存储有关该区域资源的详细信息。
- 资源管理器开始发现指定区域中的资源，并将其找到的有关这些资源的信息添加到该区域的索引中。

- 如果您的账户已包含其他区域中的聚合器索引，则资源管理器会开始将新区域索引中的信息复制到聚合器索引中，以支持跨区域搜索。

这些步骤完成后，用户就可以发现有关您的资源的信息。他们可以使用在同一区域或包含聚合器索引的区域中定义的其中一个视图进行搜索。

在区域中创建资源管理器索引

您可以使用 AWS Management Console、使用 AWS Command Line Interface（AWS CLI）中的命令或在 AWS SDK 中使用 API 操作，在另一个 AWS 区域 中创建资源管理器索引。您只能在一个区域中创建一个索引。

最小权限

要执行下列程序中的步骤，您必须具有以下权限：

- 操作：`resource-explorer-2:*` – 资源：无特定资源（`*`）
- 操作：`iam:CreateServiceLinkedRole` – 资源：无特定资源（`*`）

AWS Management Console

要在 AWS 区域 中创建资源管理器索引

1. 在资源管理器设置页面上。
2. 在索引部分中，选择创建索引。
3. 在创建索引页面上，选中您要在其中创建索引以支持搜索该区域的资源的 AWS 区域 旁的复选框。“不可用”复选框表示已包含资源管理器索引的区域。
4. （可选）在标签部分，您可以为索引指定标签键值对。
5. 选择创建索引。

   资源管理器会在页面顶部显示绿色横幅以表示成功，如果在一个或多个选定区域中创建索引出现错误，则显示红色横幅。

> **Note**
>
> 索引本地的已标记资源会在几分钟内出现在搜索结果中。未标记的资源通常需要不到两个小时的时间便可以显示，但在需求旺盛时可能需要更长的时间。完成从所有现有本地索引向新聚合器索引的初始复制过程，也可能需要长达一个小时。

下一步 – 如果您已经创建了聚合器索引，则新区域会自动开始将其索引信息复制到聚合器索引。如果您的用户在那里进行所有搜索，则新区域中的资源将会出现在这些搜索结果中，表示您已完成。

但是，如果您希望用户只能在新编入索引的区域中搜索资源，则还必须为该区域中的用户创建视图，并向您的用户授予该视图的访问权限。有关如何创建视图的说明，请参阅 管理资源管理器视图以提供搜索访问权限。

AWS CLI

要在 AWS 区域 中创建资源管理器索引

对要在其中创建索引以支持搜索该区域的资源的每个 AWS 区域，运行以下命令。以下示例命令在美国东部（弗吉尼亚州北部）（us-east-1）中注册资源管理器。

```
$ aws resource-explorer-2 create-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-11-01T20:00:59.149Z",
    "State": "CREATING"
}
```

对您要在其中开启资源管理器的每个区域重复此命令，用相应的区域代码代替 --region 参数。

由于资源管理器在后台以异步任务的形式执行某些索引创建，因此响应可能是 CREATING，表示后台进程尚未完成。

> **Note**
>
> 索引本地的已标记资源会在几分钟内出现在搜索结果中。未标记的资源通常需要不到两个小时的时间便可以显示，但在需求旺盛时可能需要更长的时间。完成从所有现有本地索引向新聚合器索引的初始复制过程，也可能需要长达一个小时。

您可以通过运行以下命令并检查 ACTIVE 状态来检查最终完成情况。

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

下一步 – 如果您已经创建了聚合器索引，则新区域会自动开始将其索引信息复制到聚合器索引。如果您的用户在那里进行所有搜索，则新区域中的资源将会出现在这些搜索结果中，表示您已完成。

但是，如果您希望用户只能在新编入索引的区域中搜索资源，则还必须为该区域中的用户创建视图，并向您的用户授予该视图的访问权限。有关如何创建视图的说明，请参阅 管理资源管理器视图以提供搜索访问权限。

AWS 选择加入区域的注意事项

选择加入区域比商业区域具有更高的安全要求，因为它涉及到通过选择加入区域中的账户共享 IAM 数据。通过 IAM 服务管理的所有数据都被视为身份数据。

您可以使用 AWS 资源探索器 控制台激活选择加入区域。有关更多信息，请参阅中的打开资源浏览器 AWS 区域 以索引您的资源。

选择退出行为

在选择退出加入的区域之前，请考虑以下行为：

> **Important**
>
> 在您选择退出包含聚合器索引的区域之前，建议您删除聚合器索引或将其降级为本地索引。资源管理器支持在分区内的所有区域中使用一个聚合器索引。

- 您的索引并未被删除，只是被禁用。如果您选择稍后再次加入，则您的设置将恢复。
- IAM 禁用 IAM 对该区域资源的访问权限。
- 资源管理器会禁用已选择退出的区域的索引并停止提取数据。`ListIndexes` API 将不再显示区域索引。
- 如果您的聚合器索引位于其他区域，则资源管理器会停止从已选择退出的区域复制数据，并在 24 小时内清理该数据。
- 如果您选择退出聚合器索引区域，则必须再次选择加入才能删除或降级索引。
- 如果您再次选择加入该区域，资源管理器会重新启用索引并开始提取数据。
- 对选择加入区域的状态的任何更改都需要大约 24 小时才能生效。

通过创建聚合器索引开启跨区域搜索

主题

关于聚合器索引

AWS 资源探索器 将其收集的有关资源的信息存储在 AWS 区域 的本地索引中，资源管理器在该区域创建和维护该索引。例如，假定您的一个 Amazon EC2 实例位于美国西部（俄勒冈州）区域。资源管理器将有关该资源的详细信息存储在美国西部（俄勒冈州）区域的本地索引中。

为了支持在您的账户跨所有 AWS 区域 搜索资源，您可以将一个区域中的本地索引转换为您账户的聚合器索引。

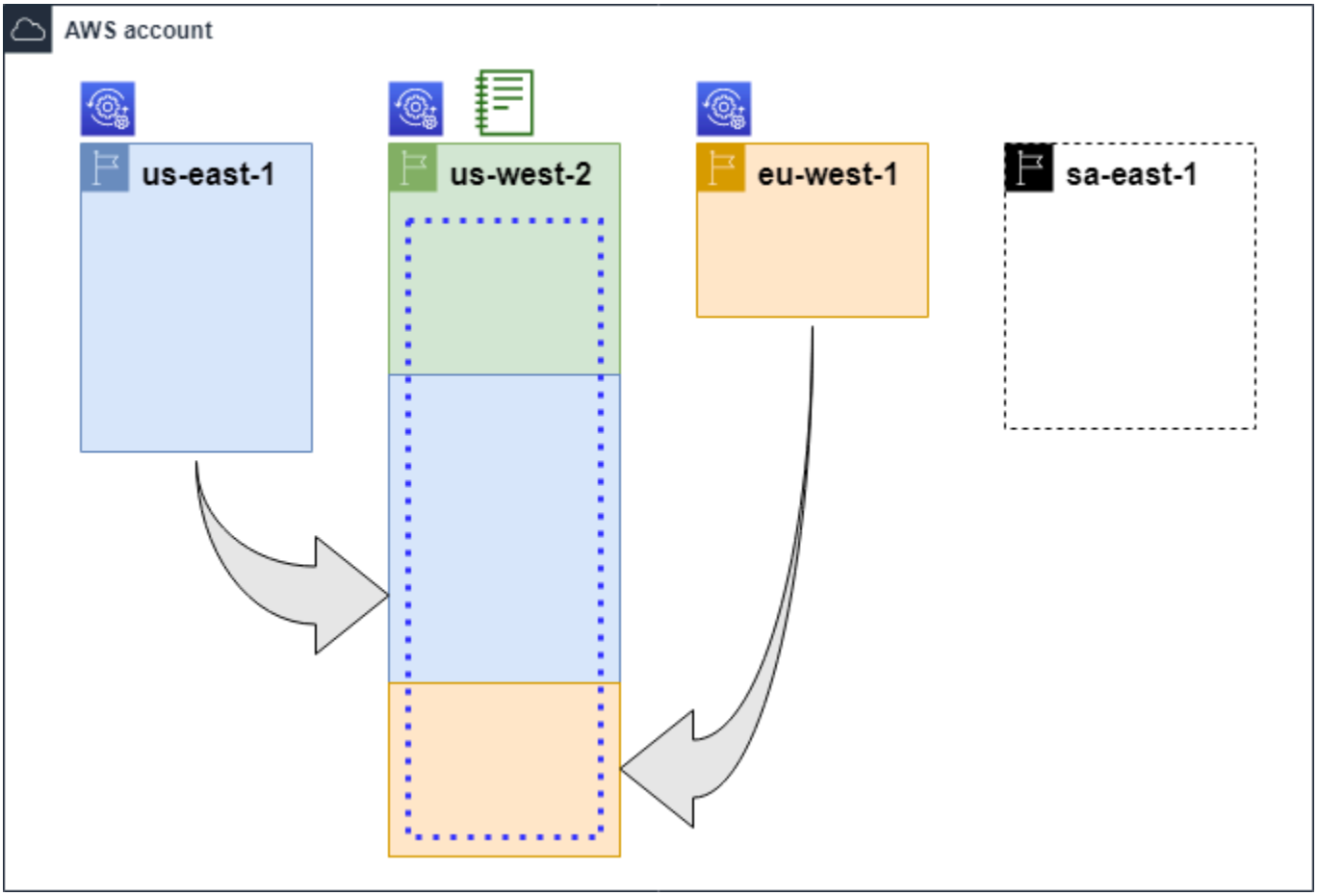
聚合器索引包含您开启资源管理器所在的每个其他区域的本地索引的复制副本。这使您可以在包含聚合器索引的区域（其结果可以包含来自账户中所有 AWS 区域 的资源）中创建视图。

下图显示了聚合器索引的工作原理的示例。在此示例 AWS 账户 中，管理员执行以下操作：

- 通过在三个 AWS 区域（`us-east-1`、`us-west-2` 和 `eu-west-1`）区域中创建索引来在这三个区域开启资源管理器。每个区域都包含自己的本地索引。
- 选择不在 `sa-east-1` 区域创建索引。用户无法在 `sa-east-1` 中执行搜索，并且该地区的资源也不会出现在任何搜索结果中。

- 为 us-west-2 区域中的账户创建聚合器索引。这会导致资源管理器将已开启资源管理器的所有其他区域中的本地索引的信息复制到聚合器索引。这允许在 us-west-2 中执行的搜索包括来自所有三个已开启资源管理器的区域的资源。

此配置意味着用户只能在 us-west-2 中执行跨区域搜索，该区域包含聚合器索引。只有来自该区域的视图才能返回账户中所有区域的结果。



图例	
	资源管理器在此 AWS 区域 中处于开启状态，其资源被编入该区域的索引中。该区域的索引（由箭头指示）也被复制到包含聚合器索引的 AWS 区域 中。
	此 AWS 区域 包含聚合器索引。资源管理器会将在所有其他 AWS 区域 中收集的资源信息复制到该区域。

	快速设置功能创建的默认视图包含所有 AWS 区域 中的所有资源。

将本地索引提升为账户的聚合器索引

首次设置 AWS 资源探索器 时，您可以选择在一个 AWS 区域 中创建聚合器索引。有关更多信息，请参阅设置和配置资源管理器。此过程旨在将其中一个本地索引提升为账户的聚合器索引（如果您在初始设置时没有这样做）。

> **Important**
>
> - 您在一个 AWS 账户 中只能有一个聚合器索引。如果该账户已有聚合器索引，则您必须先将其降级为本地索引或将其删除。
> - 删除或更改包含聚合器索引的区域后，必须等待 24 小时才能将另一个索引提升为聚合器索引。

AWS Management Console

要将本地索引提升为账户的聚合器索引

1. 打开资源管理器设置页面。
2. 在索引部分，选中要提升的索引旁边的复选框，然后选择更改索引类型。
3. 在更改 <区域名称>的索引类型对话框中，选择聚合器索引，然后选择保存更改。

AWS CLI

要将本地索引提升为账户的聚合器索引

以下示例命令将指定的 AWS 区域 中的索引类型从类型 LOCAL 更新为类型 AGGREGATOR。您必须从想要包含聚合器索引的 AWS 区域 中调用操作。

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR \
    --region us-east-1
```

```
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"AGGREGATOR"
}
```

该操作以异步方式运行，并在 State 被设置为 UPDATING 的情况下启动。要检查操作是否已完成，可以运行以下命令并在 State 响应字段中查找值 ACTIVE。您必须在包含要检查的索引的区域中运行此命令。

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "AGGREGATOR"
}
```

将聚合器索引降级为本地索引

您可以将聚合器索引降级为本地索引，例如当您要将聚合器索引移到其他 AWS 区域 时。

当您将聚合器索引降级为本地索引时，资源管理器会停止从其他 AWS 区域 复制索引。它还会启动异步后台任务，以从其他区域删除任何复制的信息。在该异步任务完成之前，某些跨区域结果可以继续出现在搜索结果中。

注意事项

- 将聚合器索引降级后，必须等待 24 小时才能将同一索引或位于不同区域的索引提升为该账户的新聚合器索引。

- 降级聚合器索引后，后台进程最多可能需要 36 小时才能完成，而来自其他区域的所有资源信息则会从该区域执行的搜索结果中消失。
- 如果您在组织范围内降级某个成员账户，则该成员可能会被从多账户搜索中移除。

您可以通过在 “设置” 页面上查看索引列表或使用GetIndex操作来检查后台任务的状态。异步任务完成后，索引中的 `Status` 字段将从 `UPDATING` 变为 `ACTIVE`。那时，只有来自本地区域的结果才会出现在查询结果中。

AWS Management Console

要将聚合器索引降级为本地索引

1. 打开资源管理器设置页面。
2. 在索引部分中，选中包含要降级为本地索引的聚合器索引的区域旁边的复选框，然后选择更改索引类型。
3. 在更改 <区域名称>的索引类型对话框中，选择本地索引，然后选择保存更改。

AWS CLI

要将聚合器索引降级为本地索引

以下示例将指定的聚合器索引降级为本地索引。您必须在当前包含聚合器索引的 AWS 区域 中调用操作。

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type LOCAL \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"LOCAL"
}
```

该操作以异步方式运行，并在 State 被设置为 UPDATING 的情况下启动。要检查操作是否已完成，可以运行以下命令并在 State 响应字段中查找值 ACTIVE。您必须在包含要检查的索引的区域中运行此命令。

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

支持在 AWS Management Console 中使用统一搜索

AWS Management Console 在每个控制台页面的顶部都有一个搜索栏。这提供了跨所有 AWS 服务 进行统一搜索的体验。统一搜索结果可能包括以下内容：

- AWS 服务 和功能控制台页面。
- AWS 文档页面。
- AWS 博客和知识库文章
- 账户中的资源 — 如果您按照以下步骤执行。

若要在统一搜索结果中查看您账户的资源，您必须执行以下步骤。您可以在 AWS 资源探索器 的初始设置期间执行此操作。如果您使用快速设置功能选项，这一切都会自动发生。

- 您必须在一个 AWS 区域 中为 AWS 账户 创建一个聚合器索引。
- 您必须在包含聚合器索引的 AWS 区域 中创建默认视图。
- 您必须向所有需要在统一搜索栏中搜索资源的主体授予使用该默认视图进行搜索的权限。

统一搜索始终使用包含聚合器索引的 AWS 区域 中的默认视图执行所有搜索。

账户操作对资源管理器多账户搜索的影响

> **Note**
>
> 从多账户搜索结果中移除账户和资源最多需要 24 小时。

账户操作会对 AWS 资源探索器 多账户搜索产生以下影响。

资源管理器已禁用

禁用账户的资源管理器时，将仅禁用您在禁用它时选择的 AWS 区域 中的该账户的资源管理器。

您必须在启用资源管理器的每个区域分别禁用它。

24 小时后，此账户的资源将不会出现在搜索结果中。

不会移除其他资源管理器数据和设置。

成员账户从组织中移除

从组织中移除成员账户后，资源管理器管理员账户将失去查看该成员账户中资源的权限。

如果被移除的账户是管理员或委派管理员账户，则这些账户之前创建的所有多账户视图也将被移除。

资源管理器继续在两个账户中运行。

资源搜索结果不再包含来自该账户的资源。

账户已暂停

账户在 AWS 中被暂停后，该账户将失去在资源管理器中查看资源的权限。已暂停账户的管理员账户可以查看现有资源。

对于组织账户，成员账户状态也可以更改为账户已暂停。如果该账户在管理员账户尝试启用账户的同时被暂停，则会发生这种情况。被暂停的账户的管理员账户无法查看该账户的资源。

否则，暂停状态不会影响成员账户状态。

90 天后，该账户将被停用或重新激活。重新激活账户后，其资源管理器权限将恢复。如果成员账户状态为账户已暂停，则管理员账户必须手动启用该账户。

账户已关闭

关闭 AWS 账户后，资源管理器会按以下方式对关闭做出响应：

- 资源管理器将在关闭账户生效之日起 90 天内保留该账户的资源。在 90 天期限结束时，资源管理器会永久删除该账户的所有资源。
- 要将资源保留超过 90 天，您可以使用带有 EventBridge 规则的自定义操作将资源存储在 Amazon S3 存储桶中。只要资源管理器保留资源，当您重新打开关闭的账户时，资源管理器就会恢复该账户的资源。
- 如果该账户是资源管理器管理员账户，则会以管理员身份移除该账户，并移除所有成员账户。如果该账户是成员账户，则会将其以成员身份从资源管理器管理员账户中解除关联和移除。
- 有关更多信息，请参阅关闭账户。

账户选择退出

如果账户选择退出某个区域，您仍会在 24 小时内在搜索结果中看到他们的资源。

24 小时后，此账户的资源将不会出现在搜索结果中。有关更多信息，请参阅 选择退出行为。

关闭一个 AWS 区域 中的资源管理器

当您不再需要在特定 AWS 区域 中搜索资源时，您可以通过删除该其索引来仅在该区域中将 AWS 资源探索器 关闭。当您执行此操作时，资源管理器将停止扫描该区域中的新资源或更新的资源。如果您的账户包含聚合器索引，则从已删除索引的复制将停止，并且已删除索引中的信息将从聚合器索引中移除，并停止显示在搜索结果中。已删除索引中的所有资源最多可能需要 24 小时才能从具有聚合器索引的区域的搜索结果中消失。

> **Note**
>
> 注册第一个 AWS 区域 时，资源管理器会在 AWS 账户 中创建一个名为 `AWSServiceRoleForResourceExplorer` 的服务相关角色（SLR）。资源管理器不会自动删除此 SLR。删除账户中每个区域的资源管理器索引后，如果您将来不会再使用资源管理器，则可以使用 IAM 控制台删除此 SLR。如果您确实删除了该角色，然后选择至少在一个 AWS 区域 中再次开启资源管理器，则资源管理器会自动重新创建服务相关角色。

您可以使用 AWS Management Console、使用 AWS Command Line Interface（AWS CLI）中的命令或在 AWS SDK 中使用 API 操作来关闭 AWS 区域 中的资源管理器。

如果您关闭了某个成员账户的资源管理器，并且该成员处于组织范围内，则该成员将从多账户搜索结果中移除。

如果您不想再支持在账户中的一个或多个 AWS 区域 中搜索资源，请执行以下过程中的步骤。

> **Note**
>
> 如果您删除的索引是 AWS 账户 的聚合器索引，则必须等待 24 小时才能将另一个本地索引提升为该账户的聚合器索引。在配置另一个聚合器索引之前，用户无法使用资源管理器执行账户范围的搜索。

AWS Management Console

要在 AWS 区域 中删除资源管理器索引

1. 打开资源管理器设置页面。
2. 在索引部分，选中具有您要删除的索引的 AWS 区域 旁边的复选框，然后选择删除。
3. 在删除索引页面上，确认您只选中了要删除的索引。在确认文本框中键入 **delete**，然后选择删除索引。

   资源管理器会在页面顶部显示绿色横幅以表示成功，如果一个或多个选定区域出现错误，则显示红色横幅。

AWS CLI

要在 AWS 区域 中删除资源管理器索引

如果您不想再支持在账户中的一个或多个 AWS 区域 中搜索资源，请运行以下命令。

为包含您要删除的索引的每个区域运行以下命令。您必须在包含要删除的索引的区域中运行此命令。以下示例命令删除了美国西部（俄勒冈州）（us-west-2）的资源管理器索引。

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222 \
    --region us-west-2
{
```

```
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
    "State": "DELETING"
}
```

由于资源管理器在后台以异步任务的形式执行某些删除清理工作，因此响应可能表明该操作为 DELETING。此状态表示后台进程尚未完成。您可以通过运行以下命令并检查要更改为 DELETED 的 State 来检查最终完成情况。

```
$ aws resource-explorer-2 get-index \
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

关闭所有 AWS 区域 中的资源管理器

如果要完全关闭 AWS 资源探索器，请执行以下步骤。

> **Note**
>
> 当您在第一个 AWS 区域 中为账户创建索引时，资源管理器会在账户中创建一个名为 AWSServiceRoleForResourceExplorer 的服务相关角色。资源管理器不会自动删除此服务相关角色。删除每个区域的资源管理器索引后，如果您确定将来不会再使用资源管理器，则可以使用 IAM 控制台删除该角色。如果您确实删除了该角色，然后选择在至少一个 AWS 区域 中启动资源管理器器，则资源管理器会重新创建服务相关角色。

关闭所有 AWS 区域 中的资源管理器

您可以使用 AWS Management Console、使用 AWS Command Line Interface（AWS CLI）中的命令或在 AWS SDK 中使用 API 操作来关闭资源管理器。

AWS Management Console

如果您不想再支持在 AWS 账户 中的任何 AWS 区域 中搜索资源，请执行以下过程中的步骤。

要关闭所有 AWS 区域 中的资源管理器

1. 打开资源管理器设置页面。
2. 在索引部分中，选中所有已注册 AWS 区域 旁边的复选框，然后选择删除。

   > **Tip**
   >
   > 您可以选中索引旁边表格标题行中的复选框，只需一个步骤即可选中所有区域的复选框。

3. 在删除索引页面上，确认要删除所有索引。在确认文本框中键入 **delete**，然后选择删除索引。

   资源管理器会在页面顶部显示绿色横幅以表示成功，如果一个或多个选定区域出现错误，则显示红色横幅。

AWS CLI

要关闭所有 AWS 区域 中的资源管理器

如果您不想再支持在您的账户中的任何 AWS 区域 中搜索资源，请运行以下命令来查找您之前开启资源管理器所在的每个 AWS 区域 中每个索引的 ARN。

```
$ aws resource-explorer-2 list-indexes --query Indexes[*].Arn[
"arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
"arn:aws:resource-explorer-2:us-west-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
"arn:aws:resource-explorer-2:us-west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd33333333"
]
```

对于每个响应，运行以下命令以删除该区域中的资源管理器索引。

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
```

```
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "State": "DELETING"
}
```

在其他每个区域中重复上一个命令。

由于资源管理器在后台以异步任务的形式执行某些清理，因此响应可能表明该操作为 DELETING。此状态表示后台进程尚未完成。您可以通过运行以下命令并检查要更改为 DELETED 的状态来检查最终完成情况。

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

为组织中的账户部署资源管理器

通过使用 AWS CloudFormation StackSetss，您可以定义并部署到组织中由 AWS Organizations 管理的所有账户。定义堆栈集时，您可以指定要在您的 AWS 区域 中和您指定的所有目标账户中创建的 AWS 资源。当所有账户都属于同一个组织时，您可以利用 AWS CloudFormation 与 Organizations 的集成，让这些服务来处理跨账户角色的创建。您可以在组织中启用自动部署，这样可以自动将堆栈实例部署到您将来可能会添加到目标组织或组织单位（OU）的新账户。如果您从组织中移除账户，则 AWS CloudFormation 会自动删除作为组织堆栈实例一部分部署的所有资源。有关 StackSets 的更多信息，请参阅《AWS CloudFormation 用户指南》中的使用 AWS CloudFormation StackSets。

您可以使用 AWS CloudFormation StackSets 在组织中的所有账户中开启和配置 AWS 资源探索器，在每个启用的区域中创建索引，并在需要时创建视图。

> **Important**
>
> 如果您尝试在某个区域中设置聚合器索引，则必须确保该账户在任何其他区域中都没有现有的聚合器索引。将聚合器索引降级到本地索引后，必须等待 24 小时才能将另一个索引提升为该账户的新聚合器索引。

先决条件

要使用 AWS CloudFormation StackSets 将资源管理器部署到组织中的账户，您或您的组织管理员必须先执行以下步骤以启用具有服务管理权限的堆栈：

1. 的组织必须已启用所有功能。如果组织仅启用了整合账单功能时，您无法创建具有服务托管权限的堆栈集。
2. 开启 AWS CloudFormation 与 Organizations 之间的可信访问权限。这会授予在组织管理账户中创建所需角色的 AWS CloudFormation 权限，成员账户 AWS CloudFormation 将部署资源管理器索引和视图。

现在，您可以创建具有服务托管权限的堆栈集。

> **Important**
>
> 您必须在组织的管理账户中创建堆栈集。AWS CloudFormation 是一项区域性服务，因此您只能在最初创建堆栈集的区域中查看和管理您创建的堆栈集。

为资源管理器创建堆栈集

完全部署的资源管理器必须部署两个堆栈集。

- 第一个堆栈集创建聚合器索引和默认视图，允许用户在账户中的所有区域中搜索资源。

  将此堆栈集仅部署到要在其中创建聚合器索引的单个区域。
- 第二个堆栈集创建本地索引和默认视图。本地索引将其内容复制到聚合器索引。

  将此堆栈集部署到账户中除包含聚合器索引的区域之外的所有已启用区域。不要在部署堆栈的账户中选择任何未启用的区域。如果您这样做，则部署将失败。

以下部分中列出了这些内容中每一个的示例模板。有关如何使用这些模板创建堆栈集的分步说明，请参阅《AWS CloudFormation 用户指南》中的使用服务托管权限创建堆栈集。

将这些堆栈集部署到您的组织后，您所选范围内的每个账户（组织或组织单位）在指定的区域中都有一个聚合索引，在其他每个区域都有本地索引。

示例 AWS CloudFormation 模板

以下示例模板创建了账户的聚合器索引和默认视图，该视图可以在部署索引的账户中跨所有区域搜索资源。

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with an Aggregator Index, and a new Default
 View.
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with an Aggregator Index,
 and a new Default View.",
```

```
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

以下示例模板在每个已启用的区域中为除了具有聚合器索引的账户之外的所有账户创建本地索引。它还创建了一个默认视图，用户只能在该区域中搜索资源。用户必须使用聚合器区域中的视图进行搜索，才能在所有区域中搜索资源。

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with a Local Index, and a new Default View.
```

```
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: LOCAL
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with a Local Index, and a
 new Default View.",
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "LOCAL",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
```

```
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

管理资源管理器视图以提供搜索访问权限

视图是搜索资源的关键。每个 AWS 资源探索器 搜索操作都必须使用一个视图。

视图指的是管理员可以用来控制对您的 AWS 账户 中的资源的相关信息的访问权限的方法。

只有有权使用视图的主体（IAM 角色或用户）才能访问该视图。要使用资源管理器成功搜索，主体必须具有对视图的 ARN 上的 `resource-explorer-2:GetView` 和 `resource-explorer-2:Search` 操作的 `Allow` 访问权限。

视图包含内置筛选条件，管理员可以使用这些筛选条件将结果限制为仅显示感兴趣的项目。例如，您可以创建一个仅包含与特定项目相关的资源的视图。不需要查看其他项目信息的用户可以使用此视图以仅查看感兴趣的资源。

视图是一种区域性资源。视图创建并存储在特定 AWS 区域 区域中，其结果中仅返回该区域中的索引的信息。要将来自账户中的所有区域的结果包括在内，视图必须位于包含聚合器索引的区域中。该区域包含账户中所有其他区域的索引的副本。

有关创建和使用视图的更多信息，请参阅以下主题。

主题

- 关于资源管理器视图
- 创建用于搜索的资源管理器视图
- 授予对资源管理器视图的访问权限以进行搜索
- 在 AWS 区域 中设置默认视图
- 向视图添加标签
- 共享资源管理器视图
- 在资源管理器中删除视图

关于资源管理器视图

AWS 资源探索器 在后台为您的资源编制索引，然后使该索引可供您查询。您可以使用本指南中记录的资源管理器 API，或使用资源管理器控制台对资源执行搜索查询。资源管理器使用其 API 为原本只能通过编程访问的 API 提供交互式图形界面。本主题中描述的概念同时适用于 API 和控制台。

视图存储在 AWS 区域 中，仅返回来自该区域索引的结果。

由于管理员可能希望限制对资源索引中包含的信息的访问权限，因此无法直接访问索引本身。相反，所有搜索都必须通过用户必须具有搜索权限的视图进行。

每个视图都有几个关键要素：

搜索权限

您可以使用标准的 AWS 权限策略来控制谁可以使用每个视图。这是由附加于主体的基于身份的权限策略提供的，这些策略使您可以精细控制谁可以看到每个视图提供的信息。例如，您可以授予访问 `Production-resources` 视图的权限，从而仅允许操作您的生产服务的工程师进行搜索。然后，您可以授予对 `Pre-production-resources` 视图的不同权限，以允许开发人员搜索预生产资源。

如果您将名为 `AWSResourceExplorerReadOnlyAccess` 的 AWS 托管策略用于主体，则会授予他们使用账户中的任何视图进行搜索的能力。

或者，您也可以创建自己的权限策略，并仅为指定的视图授予以下权限：

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

要提供访问权限，请为您的用户、组或角色添加权限：

- AWS IAM Identity Center 中的用户和组：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中 创建权限集 的说明进行操作。
- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

有关使用与视图相关的权限的更多信息，请参阅 授予对资源管理器视图的访问权限以进行搜索。

筛选搜索

视图可用作虚拟窗口，用户可以通过该窗口查看账户中的资源。您可以创建多个视图，每个视图均显示大图的不同视图。例如，您可以创建一个视图，以仅允许搜索与预生产环境关联的资源，这些

资源通过附加到资源的标签标识。然后，您可以创建一个单独的视图，以仅允许根据标签中的不同值搜索生产环境中的资源。如果您使用不同的 `FilterString` 值配置多个视图，则不必在每次搜索时重新输入这些查询参数。

视图还可以指定要在结果中包含有关资源的哪些可选信息。默认字段列表始终包含在结果中。除了默认列表外，您还可以要求视图中同时包含附加到资源的任何标签。

搜索范围

- 区域范围 – 当您使用资源管理器在 AWS 区域 中进行搜索时，结果只能包含在该区域中编制索引的资源。大多数区域的索引之所以被标记为 `LOCAL`，是因为它仅包含有关该区域内资源的信息。在这些区域进行搜索只能返回这些资源。
- 账户范围 – 您只能将一个本地索引提升为账户的聚合器索引。执行此操作时，所有其他已开启资源管理器的区域都会将其索引信息复制到包含聚合器索引的区域。如果您在该区域进行搜索，则这些结果将包括该账户中所有区域的资源。当您使用快速设置功能选项配置服务器时，资源管理器会自动在您指定的区域中创建聚合器索引。此外，快速设置功能选项会在该区域创建默认视图，以支持在所有区域中搜索账户中的所有资源。

默认视图

如果用户在未明确指定视图的情况下尝试搜索，则资源管理器将使用为该 AWS 区域 定义的默认视图。

如果该区域不存在默认视图，且用户未指定要使用的视图，则搜索将会失败并生成异常。

资源管理器会自动创建默认视图，如下所示：

- 如果您使用 AWS Management Console 开启资源管理器并选择快速设置功能选项，则必须指定哪个区域包含该账户的聚合器索引。资源管理器会自动在指定的聚合器索引区域中创建默认视图。
- 如果您使用 AWS Management Console 注册资源管理器并选择高级设置功能选项，则可以选择为指定区域中的账户创建聚合器索引。如果您执行此操作，则资源管理器会自动在聚合器索引区域中创建默认视图。
- 如果您使用控制台注册资源管理器并选择不注册聚合器索引区域，则资源管理器会为每个区域中的本地索引创建默认视图。
- 如果您使用 AWS CLI 或 API 操作注册资源管理器，则资源管理器不会自动创建默认视图。反之，您必须为希望用户搜索的每个区域手动配置默认视图。

创建用于搜索的资源管理器视图

所有搜索都必须使用视图。视图定义用于确定使用该视图的查询可以返回哪些资源的筛选条件。视图还可以控制谁能搜索资源。

视图存储在中 AWS 区域，仅返回来自该区域索引的搜索结果。如果区域包含聚合器索引，则视图会返回账户中每个区域中的索引的搜索结果。

多账户视图使您能够在组织内的账户中搜索资源。您要搜索的任何账户都需要索引。只有组织的管理账户或委派管理员才能创建多账户视图。

AWS 资源探索器 如果您在 Systems Manager 控制台的 “资源浏览器的快速设置” 或 “高级设置” 中选择了相关选项，则可以在初始设置期间为您创建默认视图。之后，您可以为不同的用户组创建具有不同筛选条件的其他视图。

您可以使用或在 AWS SDK 中运行 AWS CLI 命令 AWS Management Console 或其等效的 API 操作来创建视图。

最小权限

要运行此过程，您必须具有以下权限：

- 操作：`resource-explorer-2:CreateView`

  资源：这可以是*为了允许在账户中的任何一个 AWS 区域 中创建视图。

AWS Management Console

要创建视图

1. 打开资源管理器控制台的视图页面，然后选择创建视图。
2. 在创建视图页面上，在名称中，输入视图的名称。

   名称长度不得超过 64 个字符，可以包含字母、数字和连字符（-）。该名称在其内部必须是唯一的 AWS 区域。
3. 选择要 AWS 区域 在其中创建视图的。要创建从账户中所有区域返回资源的视图，请选择 AWS 区域 包含聚合器索引的。
4. （可选）在范围中，选择您的搜索是返回多账户资源，还是仅返回账户中的资源。账户级范围为默认范围。

只有管理账户或委派管理员才能看到创建多账户视图的选项。

5. 选择是否筛选结果。

   - 包含所有资源

     不包含任何查询筛选条件。与视图关联的索引中的所有资源都可以返回在搜索结果中。

   - 仅包含与指定筛选条件相匹配的资源

     开启资源筛选条件复选框，您可以在其中选择筛选条件名称和运算符。有关每个可用筛选条件名称和运算符的说明，请参阅 筛选条件。

   - 选择要在此视图的结果中包含的可选资源属性。选中标签旁边的复选框，以使用户根据其标签键名称和值搜索资源。如果您未在视图中包含标签，则用户无法使用标签键和值进一步筛选结果来提出搜索请求。

   - 或者，您可以将标签附加到视图。展开标签框，最多输入 50 个标签键/值对。您可以使用标签对资源进行分类，也可以将其作为基于属性的访问权限控制（ABAC）安全权限策略的一部分。有关更多信息，请参阅 向视图添加标签。

   - 选择创建视图。

   控制台返回到搜索页面，您可以在其中使用新视图进行搜索。

   下一步：向账户中的主体授予使用新视图进行搜索的权限。有关更多信息，请参阅 授予对资源管理器视图的访问权限以进行搜索。

AWS CLI

要创建视图

运行以下命令以在指定的 AWS 区域中创建一个视图。以下示例创建了一个视图，该视图仅返回与 Amazon EC2 服务相关且用 `Stage` 键和 `prod` 值标记的资源。

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name "My-EC2-Prod-Resources" \
    --filters FilterString="service:ec2 tag:stage=prod" \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
```

```
            "FilterString": "service:ec2 tag:stage=prod"
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:123456789012:view/My-EC2-
Prod-Resources/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

要创建组织级视图

下面的示例创建一个视图，该视图用于返回组织内资源。该操作必须由组织的管理账户或委派管理员账户执行。

1. 运行 `aws organizations describe-organization` 命令以获取您的组织 ARN。
2. 运行以下命令以为指定的组织创建视图。

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-org-view \
    --scope "arn:aws:organizations::111111111111:organization/o-exampleorgid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "111111111111",
        "Scope": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:111111111111:view/
entire-org-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

要创建组织单位级视图

以下示例创建了一个视图，该视图可返回该组织单位的所有成员的资源。此视图的行为类似于组织级视图。该操作必须由组织的管理账户或委派管理员账户执行。

1. 运行 `aws organizations describe-organizational-unit` 命令以获取您的组织 ARN。
2. 运行以下命令以为指定的组织单位创建视图。

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-ou-view \
    --scope "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "222222222222",
        "Scope": "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:222222222222:view/
entire-ou-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

下一步：向账户中的主体授予使用新视图进行搜索的权限。有关更多信息，请参阅 [授予对资源管理器视图的访问权限以进行搜索]

授予对资源管理器视图的访问权限以进行搜索

您必须先授予对 AWS 资源探索器 视图的访问权限，然后才能使用新视图进行搜索。为此，请对需要使用视图进行搜索的 AWS Identity and Access Management（IAM）主体使用基于身份的权限策略。

要提供访问权限，请为您的用户、组或角色添加权限：

- AWS IAM Identity Center 中的用户和组：

创建权限集合。按照《AWS IAM Identity Center 用户指南》中 创建权限集 的说明进行操作。

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。

- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

您可以使用以下方法之一：

- 使用现有的 AWS 托管策略。资源管理器提供了多个预定义的 AWS 托管策略供您使用。有关所有可用的 AWS 托管策略的详细信息，请参阅 AWS 的托管策略 AWS 资源探索器。

  例如，您可以使用 `AWSResourceExplorerReadOnlyAccess` 策略向账户中的所有视图授予搜索权限。

- 创建自己的权限策略并将其分配给主体。如果您创建自己的策略，则可以通过在策略声明的 `Resource` 元素中指定每个视图的 Amazon 资源名称（ARN）来限制对单个视图或可用视图子集的访问权限。例如，您可以使用以下示例策略授予该主体仅使用该视图进行搜索的能力。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyTestView/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
        }
    ]
}
```

使用 IAM 控制台创建权限策略，并将其与需要这些权限的主体结合使用。有关 IAM 权限策略的更多信息，请参阅以下主题：

- IAM 中的策略和权限
- 添加和移除 IAM 身份权限
- 了解策略授予的权限

使用基于标签的授权来控制对视图的访问权限

如果您选择使用仅返回包含特定资源的结果的筛选条件创建多个视图，则可能还需要将这些视图的访问权限仅限制给需要查看这些资源的主体。您可以使用基于属性的访问控制（ABAC）策略为账户中的视图提供此类安全保护。ABAC 使用的属性是附加到尝试在 AWS 中执行操作的主体和他们尝试访问的资源的标签。

ABAC 使用附加到主体的标准 IAM 权限策略。这些策略使用策略声明中的 Condition 元素，仅当附加到请求主体的标签和附加到受影响资源的标签都符合策略要求时才允许访问。

例如，您可以为支持公司生产应用程序的所有 AWS 资源添加标签 "Environment" = "Production"。为确保只有有权访问生产环境的主体才能看到这些资源，请创建一个使用将该标签用作筛选条件的资源管理器视图。然后，要将视图的访问权限仅限制给相应的主体，您可以使用条件类似于以下示例元素的策略来授予权限。

```
{
    "Effect": "Allow",
    "Action": [ "service:Action1", "service:Action2" ],
    "Resource": "arn:aws:arn-of-a-resource",
    "Condition": { "StringEquals": {"aws:ResourceTag/Environment":
 "${aws:PrincipalTag/Environment}"} }
}
```

前面的示例中的该 Condition 规定，只有当附加到进行请求的主体的 Environment 标签与附加到请求中指定的资源的 Environment 标签相匹配时，才允许该请求。如果这两个标签不完全匹配，或者缺少任何一个标签，资源管理器都会拒绝该请求。

> **Important**
>
> 要成功使用 ABAC 来保护对资源的访问，您必须首先限制对附加到主体和资源的标签进行添加或修改的权限。如果用户可以添加或修改附加到 AWS 主体或资源的标签，则该用户可能会影响受这些标签控制的权限。在安全的 ABAC 环境中，只有经批准的安全管理员才有权添加或修改附加到主体的标签，并且只有安全管理员和资源拥有者才能添加或修改附加到资源的标签。

有关如何成功实施 ABAC 策略的更多信息，请参阅《IAM 用户指南》中的下列主题：

- IAM 教程：根据标签定义访问 AWS 资源的权限
- 使用标签控制对 AWS 资源的访问权限

准备好必要的 ABAC 基础设施后，您可以使用开始使用标签来控制谁可以使用您账户中的资源管理器视图进行搜索。有关说明该原则的示例策略，请参阅下面的示例权限策略：

- 根据标签授予对视图的访问权限
- 授予根据标签创建视图的访问权限

在 AWS 区域 中设置默认视图

在 AWS 资源探索器 中，您可以在 AWS 区域 中定义多个视图，其中每个视图满足不同的搜索要求。建议您在每个区域中将一个视图设置为该区域的默认视图。

每当用户执行搜索且不明确指定要使用哪个视图时，资源管理器都会使用默认视图。每个 AWS Management Console 页面顶部的统一搜索栏还会自动使用包含聚合器索引的区域中的默认视图来查找与用户的搜索查询相匹配的资源。

您只能选择存在于区域中的视图作为该区域的默认视图。如果另一个区域有您要使用的视图，您必须先在要将其设为默认视图的区域中创建该视图的副本。

> **Tip**
>
> 没有复制视图操作。您必须在目标区域中创建视图，然后再将现有视图中的设置复制到新视图。

您可以通过使用 AWS Management Console 或在 AWS SDK 中运行 AWS CLI 命令或其等效的 API 操作，将视图指定为其区域的默认视图。

AWS Management Console

要设置默认视图

1. 在资源管理器的视图页面上，选择要设置为其区域的默认视图的视图旁边的选项按钮。
2. 选择操作，然后选择设为默认视图。

AWS CLI

要设置默认视图

运行以下命令，将指定的视图设置为其区域的默认视图。以下示例将指定视图设置为在 us-east-1 区域中执行的所有搜索的默认视图。该视图必须存在于您运行命令的区域。

```
$ aws resource-explorer-2 associate-default-view \
    --region us-east-1 \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

向视图添加标签

您可以向视图添加标签，以对其进行分类。标签是客户提供的元数据，其形式为键名称字符串和关联的可选值字符串。有关标记 AWS 资源的一般信息，请参阅 Amazon Web Services 一般参考 中的标记 AWS 资源。

在视图中添加标签

您可以通过使用 AWS Management Console 或在 AWS SDK 中运行 AWS CLI 命令或其等效的 API 操作，将标签添加到您的资源管理器视图。

AWS Management Console

要在视图中添加标签

1. 打开资源管理器的视图页面，然后选择要标记的视图的名称以显示其详细信息页面。
2. 在 Tags（标签）下，选择 Manage tags（管理标签）。
3. 要添加标签，选择添加标签，然后输入标签的键名称和可选值。

> **Note**
>
> 您也可以通过选择标签旁边的 X 来删除标签。

您最多可以将 50 个用户定义的标签附加到一个资源中。由 AWS 自动创建和管理的任何标签均不计入此配额。

4. 完成所有标签的更改后，选择保存更改。

AWS CLI

要在视图中添加标签

运行以下命令以向视图添加标签。以下示例向指定视图添加带有键名称 `environment` 和值 `production` 的标签。

```
$ aws resource-explorer-2 tag-resource \
    --resource-id arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --tags environment=production
```

如果成功，前面的命令不会产生任何输出。

> **Note**
>
> 要从视图中移除现有标签，请使用 `untag-resource` 命令。

使用标签控制权限

标签的一个关键用途是支持基于属性的访问权限控制（ABAC）策略。ABAC 允许您标记资源，从而可帮助简化权限管理。然后，您可以向用户授予以某种方式标记的资源的权限。

例如，考虑以下情景。对于名为 `ViewA` 的视图，您可以附加标签 `environment=prod`（键名=值）。另一个 `ViewB` 可能被标记了 `environment=beta`。根据每个角色或用户应该能够访问的环境，您可以使用相同的标签和值来标记您的角色和用户。

然后，您可以为您的 IAM 角色、组和用户分配 AWS Identity and Access Management（IAM）权限策略。只有当提出搜索请求的角色或用户的 `environment` 标签值与附加到视图的 `environment` 标签的值相同时，该策略才会授予使用视图进行访问和搜索的权限。

这种方法的好处在于，它是动态的，不需要您维护谁有权访问哪些资源的列表。相反，您需要确保正确标记所有资源（您的视图）和主体（IAM 角色和用户）。然后，您无需更改任何策略即可自动更新权限。

在 ABAC 策略中引用标签

标记好视图后，您可以选择使用这些标签来动态控制对这些视图的访问。以下示例策略假设您的 IAM 主体和您的视图都使用标签键 environment 和某些值进行标记。完成后，您可以将下列示例策略附加到您的主体。然后，您的角色和用户可以使用任何标有 environment 标签值（与附加到主体的 environment 标签完全匹配）的视图 Search。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:ResourceTag/environment": "${aws:PrincipalTag/environment}"
                }
            }
        }
    ]
}
```

如果主体和视图都有 environment 标签但值不匹配，或者如果其中一个缺少 environment 标签，则资源管理器会拒绝搜索请求。

有关使用 ABAC 安全地授予资源访问权限的更多信息，请参阅什么是 AWS 的 ABAC？

共享资源管理器视图

AWS 资源探索器 中的视图主要使用基于资源的策略来授予访问权限。这些策略与 Amazon S3 存储桶策略类似，将附加到视图并指定谁可以使用该视图。这与 AWS Identity and Access Management（IAM）基于身份的策略形成鲜明对比。基于 IAM 身份的策略被分配给角色、组或用户，

并且它指定角色、组或用户可以访问哪些操作和资源。您可以将任一类型的策略用于资源管理器视图，如下所示：

- 在拥有资源的管理账户或委派管理员账户中，使用任一策略类型来授予访问权限，但前提是没有其他策略明确拒绝该主体访问视图。
- 在不同账户中，您必须同时使用这两种策略类型。附加到共享账户中的视图的基于资源的策略开启了与其他使用账户的共享。但是，该策略不向使用账户中的个人用户或角色授予访问权限。使用账户中的管理员还必须为使用账户中的所需角色和用户分配基于身份的策略。该策略授予对视图的 Amazon 资源名称（ARN）的访问权限。

要与其他账户共享视图，您必须使用 AWS Resource Access Manager（AWS RAM）。AWS RAM 为您处理基于资源的策略的复杂性。在共享之前，您必须遵照以下步骤开启多账户搜索。

要共享视图，您必须为组织的管理账户或委派管理员。您可以指定要与之共享资源的账户或身份。AWS RAM 完全支持资源管理器视图。AWS RAM 根据您选择与之共享的主体的类型，使用与以下各部分中描述的策略相似的策略。有关如何共享资源的说明，请参阅《AWS Resource Access Manager 用户指南》中的共享 AWS 资源。

管理员和委派管理员可以创建和共享 3 种类型的视图：组织范围视图、组织单位（OU）范围视图和账户级范围视图。它们可以与组织、OU 或账户共享。当账户加入或离开组织时，AWS RAM 会自动授予或撤消共享的视图。

与 AWS 账户 共享视图的权限策略

以下示例策略展示了如何在两个不同的 AWS 账户 中向主体提供视图：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [ "111122223333", "444455556666" ]
            },
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            ],
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
```

```
            "Condition": {"StringEquals": {"aws:PrincipalOrgID": "o-123456789012"},
                "StringNotEquals": {"aws:PrincipalAccount": "123456789012"}
            }
        }
    ]
    }"
}
```

每个指定账户中的管理员现在必须通过将基于身份的权限策略附加到角色、组和用户来指定哪些角色和用户可以访问视图。账户 111122223333 或 444455556666 的管理员可以创建下面的示例策略。然后，他们可以将策略分配给这些账户中的角色、组和用户，允许他们使用从原始账户共享的视图进行搜索。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    ]
}
```

您可以将这些基于 IAM 身份的策略用作基于属性的访问权限控制（ABAC）安全策略的一部分。在这种模式中，您要确保您的所有资源和所有身份都被标记。然后，您可以在策略中指定哪些标签键和值必须匹配哪些标签键和值才能允许访问。有关在您的账户中标记视图的信息，请参阅 向视图添加标签。有关基于属性的访问权限控制的更多信息，请参阅《IAM 用户指南》中的什么是 AWS 的 ABAC？和使用标签控制对 AWS 资源的访问权限。

在资源管理器中删除视图

当您不再需要某个 AWS 资源探索器 视图，可以删除它。您可以通过使用 AWS Management Console 或在 AWS SDK 中运行 AWS CLI 命令或其等效的 API 操作来删除视图。

> **Note**
>
> 您无法删除当前被指定为其 AWS 区域 的默认视图的视图。要删除视图，必须将该视图作为默认视图删除。为此，您可以在该区域运行 DisassociateDefaultView API 操作。

最小权限

要运行此过程，您必须具有以下权限：

- 操作：`resource-explorer-2:DeleteView`

  资源：要删除的视图的 ARN

AWS Management Console

要删除视图

1. 在资源管理器控制台的视图页面上，选择要删除的视图旁边的选项按钮。
2. 选择 Actions，然后选择 Delete。
3. 在确认对话框中，键入视图名称，然后选择删除。

AWS CLI

要删除视图

运行以下命令以删除具有指定 Amazon 资源名称（ARN）的视图。

```
$ aws resource-explorer-2 delete-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

使用 AWS 资源探索器 搜索资源

在您的 AWS 账户 中启用 AWS 资源探索器 的主要目的是允许您的用户在账户中搜索资源。使用 AWS Management Console 或 AWS Command Line Interface（AWS CLI）以通过资源管理器搜索资源。

以下是资源管理器搜索的一些主要特征。

- 每次搜索都必须使用视图。

  视图是资源管理器用来确定谁有权查看哪些资源的视图。要在资源管理器搜索操作中使用视图，用户必须对指定视图的 `resource-explorer-2:Search` 操作具有 `Allow`。此权限来自提交请求的主体所附的基于身份的权限策略。

  视图可以包含一个筛选条件，用于限制结果中可以包含哪些资源。通过创建使用筛选条件的不同视图并向不同的主体授予对不同视图的访问权限，您可以配置一个环境，让每组用户只能查看与他们相关的资源。

  有关视图的更多信息，请参阅 管理资源管理器视图以提供搜索访问权限。

- 资源管理器使用异步后台进程来维护其索引。

  资源管理器的索引过程可能需要一些时间才能发现新创建或修改的资源并将其添加到本地索引中。资源管理器可能需要更多时间才能将本地索引中的更改复制到聚合器索引。

  这同样适用于您删除的资源。删除资源后，可能需要一段时间才能让索引过程发现该删除并从本地索引中删除该资源的信息。资源管理器需要更多时间才能将删除的内容从本地索引复制到账户的聚合器索引。

  对于资源的添加、修改和删除，资源管理器最多可能需要 36 小时才能在您已激活资源管理器的所有区域的搜索结果中显示这些更改。

- 资源管理器中的搜索发生在 AWS 区域 中。

  您开启资源管理器的每个区域都仅包含存储在该区域中的资源的索引。视图还与区域相关联，并且只能返回在该区域索引中找到的资源。唯一的例外是聚合器索引，它接收所有本地索引的复制副本，以支持在账户中的所有区域中进行搜索。

- 跨区域搜索需要账户的聚合器索引。

  要让用户跨所有 AWS 区域 搜索资源，管理员必须指定一个区域来包含该账户的聚合器索引。每个本地索引的副本会自动复制到聚合器索引。

因此，只有聚合器索引区域中的视图才能返回包含账户中所有 AWS 区域 的资源的结果。

- 查询由任意数量的自由格式文本关键字和筛选条件组成。

  自由格式关键字使用逻辑 **OR** 运算符组合在查询中。使用资源管理器定义的筛选条件名称的筛选条件使用逻辑 **AND** 运算符组合在查询中。考虑以下示例查询。

  ```
  test instance service:EC2 region:us-west-2
  ```

  资源管理器按如下方式对其进行评估。

  ```
  test OR instance AND service:EC2 AND region:us-west-2
  ```

  此查询要求匹配的资源必须是美国西部（俄勒冈州）区域的 Amazon EC2 资源，并且至少要以某种方式（例如名称、描述或标签）附加一个关键词（测试、实例）。

  > **Note**
  >
  > 由于隐式 AND，您可以成功地对只能有一个与资源关联的值的属性使用一个筛选条件。例如，一个资源只能是一个 AWS 区域 的一部分。因此，以下查询将不返回结果。
  >
  > ```
  > region:us-east-1 region:us-west-1
  > ```
  >
  > 此限制不适用于可以同时拥有多个值的属性的筛选条件，例如 `tag:`、`tag.key:` 和 `tag.value:`。

- 一次搜索只能返回前 1000 个结果。

  此要求包括使用与所有资源匹配的空查询字符串进行搜索。要查看空查询字符串返回的 1000 个以外的资源，您必须使用查询将匹配结果限制为您想要查看的结果，并将匹配数量限制在 1000 以下。

- 对于您可以执行的搜索操作数量，每个账户都有一个配额。

  配额限制了您每秒可以进行的查询次数以及每月可以进行的查询次数。有关具体的配额数量，请参阅资源管理器的配额。

AWS Management Console

要使用资源管理器搜索资源

1. 在资源搜索页面上，首先选择要使用的视图。您只能从您有权访问的视图中进行选择。
2. 在查询中，输入搜索词和筛选条件，以标识您要查看的资源。有关所有可用语法选项的信息，请参阅 资源管理器的搜索查询语法参考。
3. 按 Enter 提交您的查询。

   资源管理器显示同时与视图中定义的 `Filter` 和您提供的查询相匹配的所有结果。结果按相关性排序，匹配更多查询词的资源在列表中显示在较高位置，匹配较少搜索词的资源则显示在列表的后面。
4. 选择资源的标识符以导航到该资源类型的本机控制台，在那里您可以通过该服务支持的所有方式与该资源进行交互。

AWS CLI

要使用资源管理器搜索资源

运行以下命令以使用指定视图搜索资源。该视图必须存在于您运行操作的区域。以下示例搜索在美国东部（俄亥俄州）（us-east-2）标记为 `env=production` 的 Amazon EC2 实例。有关 `query-string` 参数的所有可用语法选项的信息，请参阅 资源管理器的搜索查询语法参考。

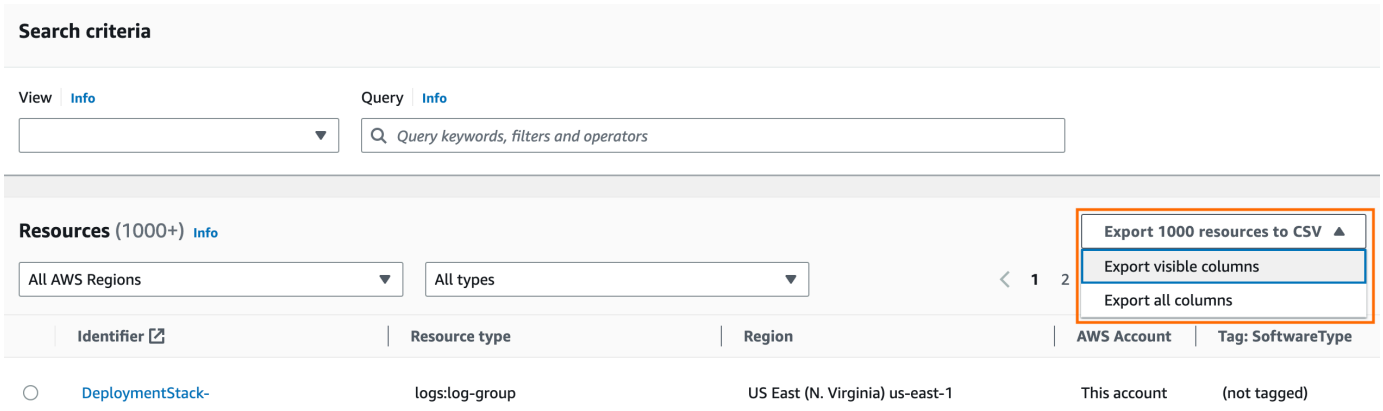
```
$ aws resource-explorer-2 search \
    --region us-east-1 \
    --query-string "resourcetype:AWS::EC2::Instance tag:env=production"
    --view-arn arn:aws:resource-explorer-2:us-east-2:123456789012:view/My-Resources-View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

将搜索结果导出为 .csv 文件

您可以将资源搜索查询结果导出为逗号分隔值（.csv）文件。.csv 文件包括标识符、资源类型、区域、AWS 账户、总标签数以及集合中的每个唯一标签键的列。.csv 文件可以帮助您配置组织中的 AWS 资源，或者确定资源之间的标记重叠或不一致问题。

1. 在资源搜索查询的结果中，选择将资源导出为 CSV。

   您可以选择仅使用当前可以看到的列导出结果，或选择使用所有可用列进行导出。



2. 在浏览器提示您时，选择打开 .csv 文件，或将其保存到方便的位置。

资源管理器的搜索查询语法参考

AWS 资源探索器 可帮助您在自己的 AWS 资源中找到个人资源 AWS 账户。为了帮助您找到所需的确切资源，资源管理器接受支持本主题所述语法的搜索查询字符串。有关演示如何使用此处所述功能的示例查询，请参阅 资源管理器搜索查询示例。

> **Note**
>
> 目前，附加到 AWS Identity and Access Management (IAM) 资源（例如角色或用户）的标签未编制索引。

查询在资源管理器中的工作原理

搜索查询始终使用视图。如果您没有明确指定一个视图，则资源管理器将使用您正在 AWS 区域 使用的默认视图。

视图决定哪些资源可供您查询。您可以创建不同的视图，每个视图都返回一组不同的资源。

例如，您可以创建一个仅包含用键 `Environment` 和值 `Production` 标记的资源的视图。然后，您可以选择仅向有业务理由查看这些资源的用户授予该视图的访问权限。包含 `Alpha` 或 `Beta` 环境资源的单独视图可由需要查看这些资源的不同用户访问。有关控制谁有权访问哪些视图的信息，请参阅 授予对资源管理器视图的访问权限以进行搜索。

查询字符串语法

本部分提供有关查询语法、筛选条件和筛选运算符的基本方面的信息。

基础知识

最基本的是，`QueryString` 是一组由逻辑 **`OR`** 运算符隐式连接的自由格式文本关键字。使用空格将每个关键字与其他关键字分开，如下例所示：

```
ec2 billing test gamma
```

资源管理器评估此关键字列表：

```
ec2 OR billing OR test OR gamma
```

资源管理器按相关性对结果进行排序，优先考虑与更多搜索词匹配的资源。与一个或多个术语不匹配的资源不会排除在结果之外。但是，资源管理器认为它们的相关性较低，并在搜索结果中将其进一步向下推送。

如果您为 QueryString 参数指定一个空字符串，则您的查询通过用于操作的视图返回可用的前 1000 个资源。任何查询可返回的最大资源数为 1000。

> **Note**
>
> AWS 保留更新用于评估自由格式文本关键字的匹配逻辑和相关性算法的权利，以便我们可以为客户提供最相关的结果。因此，使用自由文本关键字的相同查询返回的结果可能会随着时间的推移而发生变化。如果您需要更确切的结果，则建议您使用筛选条件。筛选条件匹配逻辑不会随着时间的推移而改变。

筛选条件

您可以通过添加筛选条件来更严格地限制查询结果。与文本关键字不同的是，筛选条件在查询中使用 AND 运算符进行评估。例如，考虑以下由两个自由格式关键字和两个筛选条件组成的查询：

```
test instance service:EC2 region:us-west-2
```

此查询的估算方式如下：

```
( test OR instance ) AND service:EC2 AND region:us-west-2
```

筛选条件器始终使用 AND 逻辑运算符进行评估。如果某个资源与筛选条件不匹配，则该资源不会包含在结果中。示例查询的结果包括与 Amazon EC2 关联且位于美国西部（俄勒冈州）AWS 区域 且至少以某种方式附加了其中一个关键词的所有资源。

> **Note**
>
> 由于隐式 AND，您可以成功地对只能有一个与资源关联的值的属性使用一个筛选条件。例如，一个资源只能是一个 AWS 区域的一部分。因此，以下查询将不返回结果。
>
> ```
> region:us-east-1 region:us-west-1
> ```

此限制不适用于可以同时拥有多个值的属性的筛选条件，例如 tag:、tag.key: 和 tag.value:。

下表列出了可在资源管理器搜索查询中使用的可用筛选条件名称。

筛选条件名称	说明和示例
accountid:	AWS 账户 拥有资源的。资源管理器在结果中仅包含指定账户所拥有的资源。 accountid:123456789012
application:	此筛选条件使您能够搜索带有 awsApplication 标签键和资源组值的资源。您可以按应用程序名称或应用程序资源组 ARN 进行搜索。 application:MyApplicationName application:arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced **Note** 要使用此筛选条件，您的视图必须有权访问标记数据。
id:	单个资源的标识符，以 Amazon 资源名称（ARN）表示。 id:arn:aws:license-manager: us-east-1 :123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea26EXAMPLE
region:	资源 AWS 区域 所在的位置。资源浏览器仅在结果中包含驻留在指定中的资源 AWS 区域。 region:us-east-1

筛选条件名称	说明和示例
	Note 仅键入区域代码（不带筛选条件，例如 us-east-1 ）不会返回与 region:us-east-1 相同的结果。之所以出现这种结果是因为，作为一个不是筛选条件的自由格式文本关键字，区域代码被分解成不同的部分。例如，以 us、east 和 1 的形式搜索 us-east-1 。当您使用 region: 前缀时，不会对组件进行这种细分。
region:global	region:筛选器的特殊情况，您可以使用它来查找与个人无关 AWS 区域 但被视为全球范围的资源。 region:global **Note** 仅键入关键字 global 不会返回与 region:global 相同的结果，因为字面单词“global”未附加到全局资源。键入 global 作为关键字只会返回那些具有与该资源关联的文字字符串的资源。
resourcetype:	*service*:*type* 表示法中的资源类型。资源管理器在结果中仅包含指定类型的资源。 resourcetype:ec2:instance
resourcetype.supports:	此筛选器使您能够搜索支持标签的资源。 tags是唯一支持的值。资源浏览器仅在结果中包含可标记的资源。 resourcetype.supports:tags
service:	与 AWS 服务 资源类型关联的。资源管理器在结果中仅包含指定服务所创建和管理的资源。 service:ec2

筛选条件名称	说明和示例
`tag:`	表示为 <key>=<value> 的标签键/值对。资源管理器仅在结果中包含具有匹配键和指定值的标签的资源。 `tag:environment=production`
`tag:none`	`tag:` 筛选条件的一种特殊情况，使您能够搜索未附加任何用户创建标签的任何资源。 **Note** 带有 AWS 服务创建标签的资源仍会显示在此筛选条件的结果中。
`tag.key:`	标签键。资源管理器仅在结果中包含具有匹配键（无论值如何）的标签的资源。 `tag.key:environment`
`tag.value:`	标签值。资源管理器仅在结果中包含具有匹配值（无论键名称如何）的标签的资源。 `tag.value:production`

筛选条件运算符

您可以通过将下表所示的运算符之一作为字符串的一部分来修改关键字和筛选条件。

运算符	说明和示例
"multiple word phrase" 或者 *“hyphenated-phrase ”*	用双引号字符（" "）将应视为单个关键字的多字短语括起来。资源管理器仅包含与整个短语匹配、所有单词合在一起且按指定顺序排列的资源。 如果您不使用双引号，资源管理器会通过空格或连字符将短语分解为各组成部分，并包含与各个组成部分匹配的资源，即使它们不在一起或顺序不同。报价应该在操作员之后的所有内容周围。 `"This matches only resources with the whole sentence."`

运算符	说明和示例

	`This matches resources with any of the words.`
	
	`"us-east-1"` – 仅匹配与该确切区域关联的资源。
	
	`us-east-1` – 匹配任何包含“us”、“east”或“1”的资源。
	
	`-tag:"enviornment=production"`

keyword`*`	前缀通配符匹配。您只能在字符串的末尾放置通配符（星号 `*`）。资源管理器仅在结果中包含值在 `*` 前以前缀文本开头的资源。以下示例匹配所有 AWS 区域以开头的内容`us-east`。 `region:us-east*` **Important** 统一搜索会自动在字符串中第一个关键字的末尾插入通配符（`*`）运算符。这意味着统一的搜索结果包括与任何以指定关键字开头的字符串相匹配的资源。 通过查询文本框，在资源管理器控制台的资源搜索页面上执行的搜索，不会自动附加通配符。您可以在搜索字符串中的任何术语后面手动插入 `*`。

运算符	说明和示例

-keyword	Not 运算符。您可以在其关键字或筛选条件的开头放置连字符 (-) ，以反转搜索结果。资源管理器会从结果中排除与该运算符后面的关键字或筛选条件匹配的任何资源。以下示例会将与 Amazon EC2 服务关联的所有资源排除在结果之外。
	
	`-service:ec2`
	
	Important
	如果您使用 AWS CLI `search`命令并且您的`--query-string` 参数值将`-`运算符作为第一个字符，则必须使用等号字符 (=) 而不是通常的空格字符将参数名称与其值分开。如果您使用空格字符，则 CLI 会误解该字符串。例如，下面的查询将失败。
	
	`aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"`
	
	以下经过更正的查询字符串用 = 替换了空格，将按预期工作。
	
	`aws resource-explorer-2 search --query-string="-tag:none region:us-east-1"`
	
	如果您更改查询字符串中筛选条件的顺序，使 - 不作为参数值中的第一个字符，则可以使用标准空格字符。以下查询字符串有效。
	
	`aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"`

运算符	说明和示例
\<*special character*>	您可以对特殊字符进行转义，这些特殊字符必须完全按照显示的内容包含，而不是对其进行解释。如果您的文本包含其中一个特殊字符（ * " - : = \），您必须在该字符前面加上反斜杠（\），以确保该字符是按字面意思理解的。以下示例说明如何使用包含连字符（-）字符（"my-key-word" ）的自由格式文本关键字。 此外，为防止资源管理器将连字符处的表达式分解为三个单独的关键字，可以用双引号将整个短语括起来。 "my\-key\-word" 要插入字面反斜杠，请连续插入两个反斜杠字符。第一个反斜杠被解释为转义符，第二个反斜杠是要插入的字面字符。 "some_text\\some_more_text"

Note

如果视图包含附加到资源的标签，则 Search 操作不会引发搜索字符串的验证错误，因为无效的筛选条件也可能被解释为自由格式的文本搜索。例如，尽管 cat:blue 看起来像一个筛选条件，但资源管理器不能将其解析为筛选条件，因为 cat: 不是有效的已定义筛选条件之一。取而代之的是，资源管理器将整个字符串解释为自由格式的搜索字符串，以允许它匹配标签键名称或 ARN 的一部分等。
如果满足以下任一条件，操作将引发验证错误：

- 该视图不包含有关标签的信息
- 搜索查询明确使用标签筛选条件（tag.key:、tag.value: 或 tag:）

资源管理器搜索查询示例

以下示例显示了可以在 AWS 资源探索器 中使用的常见查询类型的语法。

Important

如果您使用 AWS CLI `search` 命令并且您的 `--query-string` 参数值将 `-` 运算符作为第一个字符，则必须使用等号字符（`=`）而不是通常的空格字符将参数名称与其值分开。如果您使用空格字符，则 CLI 会误解该字符串。例如，下面的查询将失败。

```
aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"
```

以下更正后的查询用 `=` 替换了空格，将按预期运行。

```
aws resource-explorer-2 search --query-string="-tag:none region:us-east-1"
```

如果您更改查询字符串中筛选条件的顺序，使 `-` 不作为参数值中的第一个字符，则可以使用标准空格字符。以下查询有效。

```
aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"
```

搜索未标记的资源

如果您想在账户中使用基于属性的访问权限控制（ABAC）、使用基于成本的分配，或对资源执行基于标签的自动化，则需要知道账户中哪些资源可能缺少标签。以下示例查询使用特殊情况筛选条件标签：无来返回缺少用户生成标签的所有资源。

`tag:none` 筛选条件仅适用于用户创建的标签。由 AWS 生成和维护的标签不受此筛选条件的限制，并且仍会显示在结果中。

```
tag:none
```

要同时排除 AWS 创建的所有系统标签，请按下例所示添加第二个筛选条件。查询字符串中的第一个元素通过筛选掉所有用户创建的标签来复制前面的示例。AWS 创建的系统标签始终以字母 `aws` 开头。因此，您可以将逻辑 NOT 运算符（`-`）与 tag.key 筛选条件一起使用，以排除任何带有密钥名称以 `aws` 开头的标签的资源。

```
tag:none -tag.key:aws*
```

搜索标记的资源

要查找所有带有任何类型标签的资源，您可以如下所示使用逻辑 NOT 运算符（-）和特殊情况标签：无筛选条件。

```
-tag:none
```

搜索缺少特定标签的资源

同样与 ABAC 相关的是，您可能需要搜索所有未带有指定键的标签的资源。以下示例使用逻辑 NOT 运算符 - 返回缺少带有键名称 Department 的标签的所有资源。

```
-tag.key:Department
```

搜索标签值无效的资源

出于合规性考虑，您可能希望搜索所有在重要标签上缺少标签值或存在拼写错误的资源。以下示例返回所有带有键名称为 environment 的标签的资源。但是，该查询会筛选出任何有效值为 prod、integ 或 dev 的资源。此查询中出现的任何结果都有其他一些值，您应该对它们进行调查并更正。

> **Important**
>
> 资源管理器搜索不区分大小写，也无法区分键名称和仅因大小写方式而不同的值。例如，以下示例中的值与 PROD、prod、PrOd 或任何变体匹配。但是，有些应用程序以区分大小写的方式使用标签。建议您对组织的大小写策略进行标准化，例如仅使用小写的标签键名称和值。一致的方法可以帮助避免由于标签的大小写不同而引起的混淆。

```
tag.key:environment -tag:environment=prod -tag:environment=integ -tag:environment=dev
```

在 AWS 区域 的子集中搜索资源

使用 '*' 通配符运算符匹配世界上某个地区的所有区域。以下示例返回位于欧洲（EU）区域的所有资源。

```
region:eu-*
```

搜索全局资源

使用 `region:` 筛选条件的特殊情况 `global` 值来查找被认为是全局性且与单个区域无关的资源。

```
region:global
```

搜索位于特定区域的特定类型的资源

使用多个筛选条件时，资源管理器通过将前缀与隐式逻辑 AND 运算符组合来计算表达式。以下示例返回亚太地区（香港）区域中且 AND 均为 Amazon EC2 实例的所有资源。

```
region:ap-east-1 resourcetype:ec2:instance
```

> **Note**
>
> 由于隐式 AND，您可以成功地对只能有一个与资源关联的值的属性使用一个筛选条件。例如，一个资源只能是一个 AWS 区域 的一部分。因此，以下查询将不返回结果。
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> 此限制不适用于可以同时拥有多个值的属性的筛选条件，例如 `tag:`、`tag.key:` 和 `tag.value:`。

搜索包含多词术语的资源

用双引号（`"`）将多词术语括起来，以仅返回整个术语按指定顺序排列的结果。如果不使用双引号，资源管理器将返回与构成该术语的任何单个单词相匹配的资源。例如，以下查询使用双引号仅返回与术语 `"west wing"` 匹配的资源。该查询不匹配 `us-west-2` AWS 区域（或其代码中包含 `west` 的任何其他区域）中的资源或与“wing”一词匹配但没有“west”一词的资源。

```
"west wing"
```

搜索作为指定 CloudFormation 堆栈一部分的资源

当您创建资源作为 AWS CloudFormation 堆栈的一部分时，它们都会自动用堆栈的名称进行标记。以下示例返回作为指定堆栈的一部分创建的所有资源。

```
tag:aws:cloudformation:stack-name=my-stack-name
```

在 AWS Management Console 中使用统一搜索

AWS Management Console 在每个 AWS 控制台页面的顶部都有一个搜索栏。此搜索栏可用于搜索 AWS 服务 文档和博客主题，并将您直接带到 AWS 服务控制台页面。如果您通过打开所需的资源管理器功能来开启统一搜索功能，它还可以返回您的 AWS 账户 中的资源。

通过统一搜索，您的用户可以从任何 AWS 服务 控制台搜索资源，而无需先导航到 AWS 资源探索器控制台。

> **Tip**
>
> 如果要使用统一搜索栏专门搜索资源，请通过键入 **`/Resources`** 开始搜索查询。这会导致 AWS 资源在搜索结果中的排名高于不代表资源的结果。

主题

> **Important**
>
> 统一搜索会自动在字符串中第一个关键字的末尾插入通配符（*）运算符。这意味着统一的搜索结果包括与任何以指定关键字开头的字符串相匹配的资源。
> 通过查询文本框，在资源管理器控制台的资源搜索页面上执行的搜索，不会自动附加通配符。您可以在搜索字符串中的任何术语后面手动插入 *。

检查是否启用了统一搜索

要查看您的 AWS 账户 中是否启用了统一搜索，请查看设置页面的顶部。资源管理器会在其中显示每个要求的当前状态。统一搜索的要求如下：

- 您必须至少在一个 AWS 区域 中开启资源管理器。只有具有资源管理器索引的区域中的资源才能显示在统一搜索结果中。
- 您必须在您选择的区域中创建聚合器索引。在该区域执行的搜索会返回账户中所有注册区域的结果。

- 您必须在包含聚合器索引的区域中创建默认视图。所有需要使用统一搜索来搜索资源的用户都必须拥有使用此默认视图的权限。
- 必须为用户的 IAM 主体分配一个 AWS Identity and Access Management（IAM）权限策略，该策略授予执行 `resource-explorer-2:Get*`、`resource-explorer-2:List*`、`resource-explorer-2:Describe*`、`resource-explorer-2:Search` 操作的权限。您可以使用自己的自定义 IAM policy 授予这些权限。这些权限已包含在以下可供您使用的 AWS 托管策略中：
  - AWSResourceExplorerReadOnlyAccess
  - AWSResourceExplorerFullAccess

开启统一搜索

要允许在搜索结果中包含您账户的资源，以便在任何 AWS 控制台中进行统一搜索，您必须完成以下步骤：

1. 在您的账户中在一个或多个 AWS 区域 激活 AWS 资源探索器。
2. 注册一个区域以包含聚合器索引。
3. 在包含聚合器索引的区域中创建一个默认视图。

使用 AWS Chatbot 搜索资源

通过询问 AWS Chatbot 自然语言问题，您可以搜索和发现有关 AWS 服务 和您的 AWS 资源的信息。AWS Chatbot 使用相关 AWS 文档和支持文章摘录，直接在聊天通道中回答与服务相关的问题。AWS Chatbot 使用资源管理器搜索和查找与资源相关的问题的答案。

有关更多信息，请参阅《AWS Chatbot 管理员指南》中的什么是 AWS Chatbot？。

AWS 资源问题

AWS Chatbot 使用资源管理器搜索和发现您的资源。AWS Chatbot 在列表中显示这些搜索结果。此列表显示了排名前五的匹配资源，并包括按资源类型、AWS 区域 和标签进一步筛选结果的功能。

先决条件

要询问与 AWS Chatbot 资源相关的问题，您必须：

- 确保您具有处于活动状态的索引，且具有在 AWS 区域 中至少有一个默认视图的视图。索引和视图使资源管理器能够对您的资源进行分类和查询。请参阅资源管理器的术语和概念了解更多信息。
- 根据频道的权限方案，将 AWSResourceExplorerReadOnlyAccess 策略添加到您的频道角色或每个相应的用户角色中。
- 验证您的频道护栏政策是否允许 AWSResourceExplorerReadOnlyAccess 权限。

常见资源问题

您可以直接在聊天通道中询问这些问题。将红色文本单词替换为您自己的信息。

```
@aws What services am I using in Region?

@aws What are the resources in my account with tags?

@aws What lambda functions do I have?
```

AWS 资源探索器 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 Cloud 中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。第三方审核员定期测试和验证我们的安全性的有效性，作为 AWS 合规性计划的一部分。要了解适用于资源管理器的合规性计划，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。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 AWS 资源探索器 时应用责任共担模式。它说明了如何配置资源管理器以实现您的安全性和合规性目标。您还将了解如何使用其他 AWS 服务 以帮助您监控和保护资源管理器资源。

目录

适用于 AWS 资源探索器 的身份和访问管理

AWS Identity and Access Management (IAM) 是一项 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制可以通过身份验证（登录）和授权（具有权限）使用资源管理器资源的人员。IAM 是一项无需额外费用即可使用的 AWS 服务。

主题

- 资源管理器如何与 IAM 结合使用
- AWS 资源探索器 基于身份的策略示例
- AWS Organizations 和资源浏览器的服务控制策略示例
- AWS 的托管策略 AWS 资源探索器
- 为资源管理器使用服务相关角色
- 排除 AWS 资源探索器 权限故障

受众

使用 AWS Identity and Access Management（IAM）的方式因您可以在资源管理器中执行的操作而异。

服务用户 – 如果使用资源管理器服务来完成任务，则您的管理员会为您提供所需的凭证和权限。当您使用更多资源管理器功能来完成工作时，则可能需要额外权限。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。如果您无法访问资源管理器中的功能，请参阅 排除 AWS 资源探索器 权限故障。

服务管理员 – 如果您在公司负责管理资源管理器资源，您可能具有资源管理器资源的完全访问权限。您有责任确定您的服务用户应访问哪些资源管理器功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与资源管理器搭配使用的更多信息，请参阅 资源管理器如何与 IAM 结合使用。

IAM 管理员 – 如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对资源管理器的访问权限的详细信息。要查看您可在 IAM 中使用的资源管理器基于身份的策略示例，请参阅 AWS 资源探索器 基于身份的策略示例。

使用身份进行身份验证

身份验证是使用身份凭证登录 AWS 的方法。您必须作为 AWS 账户根用户、IAM 用户或通过担任 IAM 角色进行身份验证（登录到 AWS）。

您可以使用通过身份源提供的凭证以联合身份登录到 AWS。AWS IAM Identity Center(IAM Identity Center) 用户、您公司的单点登录身份验证以及您的 Google 或 Facebook 凭证都是联合身份的示例。当您以联合身份登录时，管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合身份验证访问 AWS 时，您就是在间接担任角色。

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

如果您以编程方式访问 AWS，则 AWS 将提供软件开发工具包 (SDK) 和命令行界面 (CLI)，以便使用您的凭证以加密方式签署您的请求。如果您不使用 AWS 工具，则必须自行对请求签名。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的签署 AWS API 请求。

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

AWS 账户 根用户

创建 AWS 账户 时，最初使用的是一个对账户中所有 AWS 服务 和资源拥有完全访问权限的登录身份。此身份称为 AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

用户和组

IAM 用户是 AWS 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用群组的身份登录。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，使用群组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

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担任。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

角色

IAM 角色是 AWS 账户 中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过切换角色，在 AWS Management Console 中暂时担任 IAM 角色。您可以调用 AWS CLI 或 AWS API 操作或使用自定义网址以代入角色。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。

具有临时凭证的 IAM 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。为控制身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户或角色可代入 IAM 角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户存取权限的主要方式。但是，对于某些 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座席）。要了解用于跨账户存取的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 - 某些 AWS 服务使用其他 AWS 服务中的特征。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 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：当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。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 使用主体调用 AWS 服务 的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的政策详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而担任的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务 委派权限的角色。
  - 服务相关角色 - 服务相关角色是与 AWS 服务关联的一种服务角色。服务可以担任代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 - 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 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 IAM 用户，请参阅《IAM 用户指南》中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您将创建策略并将其附加到 AWS 身份或资源，以控制 AWS 中的访问。策略是 AWS 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，AWS 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 AWS 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。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，管理员可以向角色添加 IAM 策略，并且用户可以担任角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从 AWS Management Console、AWS CLI 或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户群组或角色）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 policy。

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、群组或角色中。托管策略是可以附加到AWS 账户中的多个用户、组和角色的独立策略。托管式策略包括 AWS 托管式策略和客户管理型策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 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。主体可以包括账户、用户、角色、联合用户或 AWS 服务。

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

AWS 资源探索器 不支持基于资源的策略。

访问控制列表 (ACL)

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

Amazon S3、AWS WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表 (ACL) 概览。

AWS 资源探索器 不支 ACL。

其他策略类型

AWS 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型授予的最大权限。

- 权限边界 - 权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可以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 (SCP) – SCP 是 JSON 策略，指定了组织或组织单位 (OU) 在 AWS Organizations 中的最大权限。AWS Organizations 服务可以分组和集中管理您的企业拥有的多个 AWS 账户 账户。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体（包括每个 AWS 账户根用户）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略 - 会话策略是当您以编程方式为角色或联合身份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 AWS 如何确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测逻辑。

资源管理器如何与 IAM 结合使用

在使用 IAM 管理对 AWS 资源探索器 的访问权限之前，您应了解哪些 IAM 功能可与资源管理器结合使用。要大致了解资源管理器和其他 AWS 服务 如何与 IAM 一起使用，请参阅《IAM 用户指南》中的与 IAM 一起使用的 AWS 服务。

主题

与其他 AWS 服务 一样，资源管理器需要权限才能使用其操作与您的资源进行交互。要进行搜索，用户必须有权检索视图的详细信息，并且还有权使用视图进行搜索。要创建索引或视图，或者修改它们或任何其他资源管理器设置，您必须具有其他权限。

分配 IAM 基于身份的策略，向相应的 IAM 主体授予这些权限。资源管理器提供了多个托管策略，用于预定义常用权限集。您可以将它们分配给您的 IAM 主体。

资源管理器基于身份的器策略

通过使用 IAM 基于身份的策略，您可以指定特定资源的允许或拒绝的操作和资源，以及指定允许或拒绝这些操作的条件。资源管理器支持特定的操作、资源和条件键。要了解您在 JSON 策略中使用的所有元素，请参阅 IAM 用户指南中的 IAM JSON 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内容。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 策略的 `Action` 元素描述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。有一些例外情况，例如没有匹配 API 操作的仅限权限 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相关操作的权限。

资源管理器中的策略操作在操作前使用 `resource-explorer-2` 前缀。例如，要授予某人使用视图进行搜索的权限，使用资源管理器 `Search` API 操作，将 `resource-explorer-2:Search` 操作包含在分配该主体的策略中。策略语句必须包含 `Action` 或 `NotAction` 元素。资源管理器定义了一组自己的操作，以描述您可以使用该服务执行的任务。这些操作与资源管理器 API 操作一致。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下例所示。

```
"Action": [
      "resource-explorer-2:action1",
      "resource-explorer-2:action2"
```

```
]
```

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

```
"Action": "resource-explorer-2:Describe*"
```

要查看资源管理器操作的列表，请参阅《AWS 服务授权参考》中的 AWS 资源探索器 定义的操作。

资源

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。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 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 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": "*"
```

视图

资源管理器的主要资源类型是视图。

资源管理器视图资源采用以下 ARN 格式。

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${unique-id}
```

资源管理器的 ARN 格式显示在以下示例中。

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-Search-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> 视图的 ARN 末尾包含一个唯一标识符，用于确保每个视图都是唯一的。这有助于确保授予对已删除的旧视图的访问权限的 IAM policy 不会被意外授予对恰好与旧视图同名的新视图的访问权限。每个新视图最后都会收到一个新的、唯一的 ID，用于确保 ARN 永远不会被重复使用。

有关 ARN 格式的更多信息，请参阅 Amazon Resource Name (ARN)。

您可以使用分配给 IAM 主体的 IAM 基于身份的策略，并将视图指定为 Resource。这样做可以让您通过一个视图向一组主体授予搜索权限，并通过完全不同的视图向另一组主体授予访问权限。

例如，要向 IAM policy 中名为 ProductionResourcesView 的单个视图授予权限，请先获取该视图的 Amazon 资源名称（ARN）。您可以使用控制台中的视图页面查看视图的详细信息，也可以调用 ListViews 操作来检索您想要的视图的完整 ARN。然后，将其包含在策略声明中，如以下示例所示，以授予仅修改一个视图定义的权限。

```
"Effect": "Allow",
"Action": "UpdateView",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
ProductionResourcesView/<unique-id>"
```

要允许对属于特定账户的所有视图执行操作，请在 ARN 的相关部分中使用通配符（*）。以下示例向指定 AWS 区域 和账户中的所有视图授予搜索权限。

```
"Effect": "Allow",
"Action": "Search",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*"
```

某些资源管理器操作（例如 CreateView）不是针对特定资源执行的，因为如以下示例所示，该资源尚不存在。在这些情况下，您必须对整个资源 ARN 使用通配符（*）。

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "*"
```

如果指定以通配符结尾的路径，则可以将 CreateView 操作限制为仅使用已批准的路径创建视图。以下策略示例展示了如何允许主体仅在路径 view/ProductionViews/ 中创建视图。

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/ProductionViews/*""
```

索引

您可以用来控制对资源管理器功能的访问权限的另一种资源类型是索引。

与索引交互的主要方式是通过在该区域中创建索引在 AWS 区域 中开启资源管理器。之后，您可以通过与视图交互来完成几乎所有其他操作。

您可以用索引执行的一项操作是控制谁可以在每个区域中创建视图。

> **Note**
>
> 创建视图后，IAM 仅授权针对视图的 ARN 而不是索引执行所有其他视图操作。

索引有一个 ARN，您可以在权限策略中引用它。资源管理器索引 ARN 的格式如下。

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${unique-id}
```

参见以下资源管理器索引 ARN 示例。

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222
```

某些资源管理器操作会针对多种资源类型检查身份验证。例如，CreateView 操作对索引的 ARN 和视图的 ARN 进行授权，就像在资源管理器创建视图后一样。要授予管理员管理资源管理器服务的权限，您可以使用 `"Resource": "*"` 授权对任何资源、索引或视图执行操作。

或者，您可以将主体限制为只能使用指定的资源管理器资源。例如，要将操作仅限于指定区域中的资源管理器资源，您可以包括一个与索引和视图都匹配但仅调用单个区域的 ARN 模板。在以下示例中，ARN 仅在指定账户的 `us-west-2` 区域中匹配索引或视图。在 ARN 的第三个字段中指定区域，但在最后一个字段中使用通配符（`*`）来匹配任何资源类型。

```
"Resource": "arn:aws:resource-explorer-2:us-west-2:123456789012:*
```

有关更多信息，请参阅《AWS 服务授权参考》中的 AWS 资源探索器 定义的资源。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 AWS 资源探索器 定义的操作。

条件键

资源管理器不提供任何特定于服务的条件键，但支持使用某些全局条件键。要查看所有 AWS 全局条件键，请参阅《IAM 用户指南》中的 AWS 全局条件上下文键。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。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 AWS 使用逻辑 OR 运算来评估条件。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，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM policy 元素：变量和标签。

AWS支持全局条件键和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅《IAM 用户指南》中的 AWS 全局条件上下文键。

要查看可在资源管理器中使用的条件键的列表，请参阅《AWS 服务授权参考》中 AWS 资源探索器 的条件键。要了解您可以对哪些操作和资源使用条件键，请参阅 AWS 资源探索器 定义的操作。

示例

要查看资源管理器基于身份的策略示例，请参阅 AWS 资源探索器 基于身份的策略示例。

根据资源管理器标签进行授权

您可以将标签附加到资源管理器视图中，或将请求中的标签传递到资源管理器。要基于标签控制访问，您需要使用 `resource-explorer-2: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。有关标记资源管理器资源的更多信息，请参阅 向视图添加标签。有关在资源管理器中使用基于标签的授权，请参阅 使用基于标签的授权来控制对视图的访问权限。

资源管理器的 IAM 角色

IAM 角色是您的 AWS 账户 中具有特定权限的主体。

将临时凭证用于资源管理器

您可以使用临时凭证进行联合身份登录，担任 IAM 角色或担任跨账户角色。您可以调用 AWS Security Token Service (AWS STS) API 操作（如 AssumeRole 或 GetFederationToken）以获得临时安全凭证。

资源管理器支持使用临时凭证。

服务相关角色

服务相关角色允许 AWS 服务访问其它服务中的资源以代表您完成操作。服务相关角色显示在您的 IAM 账户中，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。

资源管理器使用服务相关角色来执行其工作。有关资源管理器服务相关角色的详细信息，请参阅 为资源管理器使用服务相关角色。

AWS 资源探索器 基于身份的策略示例

默认情况下，AWS Identity and Access Management（IAM）主体，例如角色、组和用户，没有创建或修改资源管理器资源的权限。它们还无法使用 AWS Management Console、AWS Command Line Interface（AWS CLI）或 AWS API 执行任务。IAM 管理员必须创建 IAM policy，以便为主体授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略分配给需要这些权限的 IAM 主体。

要提供访问权限，请为您的用户、组或角色添加权限：

- AWS IAM Identity Center 中的用户和组：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中 创建权限集 的说明进行操作。
- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

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
- 使用资源管理器控制台
- 根据标签授予对视图的访问权限
- 授予根据标签创建视图的访问权限

- 允许主体查看他们自己的权限

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资源管理器资源。这些操作可能会使 AWS 账户 产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- AWS 托管策略及转向最低权限许可入门 - 要开始向用户和工作负载授予权限，请使用 AWS 托管策略来为许多常见使用场景授予权限。您可以在 AWS 账户 中找到这些策略。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。

使用资源管理器控制台

对于要在 AWS 资源探索器 控制台中搜索的主体，他们必须具有一组最低的权限。如果没有创建具有所需的最低权限的基于身份的策略，对于账户中的主体，资源管理器控制台将无法按预期正常运行。

您可以使用名为 `AWSResourceExplorerReadOnlyAccess` 的 AWS 托管策略来授予使用资源管理器控制台通过账户中的任何视图进行搜索的权限。要授予仅使用单个视图进行搜索的权限，请参阅 授予对资源管理器视图的访问权限以进行搜索 和以下两个部分中的示例。

对于仅调用 AWS CLI 或 AWS API 的主体，您不需要允许最低控制台权限。相反，您可以选择仅授予与主体需要执行的 API 操作相匹配的操作的访问权限。

根据标签授予对视图的访问权限

在本示例中，您希望向账户中的主体授予对 AWS 账户 中的资源管理器视图的访问权限。为此，您需要将基于 IAM 身份的策略分配给您希望能够在资源管理器中搜索的主体。以下示例 IAM policy 授予对任何请求的访问权限，其中附加到调用主体的 `Search-Group` 标签与请求中使用的视图所附加的相同标签的值完全匹配。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:*:*:view/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Search-Group": "${aws:PrincipalTag/
Search-Group}"}
            }
        }
    ]
}
```

您可以将该策略分配给您账户中的 IAM 主体。如果带有标签 `Search-Group=A` 的主体尝试使用资源管理器视图进行搜索，则还必须对该视图添加标签 `Search-Group=A`。如果不是，则主体将被拒绝访问。条件标签键 `Search-Group` 匹配 `Search-group` 和 `search-group`，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。

> **Important**
>
> 要在 AWS Management Console 的统一搜索结果中查看您的资源，主体必须同时拥有包含聚合器索引的 AWS 区域 中的默认视图的 `GetView` 和 `Search` 权限。授予这些权限的最简单方法是保留使用快速或高级设置开启资源管理器时附加到视图的默认的基于资源的权限。
> 对于这种情况，您可以考虑将默认视图设置为筛选出敏感资源，然后设置向其授予基于标签的访问权限的其他视图，如上例所述。

授予根据标签创建视图的访问权限

在此示例中，您希望仅允许标记为与索引相同的主体能够在包含索引的 AWS 区域 中创建视图。为此，请创建基于身份的权限以允许主体使用视图进行搜索。

现在您已经准备好授予创建视图的权限。您可以将此示例中的语句添加到用于向相应主体授予 Search 权限的相同权限策略中。根据调用视图要关联的操作和索引的主体所附加的标签，允许或拒绝这些操作。当附加到调用方主体的 Allow-Create-View 标签的值与创建视图的区域中附加到索引的同一个标签的值不完全匹配时，以下示例 IAM policy 拒绝任何创建视图的请求。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "resource-explorer-2:CreateView",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {"aws:ResourceTag/Allow-Create-View":
 "${aws:PrincipalTag/Allow-Create-View}"}
            }
        }
    ]
}
```

允许主体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": "*"
        }
    ]
}
```

AWS Organizations 和资源浏览器的服务控制策略示例

AWS 资源探索器 支持服务控制策略 (SCP)。SCP 是您附加到组织中元素的策略，用于对该组织内的权限进行管理。SCP 适用于组织 AWS 账户 中您附加 SCP 的元素下的所有人。SCP 为您组织中的所有账户提供对最大可用权限的集中控制。它们可以帮助您确保 AWS 账户 遵守组织的访问控制准则。有关更多信息，请参阅 AWS Organizations 用户指南中的服务控制策略。

先决条件

要使用 SCP，您必须先执行以下操作：

- 启用组织中的所有功能。有关更多信息，请参阅《AWS Organizations 用户指南》中的启用企业中的所有功能。
- 启用 SCP 以在您的组织内使用。有关更多信息，请参阅《AWS Organizations 用户指南》中的启用和禁用策略类型。
- 创建您需要的 SCP。有关创建 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的创建和更新 SCP。

示例服务控制策略

以下示例说明如何使用基于属性的访问权限控制（ABAC）来控制对资源管理器管理操作的访问权限。除非对提出请求的 IAM 主体进行了 ResourceExplorerAdmin=TRUE 标记，否则此示例策略拒绝访问除搜索所需的两个权限 resource-explorer-2:Search 和 resource-explorer-2:GetView 之外的所有资源管理器操作。有关在资源管理器中使用 ABAC 的更完整讨论，请参阅 使用基于标签的授权来控制对视图的访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView""
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
          "StringNotEqualsIgnoreCase": {"aws:PrincipalTag/ResourceExplorerAdmin":
 "TRUE"}
      }
    ]
}
```

AWS 的托管策略 AWS 资源探索器

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管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 托管策略可能不会为您的特定用例授予最低权限权限，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 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

包含资源浏览器权限的常规 AWS 托管策略

- AdministratorAccess— 授予对 AWS 服务 和资源的完全访问权限。
- ReadOnly访问权限-授予对 AWS 服务 和资源的只读访问权限。
- ViewOnly访问权限-授予查看其资源和基本元数据的权限 AWS 服务。

> **Note**
>
> `ViewOnlyAccess` 策略中包含的资源管理器 `Get*` 权限的执行方式与 `List` 权限类似，尽管它们只返回一个值，原因是一个区域只能包含一个索引和一个默认视图。

AWS 资源浏览器的托管策略

- AWSResourceExplorerFullAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy

AWS 托管策略： AWSResourceExplorerFullAccess

您可以将 `AWSResourceExplorerFullAccess` 策略分配到 IAM 身份。

此策略授予允许完全管理控制资源管理器服务的权限。您可以在账户中的 AWS 区域 中执行开启和管理资源管理器所涉及的所有任务。

权限详细信息

此策略包括允许对资源管理器执行所有操作的权限，包括在中打开和关闭资源管理器 AWS 区域、为帐户创建或删除聚合器索引、创建、更新和删除视图以及搜索。此策略还包括不属于资源管理器的权限：

- ec2:DescribeRegions – 允许资源管理器访问有关您账户中的区域的详细信息。
- ram:ListResources – 允许资源管理器列出资源所属的资源共享。
- ram:GetResourceShares – 允许资源管理器识别有关您拥有或与您共享的资源共享的详细信息。
- iam:CreateServiceLinkedRole – 允许资源管理器在您通过创建第一个索引打开资源管理器时创建所需的服务相关角色。
- organizations:DescribeOrganization – 允许资源管理器访问有关您的组织的信息。

要查看此 AWS 托管策略的最新版本，请参阅AWSResourceExplorerFullAccess《AWS 托管策略参考指南》。

AWS 托管策略： AWSResourceExplorerReadOnlyAccess

您可以将 AWSResourceExplorerReadOnlyAccess 策略分配到 IAM 身份。

此策略授予只读权限，从而授予用户基本搜索权限，以发现其资源。

权限详细信息

此策略包括允许用户执行资源管理器 Get*、List* 和 Search 操作的权限，以查看有关资源管理器组件和配置设置的信息，但不允许用户对其进行更改。用户也可以进行搜索。此策略还包括不属于资源管理器的两个权限：

- ec2:DescribeRegions – 允许资源管理器访问有关您账户中的区域的详细信息。
- ram:ListResources – 允许资源管理器列出资源所属的资源共享。
- ram:GetResourceShares – 允许资源管理器识别有关您拥有或与您共享的资源共享的详细信息。
- organizations:DescribeOrganization – 允许资源管理器访问有关您的组织的信息。

要查看此 AWS 托管策略的最新版本，请参阅AWSResourceExplorerReadOnlyAccess《AWS 托管策略参考指南》。

AWS 托管策略： AWSResourceExplorerServiceRolePolicy

您不能自行将 AWSResourceExplorerServiceRolePolicy 附加到任何 IAM 实体。此策略只能附加到服务相关角色，以允许资源管理器代表您执行操作。有关更多信息，请参阅 为资源管理器使用服务相关角色。

此策略授予资源管理器检索有关您的资源的信息所需的权限。资源浏览器会在您注册的每个索引中填充它所维护 AWS 区域 的索引。

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

AWS 托管策略： AWSResourceExplorerOrganizationsAccess

您可以将 AWSResourceExplorerOrganizationsAccess 分配到 IAM 身份。

此策略向资源管理器授予管理权限，并向其他人授予只读权限 AWS 服务 以支持此访问权限。 AWS Organizations 管理员需要这些权限才能在控制台中设置和管理多账户搜索。

权限详细信息

此策略包括允许管理员为组织设置多账户搜索的权限：

- ec2:DescribeRegions – 允许资源管理器访问有关您账户中的区域的详细信息。
- ram:ListResources – 允许资源管理器列出资源所属的资源共享。
- ram:GetResourceShares – 允许资源管理器识别有关您拥有或与您共享的资源共享的详细信息。
- organizations:ListAccounts – 允许资源管理器识别组织内的账户。
- organizations:ListRoots – 允许资源管理器识别组织内的根账户。
- organizations:ListOrganizationalUnitsForParent – 允许资源管理器识别父级组织单位或根组织中的组织单位（OU）。
- organizations:ListAccountsForParent – 允许资源管理器识别组织中包含于指定目标根或 OU 之中的账户。
- organizations:ListDelegatedAdministrators— 允许资源浏览器识别此组织中指定为委派管理员的 AWS 帐户。
- organizations:ListAWSServiceAccessForOrganization— 允许资源浏览器识别支持与您的组织集成的列表。 AWS 服务
- organizations:DescribeOrganization – 允许资源管理器检索有关用户账户所属组织的信息。
- organizations:EnableAWSServiceAccess— 允许资源浏览器启用 AWS 服务 （由指定的服务ServicePrincipal）与的集成 AWS Organizations。
- organizations:DisableAWSServiceAccess— 允许资源浏览器禁用 AWS 服务 （由指定的服务 ServicePrincipal）与的集成 AWS Organizations。

- organizations:RegisterDelegatedAdministrator— 允许资源浏览器使指定的成员帐户能够管理指定 AWS 服务的组织功能。
- organizations:DeregisterDelegatedAdministrator— 允许资源浏览器删除指定成员 AWS 账户 作为指定成员的委托管理员 AWS 服务。
- iam:GetRole – 运行资源管理器检索有关指定角色的信息，包括角色的路径、GUID、ARN 以及授权代入角色的角色信任策略。
- iam:CreateServiceLinkedRole – 允许资源管理器在您通过创建第一个索引打开资源管理器时创建所需的服务相关角色。

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

资源浏览器对 AWS 托管策略的更新

查看自该服务开始跟踪资源 AWS 管理器托管策略变更以来这些更新的详细信息。有关此页面更改的自动提醒，请在资源管理器文档历史记录页面上订阅 RSS 源。

更改	描述	日期
AWSResourceExplorerServiceRolePolicy-更新了策略权限以查看其他资源类型	资源管理器为服务相关角色策略添加了权限 AWSResourceExplorerServiceRolePolicy，该策略允许资源浏览器查看其他资源类型： • apprunner:ListVpcConnectors • backup:ListReportPlans • emr-serverless:ListApplications • events:ListEventBuses • geo:ListPlaceIndexes • geo:ListTrackers	2023 年 12 月 12 日

更改	描述	日期
	• greengrass:ListComponents • greengrass:ListComponentVersions • iot:ListRoleAliases • iottwinmaker:ListComponentTypes • iottwinmaker:ListEntities • iottwinmaker:ListScenes • kafka:ListConfigurations • kms:ListKeys • kinesisanalytics:ListApplications • lex:ListBots • lex:ListBotAliases • mediapackage-vod:ListPackagingConfigurations • mediapackage-vod:ListPackagingGroups • mq:ListBrokers • personalize:ListDatasetGroups • personalize:ListDatasets • personalize:ListSchemas	

更改	描述	日期
	• route53:ListHealthChecks • route53:ListHostedZones • secretsmanager:ListSecrets	
新 托管式策略	资源浏览器添加了以下 AWS 托管策略： • AWSResourceExplorerOrganizationsAccess	2023 年 11 月 14 日
更新了 托管策略	资源管理器更新了以下 AWS 托管策略以支持多账户搜索： • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess	2023 年 11 月 14 日

更改	描述	日期
AWSResourceExplorerServiceRolePolicy— 更新了支持通过 Organizations 进行多账户搜索的政策	资源管理器为服务相关角色策略 AWSResourceExplorerServiceRolePolicy 添加了权限，该策略允许资源管理器支持使用 Organizations 进行多账户搜索： • organizations:ListAWSServiceAccessForOrganization • organizations:DescribeAccount • organizations:DescribeOrganization • organizations:ListAccounts • organizations:ListDelegatedAdministrators	2023 年 11 月 14 日

更改	描述	日期
AWSResourceExplorerServiceRolePolicy— 更新了政策以支持其他资源类型	资源管理器为服务相关角色策略 AWSResourceExplorerServiceRolePolicy 添加了权限，该策略允许服务为以下资源类型编制索引： • accessanalyzer:analyzer • acmpca:certificateauthority • amplify:app • amplify:backendenvironment • amplify:branch • amplify:domainassociation • amplifyuibuilder:component • amplifyuibuilder:theme • appintegrations:eventintegration • apprunner:service • appstream:appblock • appstream:application • appstream:fleet • appstream:imagebuilder • appstream:stack • appsync:graphqlapi • aps:rulegroupsnamespace • aps:workspace • apigateway:restapi • apigateway:deployment • athena:datacatalog • athena:workgroup	2023 年 10 月 17 日

更改	描述	日期
	• autoscaling:autoscalinggroup • backup:backupplan • batch:computeenvironment • batch:jobqueue • batch:schedulingpolicy • cloudformation:stack • cloudformation:stackset • cloudfront:fieldlevelencryptionconfig • cloudfront:fieldlevelencryptionprofile • cloudfront:originaccesscontrol • cloudtrail:trail • codeartifact:domain • codeartifact:repository • codecommit:repository • codeguruprofiler:profilinggroup • codestarconnections:connection • databrew:dataset • databrew:recipe • databrew:ruleset • detective:graph • directoryservices:directory • ec2:carriergateway • ec2:verifiedaccessendpoint • ec2:verifiedaccessgroup	

更改	描述	日期
	• ec2:verifiedaccessinstance • ec2:verifiedaccesstrustprovider • ecr:repository • elasticache:cachesecuritygroup • elasticfilesystem:accesspoint • events:rule • evidently:experiment • evidently:feature • evidently:launch • evidently:project • finspace:environment • firehose:deliverystream • faultinjectionsimulator:experimenttemplate • forecast:datasetgroup • forecast:dataset • frauddetector:detector • frauddetector:entitytype • frauddetector:eventtype • frauddetector:label • frauddetector:outcome • frauddetector:variable • gamelift:alias • globalaccelerator:accelerator • globalaccelerator:endpointgroup	

更改	描述	日期
	• globalaccelerator:listener • glue:database • glue:job • glue:table • glue:trigger • greengrass:group • healthlake:fhirdatastore • iam:virtualmfadevice • imagebuilder:compo nentbuildversion • imagebuilder:component • imagebuilder:containerrecip e • imagebuilder:distributionco nfiguration • imagebuilder:image buildversion • imagebuilder:imagepipeline • imagebuilder:imagerecipe • imagebuilder:image • imagebuilder:infrastructure configuration • iot:authorizer • iot:jobtemplate • iot:mitigationaction • iot:provisioningtemplate • iot:securityprofile • iot:thing • iot:topicruledestination • iotanalytics:channel	

更改	描述	日期
	• iotanalytics:dataset • iotanalytics:datastore • iotanalytics:pipeline • iotevents:alarmmodel • iotevents:detectormodel • iotevents:input • iotsitewise:assetmodel • iotsitewise:asset • iotsitewise:gateway • iottwinmaker:workspace • ivs:channel • ivs:streamkey • kafka:cluster • kinesisvideo:stream • lambda:alias • lambda:layerversion • lambda:layer • lookoutmetrics:alert • lookoutvision:project • mediapackage:channel • mediapackage:origi nendpoint • mediatailor:playbackconfigu ration • memorydb:acl • memorydb:cluster • memorydb:parametergroup • memorydb:user • mobiletargeting:app	

更改	描述	日期
	• mobiletargeting:segment • mobiletargeting:template • networkfirewall:firewallpolicy • networkfirewall:firewall • networkmanager:glo balnetwork • networkmanager:device • networkmanager:link • networkmanager:attachment • networkmanager:cor enetwork • panorama:package • qldb:journalkinesisstreamsf orledger • qldb:ledger • rds:bluegreendeployment • refactorspaces:application • refactorspaces:environment • refactorspaces:route • refactorspaces:service • rekognition:project • resiliencehub:app • resiliencehub:resiliencypol icy • resourcegroups:group • route53:recoverygroup • route53:resourceset • route53:firewalldomain • route53:firewallrulegroup • route53:resolverendpoint	

更改	描述	日期
	• route53:resolverrule • sagemaker:model • sagemaker:notebook instance • signer:signingprofile • ssmincidents:responseplan • ssm:inventoryentry • ssm:resourcedatasync • states:activity • timestream:database • wisdom:assistant • wisdom:assistantassociation • wisdom:knowledgebase	

更改	描述	日期
AWSResourceExplorerServiceRolePolicy— 更新了政策以支持其他资源类型	资源管理器为服务相关角色策略 AWSResourceExplorerServiceRolePolicy 添加了权限，该策略允许服务为以下资源类型编制索引： • codebuild:project • codepipeline:pipeline • cognito:identitypool • cognito:userpool • ecr:repository • efs:filesystem • elasticbeanstalk:application • elasticbeanstalk:applicationversion • elasticbeanstalk:environment • iot:policy • iot:topicrule • stepfunctions:statemachine • s3:bucket	2023 年 8 月 1 日

更改	描述	日期
AWSResourceExplorerServiceRolePolicy— 更新了政策以支持其他资源类型	资源管理器为服务相关角色策略 AWSResourceExplorerServiceRolePolicy 添加了权限，该策略允许服务为以下资源类型编制索引： • elasticache:cluster • elasticache:globalreplicationgroup • elasticache:parametergroup • elasticache:replicationgroup • elasticache:reserved-instance • elasticache:snapshot • elasticache:subnetgroup • elasticache:user • elasticache:usergroup • lambda:code-signing-config • lambda:event-source-mapping • sqs:queue	2023 年 3 月 7 日
新的托管式策略	资源浏览器添加了以下 AWS 托管策略： • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess • AWSResourceExplorerServiceRolePolicy	2022 年 11 月 7 日

更改	描述	日期
资源管理器开启跟踪更改	资源浏览器开始跟踪其 AWS 托管策略的更改。	2022 年 11 月 7 日

为资源管理器使用服务相关角色

AWS 资源探索器 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，它与资源管理器直接相关。服务相关角色由资源管理器预定义，并包含相关服务代表您调用其他 AWS 服务 所需的所有权限。

服务相关角色可让您更轻松地配置资源管理器，因为您不必手动添加必要的权限。资源管理器定义其服务相关角色的权限，除非另外定义，否则只有资源管理器可以代入该角色。定义的权限同时包括信任策略和权限策略，以及不能分配给任何其他 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《IAM 用户指南》中的与 IAM 配合使用的 AWS 服务。在那里可查找服务相关角色列为是的服务。请选择是与查看该服务的服务相关角色文档的链接。

资源管理器的服务相关角色权限

资源管理器使用名为 `AWSServiceRoleForResourceExplorer` 的服务相关角色。此角色向资源管理器服务授予权限，以代表您查看 AWS 账户 中的资源和 AWS CloudTrail 事件，并为这些资源编制索引，以支持搜索。

`AWSServiceRoleForResourceExplorer` 服务相关角色仅信任具有以下服务主体的服务来代入角色：

- `resource-explorer-2.amazonaws.com`

名为 AWSResourceExplorerServiceRolePolicy 的角色权限策略允许资源管理器的只读访问权限，以检索受支持的 AWS 资源的资源名称和属性。要查看资源管理器支持的服务和资源，请参阅可使用资源管理器搜索的资源类型。有关该角色可以执行的所有操作的完整列表，您可以在 IAM 控制台中查看 `AWSResourceExplorerServiceRolePolicy` 策略。

主体是一个 IAM 实体，例如用户、组或角色。如果您让资源管理器在账户的第一个区域中创建索引时为您创建服务相关角色，则执行该任务的主体只需要创建资源管理器索引所需的权限。要使用 IAM 手动创建服务相关角色，则执行任务的主体必须拥有创建服务相关角色的权限。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为资源管理器创建服务相关角色

您无需手动创建服务相关角色。当你在中开启资源管理器AWS Management Console，或者使用AWS CLI或 AWS API AWS 区域 在账户中的第一个资源管理器中运行CreateIndex时，资源浏览器会为你创建服务相关角色。

如果删除此服务相关角色，然后需要再次创建它，则可以使用相同的流程在您的账户中重新创建此角色。当您进入账户RegisterResourceExplorer的第一个区域时，资源管理器会再次为您创建服务相关角色。

为资源管理器编辑服务相关角色

资源管理器不允许您编辑 AWSServiceRoleForResourceExplorer 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。

为资源管理器删除服务相关角色

您可以使用 IAM 控制台、AWS CLI 或 AWS API 来手动删除服务相关角色。为此，必须先移除账户的每个 AWS 区域 中的资源管理器索引，然后才能手动删除服务相关角色。

> **Note**
>
> 如果在您试图删除资源时资源管理器服务正在使用该角色，则删除操作会失败。如果发生这种情况，则请确保删除所有区域中的所有索引，然后等待几分钟后再重试操作。

要使用 IAM 手动删除服务相关角色

使用 IAM 控制台，即 AWS CLI 或 AWS API 来删除 AWSServiceRoleForResourceExplorer 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。

资源管理器服务相关角色支持的区域

资源管理器支持在服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅 Amazon Web Services 一般参考 中的 AWS 服务 端点。

排除 AWS 资源探索器 权限故障

使用以下信息可帮助您诊断和修复在将 AWS Identity and Access Management 资源管理器和 （IAM） 一起使用时可能遇到的常见问题。

主题

我无权在资源管理器中执行操作

如果 AWS Management Console 告诉您，您无权执行某个操作，则必须联系您的管理员寻求帮助。管理员向您提供用于尝试此操作的凭证。

例如，当某人代入 IAM 角色 `MyExampleRole` 尝试使用控制台查看有关视图的详细信息，但不具有 `resource-explorer-2:GetView` 权限时，会发生以下错误。

```
User: arn:aws:iam::123456789012:role/MyExampleRole is not authorized to perform:
 resource-explorer-2:GetView on resource: arn:aws:resource-explorer-2:us-
east-1:123456789012:view/EC2-Only-View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

在这种情况下，使用该角色的人员必须要求管理员更新该角色的权限策略，以允许使用 `resource-explorer-2:GetView` 操作访问视图。

我希望允许我的 AWS 账户 以外的人访问我的资源管理器资源

您可以创建一个角色，以便其它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：

- 要了解资源管理器是否支持这些特征，请参阅 资源管理器如何与 IAM 结合使用。
- 要了解如何为您拥有的 AWS 账户 中的资源提供访问权限，请参阅 IAM 用户指南中的为您拥有的另一个 AWS 账户 中的 IAM 用户提供访问权限。
- 要了解如何为第三方AWS 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的为第三方拥有的 AWS 账户提供访问权限。
- 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之间的差别，请参阅 IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

AWS 资源探索器 中的数据保护

AWS 责任共担模式适用于 AWS 资源探索器 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的博客文章 AWS Shared Responsibility Model and GDPR。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置单个用户。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 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务 中的所有默认安全控制。
- 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。
- 如果您在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

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）。这包括使用控制台、API、AWS CLI 或 AWS SDK 处理资源管理器或其他 AWS 服务时。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。如果您向外部服务器提供网址，我们强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

静态加密

资源管理器存储的数据包括客户使用的资源及其关联 ARN 的索引列表以及用于访问这些资源的视图。

这些数据在静态时通过使用 AWS Key Management Service（AWS KMS）对称加密密钥进行加密，这些密钥在伽罗瓦计数器模式（GCM）中实现高级加密标准（AES），具有 256 位密钥（AES-256-GCM）。

传输中加密

客户请求和所有相关数据使用传输层安全性协议（TLS）1.2 或更高版本进行传输中加密。所有资源管理器端点都支持 HTTPS 来对传输中数据进行加密。有关资源管理器服务端点的列表，请参阅 AWS 一般参考 中的 AWS 资源探索器 端点和配额。

AWS 资源探索器 的合规性验证

要了解 AWS 服务 是否在特定合规性计划范围内，请参阅合规性计划范围内的 AWS 服务 服务。有关常规信息，请参阅AWS 合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅《AWS Artifact 用户指南》中的在 AWS Artifact 中下载报告。

您使用资源管理器的合规性责任取决于您数据的敏感度、贵公司的合规性目标以及适用的法律法规。AWS 提供以下资源来帮助满足合规性：

- 安全性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，并提供了在AWS上部署基于安全性和合规性的基准环境的步骤。
- Amazon Web Services 上的 HIPAA 安全性和合规性架构设计 – 该白皮书介绍了公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。

> **Note**
>
> 并非所有 AWS 服务 都符合 HIPAA 要求。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- 《AWS Config 开发人员指南》中的 Evaluating Resources with Rules – AWS Config 评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub – 此AWS服务提供了AWS中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实操。

AWS 资源探索器 中的故障恢复能力

AWS 全球基础设施围绕 AWS 区域和可用区而构建。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。

有关AWS 区域和可用区的更多信息，请参阅AWS全球基础设施。

AWS 资源探索器 中的基础设施安全性

作为一项托管式服务，AWS 资源探索器 受 AWS 全球网络安全保护。有关 AWS 安全服务以及 AWS 如何保护基础架构的信息，请参阅 AWS 云安全。要按照基础设施安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的 基础设施保护。

您可以使用 AWS 发布的 API 调用通过网络访问资源管理器。客户端必须支持以下内容：

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

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

有关 AWS 全球网络安全程序的更多信息，请参阅 Amazon Web Services：安全过程概述白皮书。

监控 AWS 资源探索器

监控是保持 AWS 资源探索器 和您的其他 AWS 解决方案的可靠性、可用性和性能的重要方面。AWS 提供了以下一些监控工具来监控资源管理器、在出现错误时进行报告并适时自动采取措施。

- AWS CloudTrail 捕获由您的 AWS 账户 或代表该账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以标识哪些用户和账户调用了 AWS、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 使用 AWS CloudTrail 记录 AWS 资源探索器 API 调用 和 AWS CloudTrail 用户指南。

使用 AWS CloudTrail 记录 AWS 资源探索器 API 调用

AWS 资源探索器 与 AWS CloudTrail 集成，后者是记录用户、角色或 AWS 服务 在资源管理器中所执行操作的服务。CloudTrail 将资源管理器的所有 API 调用作为事件捕获。捕获的调用包含来自资源管理器控制台和代码对资源管理器 API 操作的调用。

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（包括资源管理器的事件）。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。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，您可以确定向资源管理器发出了什么请求、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 中的资源管理器信息

在您创建 AWS 账户 时，将在该账户上启用 CloudTrail。当资源管理器中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务 事件一起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。

> **Important**
>
> 您可以通过搜索事件来源 = resource-explorer-2.amazonaws.com 来找到所有资源管理器事件

要持续记录 AWS 账户 中的事件（包括资源管理器的事件），请创建跟踪。通过跟踪记录，CloudTrail 可将日志文件传送至 Simple Storage Service（Amazon S3）存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事

件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）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 AWS CloudTrail 用户指南 中的以下主题：

- 为您的 AWS 账户 创建跟踪
- AWS 服务与 CloudTrail Logs 的集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件
- 从多个账户接收 CloudTrail 日志文件

CloudTrail 记录所有资源管理器操作，AWS 资源探索器 API 参考中介绍了这些操作。例如，对 `CreateIndex`、`DeleteIndex` 和 `UpdateIndex` 操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含相应信息，可帮助您确定提出请求的人员。

- AWS 账户 根凭证
- 来自 AWS Identity and Access Management（IAM）角色或联合用户的临时安全凭证。
- 来自 IAM 用户的长期安全凭证。
- 另一项 AWS 服务。

> **Important**
>
> 出于安全考虑，所有 `Tags`、`Filters` 和 `QueryString` 值均从 CloudTrail 跟踪条目中编辑。

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

了解资源管理器日志文件条目

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，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 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。

主题

- CreateIndex

- DeleteIndex
- UpdateIndexType
- 搜索
- CreateView
- DeleteView
- DisassociateDefaultView

CreateIndex

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


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-166EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-166EXAMPLE",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:13:59Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
```

```
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-index",
    "requestParameters": {
        "ClientToken": "792ee665-58af-423c-bfdb-d7c9aEXAMPLE"
    },
    "responseElements": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "State": "CREATING",
        "CreatedAt": "2022-08-23T19:13:59.775Z"
    },
    "requestID": "a193afe9-17ff-4f30-ae0a-73bb0EXAMPLE",
    "eventID": "2ec50598-4de6-474d-bd0e-f5c00EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

DeleteIndex

下面的示例显示了一个 CloudTrail 日志条目，该条目用于说明 `DeleteIndex` 操作。

> **Note**
>
> 此操作还会异步删除该区域中的账户的所有视图，从而为每个删除的视图生成一个 `DeleteView` 事件。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:My-Role-Name",
        "arn": "arn:aws:sts::123456789012:assumed-role/My-Admin-Role/My-Delegated-
Role",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/My-Admin-Role",
                "accountId": "123456789012",
                "userName": "My-Admin-Role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T18:33:06Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:04:06Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-index",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "State": "DELETING",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "requestID": "d7d80bd2-cd2d-47fb-88d6-5133aEXAMPLE",
    "eventID": "675eab39-c514-4d32-989d-0ea98EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


UpdateIndexType

以下示例显示了一个 CloudTrail 日志条目，该条目演示了将索引从类型 LOCAL 提升为 AGGREGATOR 的 UpdateIndexType 操作。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:21:18Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "UpdateIndexType",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.update-index-type",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "Type": "AGGREGATOR"
    },
    "responseElements": {
        "Type": "AGGREGATOR",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "LastUpdatedAt": "2022-08-23T19:21:17.924Z",
        "State": "UPDATING"
    },
```

```
    "requestID": "a145309d-df14-4c2e-a9f6-8ed45EXAMPLE",
    "eventID": "ed33ab96-f5c6-4a77-a69a-8585aEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

搜索

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

> **Note**
>
> 出于安全考虑，对 `Tag`、`Filters` 和 `QueryString` 参数的所有引用均在 CloudTrail 跟踪条目中编辑。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
```

```
    },
    "eventTime": "2022-08-03T16:50:11Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "Search",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.search",
    "requestParameters": {
        "QueryString": "***"
    },
    "responseElements": null,
    "requestID": "22320db5-b194-446f-b9f4-e603bEXAMPLE",
    "eventID": "addb3bca-0c41-46bf-a5e6-42299EXAMPLE",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

CreateView

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-01-20T21:54:48Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-view",
    "requestParameters": {
        "ViewName": "CTTagsTest",
        "Tags": "***"
    },
    "responseElements": {
        "View": {
            "Filters": "***",
            "IncludedProperties": [],
            "LastUpdatedAt": "2023-01-20T21:54:48.079Z",
            "Owner": "123456789012",
            "Scope": "arn:aws:iam::123456789012:root",
            "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    },
    "requestID": "b22d8ced-4905-42c4-b1aa-ef713EXAMPLE",
    "eventID": "f62e339f-1070-41a8-a6ec-12491EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

DeleteView

下面的示例显示了一个 CloudTrail 日志条目，该条目演示了当 DeleteView 操作由于相同 AWS 区域中的 DeleteIndex 操作而自动开始时可能发生的事件。

> **Note**
>
> 如果已删除的视图是该区域的默认视图，则此操作还会异步取消该视图作为默认视图的关联。这将生成一个 DisassociateDefaultView 事件。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-09-16T19:33:27Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "cd174d1e-0a24-4b47-8b67-d024aEXAMPLE",
    "readOnly": false,
    "resources": [{
```

```
        "accountId": "334026708824",
        "type": "AWS::ResourceExplorer2::View",
        "ARN": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }],
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

DisassociateDefaultView

下面的示例显示了一个 CloudTrail 日志条目，该条目演示了当 DisassociateDefaultView 操作由于当前默认视图上的 DeleteView 操作而自动开始时可能发生的事件。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "resource-explorer-2.amazonaws.com"
    },
    "eventTime": "2022-09-16T19:33:26Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DisassociateDefaultView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.disassociate-default-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "d8016cb1-5c23-4ea4-bda2-70b03EXAMPLE",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

使用 CloudFormation 创建资源管理器资源

AWS 资源探索器 与 AWS CloudFormation 集成，后者是一项可帮助您建模和设置 AWS 资源的服务。此集成可帮助您花费更少的时间来创建和管理您的资源和基础设施。您可以创建一个描述所需的全部 AWS 资源的模板，CloudFormation 将为您预调配和配置这些资源。资源的示例包括索引、视图或为 AWS 区域 进行的默认视图分配。

在您使用 CloudFormation 时，可重复使用您的模板来不断地重复设置您的资源管理器资源。描述您的资源一次，然后在多个 AWS 账户 和区域中反复预调配相同的资源。

使用 AWS CloudFormation 将资源管理器部署到 AWS Organizations

您可以使用 AWS CloudFormation StackSets 将资源管理器部署到组织中的所有账户。当您在组织中添加或创建成员账户时，StackSets 可以自动将每个 AWS 区域 的索引配置到新的成员账户，包括您指定的聚合器索引。有关说明，请参阅 为组织中的账户部署资源管理器。

资源管理器和 CloudFormation 模板

要为资源管理器和相关服务预调配和配置资源，您必须了解 AWS CloudFormation 模板。模板是 JSON 或 YAML 格式的文本文件。这些模板描述要在 CloudFormation 堆栈中预调配的资源。如果您不熟悉 JSON 或 YAML，可以在 AWS CloudFormation Designer 的帮助下开始使用 CloudFormation 模板。有关更多信息，请参阅AWS CloudFormation用户指南中的什么是 AWS CloudFormation Designer？。

资源管理器支持在 CloudFormation 中创建以下资源类型：

- 索引 – 在区域中创建索引并在该区域开启资源管理器。您可以将索引指定为 AWS 账户 的本地索引或聚合器索引。有关更多信息，请参阅 在 AWS 区域 中启用资源管理器以索引您的资源 和 通过创建聚合器索引开启跨区域搜索：
- 视图 – 创建一个视图，用于确定用户执行搜索时可以显示哪些结果。每个搜索操作都必须指定一个视图。您必须授予用户使用您希望他们访问的视图的权限。有关更多信息，请参阅管理资源管理器视图以提供搜索访问权限。

> **Note**
>
> 必须先在某个区域中创建索引，然后才能在该区域中创建视图。如果您创建索引和视图作为同一个堆栈的一部分，请使用视图上的 DependsOn 属性，如以下示例模板所示，以确保首先创建索引。

- DefaultViewAssociation – 将指定的视图分配为其区域中的默认视图。当用户未明确指定用于搜索操作的视图时，资源管理器会尝试使用与用户执行搜索所在区域关联的默认视图。有关更多信息，请参阅在 AWS 区域 中设置默认视图。

以下示例说明了如何在同一个区域中创建一个索引和一个视图，并将该视图设置为该区域的默认视图。

YAML

```
Description: >-
  Sample CFN Stack setting up Resource Explorer with an aggregator index and a default
 view
Resources:
  SampleIndex:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
  SampleView:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: mySampleView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
    DependsOn: SampleIndex
  SampleDefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref SampleView
```

JSON

```
{
    "Description": "Sample CFN Stack setting up Resource Explorer with an aggregator
 index and a default view ",
    "Resources": {
        "SampleIndex": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
```

```
                "Tags": {
                    "Purpose": "ResourceExplorer Sample Stack"
                }
            }
        },
        "SampleView": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "mySampleView",
                "IncludedProperties": [
                    {
                        "Name": "tags"
                    }
                ],
                "Tags": {
                    "Purpose": "ResourceExplorer Sample CFN Stack"
                }
            },
            "DependsOn": "SampleIndex"
        },
        "SampleDefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "SampleView"
                }
            }
        }
    }
}
```

有关更多信息（包括资源管理器索引和视图的 JSON 和 YAML 模板示例），请参阅《AWS CloudFormation 用户指南》中的 ResourceExplorer2 资源类型参考。

了解有关 AWS CloudFormation 的更多信息

要了解有关 CloudFormation 的更多信息，请参阅以下资源：

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

资源管理器问题排查

如果您在使用资源管理器时遇到问题，请查询本部分中的相关主题。另请参阅本指南的安全部分中的排除 AWS 资源探索器 权限故障。

主题

一般性问题

主题

我收到了资源管理器的链接，但是当我打开它时，控制台只显示错误。

某些第三方工具会生成指向资源管理器中页面的链接 URL。在某些情况下，这些 URL 不包含将控制台定向到特定 AWS 区域 的参数。如果您打开这样的链接，则资源管理器控制台不会被告知要使用哪个区域，并且默认为使用用户上次登录的区域。如果用户无权访问该区域的资源管理器，则控制台将尝试使用美国东部（弗吉尼亚州北部）（us-east-1）区域，如果控制台无法访问 us-east-1，则会尝试使用美国西部（俄勒冈州）（us-west-2）。

如果用户没有权限访问这些区域中任何一个区域的索引，则资源管理器控制台会返回错误。

您可以通过确保所有用户都具有以下权限来防止出现此问题：

- ListIndexes – 没有特定的资源；使用 *。
- GetIndex 用于在账户中创建的每个索引的 ARN。为了避免在删除并重新创建索引时必须重做权限策略，建议您使用 *。

实现该目标的最低策略可能类似于此示例：

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetIndex",
                "resource-explorer-2:ListIndexes",
            ],
            "Resource": "*"
        }
    ]
}
```

或者，您可以考虑将 AWS 托管权限 AWSResourceExplorerReadOnlyAccess 授予所有需要使用资源管理器的用户。这将授予这些必需的权限，以及查看该区域可用视图并使用这些视图进行搜索所需的权限。

为什么控制台中的统一搜索会导致我的 CloudTrail 日志中出现“访问被拒绝”错误？

AWS Management Console 中的统一搜索使主体能够从 AWS Management Console 中的任何页面进行搜索。如果资源管理器已开启并配置为支持统一搜索，则结果可能包括主体人账户中的资源。每当您开始在统一搜索栏中键入内容时，统一搜索都会尝试调用 `resource-explorer-2:ListIndexes` 操作来检查结果中是否可以包含用户账户中的资源。

统一搜索使用当前登录用户的权限来执行此检查。如果该用户没有权限调用在附加的 AWS Identity and Access Management（IAM）权限策略中授予的 `resource-explorer-2:ListIndexes`，则检查将失败。该失败将作为 `Access denied` 条目添加到您的 CloudTrail 日志中。

该 CloudTrail 日志条目具有以下特性：

- 事件源：`resource-explorer-2.amazonaws.com`
- 事件名称：`ListIndexes`
- 错误代码：`403`（访问被拒绝）

以下 AWS 托管策略包含调用 `resource-explorer-2:ListIndexes` 的权限。如果您将其中任何一个分配给主体或包含此权限的任何其他策略，则不会发生此错误：

- AWSResourceExplorerReadOnlyAccess

- AWSResourceExplorerFullAccess
- ReadOnlyAccess
- ViewOnlyAccess

资源管理器设置和配置问题排查

使用此处的信息，可帮助您诊断和修复初始设置或配置 AWS 资源探索器 时可能出现的问题。

主题

当我向资源管理器发出请求时，收到了“访问被拒绝”消息

- 验证您是否具有调用您请求的操作和资源的权限。管理员可以通过向您的 IAM 主体（例如角色、组或用户）分配 AWS Identity and Access Management（IAM）权限策略来授予权限。

  要提供访问权限，请为您的用户、组或角色添加权限：

  - AWS IAM Identity Center 中的用户和组：

    创建权限集合。按照《AWS IAM Identity Center 用户指南》中 创建权限集 的说明进行操作。

  - 通过身份提供商在 IAM 中托管的用户：

    创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。

  - IAM 用户：
    - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
    - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

  该策略必须允许您要访问的 `Resource` 上所请求的 `Action`。

  如果授予这些权限的策略语句包含任何条件 (例如，当日时间或 IP 地址限制)，则您还必须在发送请求时满足这些要求。有关查看或修改适用于 IAM 主体的策略的信息，请参阅《IAM 用户指南》中的管理 IAM policy。

- 如果您手动对 API 请求进行签名（而不使用 AWS SDK），则请确认您已正确对请求进行签名。

当我使用临时安全凭证发送请求时，收到了“access denied”(拒绝访问) 消息

- 请确认您用于发出请求的 IAM 主体具有正确的权限。临时安全凭证权限派生自 IAM 中定义的主体，因此权限范围仅限于该主体的权限。有关临时安全凭证权限的确定方式的更多信息，请参阅《IAM 用户指南》中的控制临时安全凭证的权限。
- 验证您的请求是否采用了正确的签名和适当的格式。有关详细信息，请参阅所选 SDK 的工具包文档或《IAM 用户指南》中的将临时凭证用于 AWS 资源。
- 验证您的临时安全凭证没有过期。有关更多信息，请参阅《IAM 用户指南》中的请求临时安全凭证。

资源管理器搜索问题排查

使用此处的信息可帮助您诊断和修复在使用资源管理器搜索资源时可能出现的常见错误。

主题

为什么我的资源管理器搜索结果中缺少某些资源？

某些资源可能无法按预期显示在搜索结果中，以下列表提供了原因：

初始索引未完成

在 AWS 区域 中首次打开资源管理器后，可能需要长达 36 小时才能完成对聚合器索引的索引和复制。请稍后重新尝试搜索。

资源是新的

新资源可能需要几分钟才会由资源管理器发现并将其添加到本地索引中。过几分钟再试。

有关一个区域内新资源的信息尚未传播到聚合器索引

在一个区域中发现的新资源的详细信息可能需要一些时间才能在自己的区域中编制索引，然后复制到该账户的聚合器索引中。只有在复制完成后，新资源才能显示在跨区域搜索结果中。请稍后重新尝试搜索。

拥有资源的区域未开启资源管理器

您的管理员决定了资源管理器可以在哪些 AWS 区域 中运行。设置页面显示了哪些区域已开启资源管理器并包含索引。如果拥有资源的区域未开启，则请让您的管理员在该区域开启资源管理器。

资源存在于不同的区域，并且搜索的区域不包含聚合器索引

您只能使用包含聚合器索引的区域中的视图，对账户中所有区域的资源进行搜索。在任何其他区域进行搜索时，只会返回您执行搜索的区域中的资源。

视图上的筛选条件不包括该资源

每个视图都可以在配置中包含筛选条件，以限制使用该视图创建的搜索结果中可以包含哪些结果。确保您要查找的资源与您用于搜索的视图中的筛选条件相匹配。有关筛选器的更多信息，请参阅筛选条件。有关视图的更多信息，请参阅 关于资源管理器视图。

资源浏览器不支持该资源类型

资源管理器不支持某些资源类型。有关更多信息，请参阅您可以使用资源管理器搜索的资源类型：

未在控制台区域配置索引或视图

如果索引或视图未在控制台使用该控件的预期区域中配置，则您将看不到预期的结果。有关更多信息，请参阅 通过创建聚合器索引开启跨区域搜索 和 关于资源管理器视图。

您的视图不包含标签

标签是资源管理器控件所必需的。如果您的视图不包含标签，则这些资源将不会包含在结果中。有关更多信息，请参阅向视图添加标签：

您的搜索使用了错误的搜索查询语法

在资源管理器中搜索是该服务所独有的。如果没有正确的语法，您将无法找到所需的资源。有关更多信息，请参阅资源管理器的搜索查询语法参考：

您最近为自己的资源添加了标签

在为资源添加标签后，会有 30 秒的延迟，该资源才会显示在搜索结果中。

资源类型不支持标签过滤器

如果资源类型不支持标签过滤器，则它们将不会显示在资源管理器小组件中。不支持标签过滤器的资源类型有：

- cloudfront:cache-policy
- cloudfront:origin-access-identity
- cloudfront:function
- cloudfront:origin-request-policy
- cloudfront:realtime-log-config
- cloudfront:response-headers-policy
- cloudwatch:dashboard
- docdb:globalcluster
- elasticache:globalreplicationgroup
- iam:group
- lambda:code-signing-config
- lambda:event-source-mapping
- ssm:windowtarget
- ssm:windowtask
- rds:auto-backup
- rds:global-cluster
- s3:accesspoint

为什么我的资源没有显示在控制台的统一搜索结果中？

统一的搜索结果可在每个 AWS Management Console 页面顶部的搜索栏中找到。但是，只有在完成以下配置选项之后，搜索才能返回与搜索结果中的查询相匹配的资源：

- 账户中的其中一个区域中必须有聚合器索引。
- 包含聚合器索引的区域中必须有默认视图。
- 所有主体（IAM 角色和用户）都必须具有使用该默认视图进行搜索的权限。

为什么控制台和资源管理器中的统一搜索有时会得到不同的结果？

统一的搜索结果可在每个 AWS Management Console 页面顶部的搜索栏中找到。使用统一搜索时，统一搜索过程会自动在查询字符串中键入的第一个词的末尾，插入一个通配符（*）。该通配符在统一搜索框中不可见，但它确实会影响结果。

> **Important**
>
> 统一搜索会自动在字符串中第一个关键字的末尾插入通配符（*）运算符。这意味着统一的搜索结果包括与任何以指定关键字开头的字符串相匹配的资源。
> 通过查询文本框，在资源管理器控制台的资源搜索页面上执行的搜索，不会自动附加通配符。您可以在搜索字符串中的任何术语后面手动插入 *。

我需要什么权限才能搜索资源？

要进行搜索，您必须有权对位于调用该操作的区域中的视图执行以下两项操作：

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

这可以通过在分配给您的 IAM 主体的策略中添加类似于以下示例的语句来完成。

```
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-
View-Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
```

您可以将特定视图的 Amazon 资源编号（ARN）替换为包含通配符（*）的 ARN，以向所有匹配的视图授予权限。

如果您未在请求中指定视图，则资源管理器会自动使用您提出请求所在区域的默认视图。如果您没有使用默认视图的权限，请咨询您的管理员。

> **Note**
>
> 即使您在资源管理器搜索查询的结果中看到某个资源，也需要对资源本身具有权限才能与该资源进行交互。

您可以使用资源管理器搜索的资源类型

主题

下表列出了支持在 AWS 资源探索器中搜索的资源类型。

> **注意**
>
> - 某些资源类型由 Amazon 资源名称（ARN）字符串标识，这些字符串与其他资源类型共享通用格式。发生这种情况时，资源管理器可以将此类资源报告为其他资源类型。有关受此问题影响的资源类型列表，请参阅 显示为其他类型的资源类型。
> - 目前，附加到 AWS Identity and Access Management (IAM) 资源（例如角色或用户）的标签无法用于搜索。
> - 如果您对某些资源拥有加密访问权限，则资源管理器将无法发现它们。您将不会在搜索结果中看到这些资源。

支持的服务和资源类型

支持的 AWS 服务

- Amazon API Gateway
- AWS App Runner
- 亚马逊 AppStream 2.0
- AWS AppSync
- Amazon Athena
- AWS Backup
- AWS Batch
- AWS CloudFormation

- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- CloudWatch 很明显 Amazon
- Amazon CloudWatch 日志
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- Amazon P CodeGuru rofiler
- AWS CodePipeline
- AWS CodeConnections
- Amazon Cognito
- Amazon Connect
- Amazon Connect Wisdom
- Amazon Detective
- Amazon DynamoDB
- EC2 Image Builder
- Amazon ECR Public
- AWS Elastic Beanstalk
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- AWS Elemental MediaPackage
- AWS Elemental MediaTailor
- Amazon EMR Serverless
- Amazon EventBridge

- AWS Fault Injection Service
- Amazon Forecast
- Amazon Fraud Detector
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS Identity and Access Management
- Amazon Interactive Video Service
- AWS IoT
- AWS IoT Analytics
- AWS IoT Events
- AWS IoT Greengrass Version 1
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- Amazon Kinesis
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- Amazon Location Service
- Amazon Lookout for Metrics
- Amazon Lookout for Vision
- 适用于 Apache Flink 的亚马逊托管服务
- Amazon Managed Service for Prometheus
- Amazon Managed Service for Prometheus
- Amazon Managed Streaming for Apache Kafka
- AWS Migration Hub Refactor Spaces

- AWS Network Firewall
- AWS Network Manager
- 亚马逊 OpenSearch 服务
- AWS Panorama
- Amazon Personalize
- AWS Private Certificate Authority
- Amazon QLDB
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (Amazon RDS)
- AWS Resilience Hub
- AWS Resource Groups
- AWS 资源探索器
- Amazon Route 53
- Amazon Route 53 Recovery 就绪性
- Amazon Route 53 Resolver
- Amazon SageMaker
- AWS Secrets Manager
- AWS Service Catalog
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager
- AWS Verified Access
- AWS Wavelength

Amazon API Gateway

- `apigateway:restapis`

AWS App Runner

- apprunner:vpcconnector

亚马逊 AppStream 2.0

- appstream:appblock
- appstream:application
- appstream:fleet
- appstream:stack

AWS AppSync

- appsync:apis

Amazon Athena

- athena:datacatalog
- athena:workgroup

AWS Backup

- backup:backupplan

AWS Batch

- batch:computeenvironment
- batch:jobqueue
- batch:schedulingpolicy

AWS CloudFormation

- cloudformation:stack

- cloudformation:stackset

Amazon CloudFront

- cloudfront:cache-policy
- cloudfront:distribution
- cloudfront:function
- cloudfront:fieldlevelencryptionconfig
- cloudfront:fieldlevelencryptionprofile
- cloudfront:origin-access-identity
- cloudfront:originaccesscontrol
- cloudfront:origin-request-policy
- cloudfront:realtime-log-config
- cloudfront:response-headers-policy

AWS CloudTrail

- cloudtrail:trail

Amazon CloudWatch

- cloudwatch:alarm
- cloudwatch:dashboard
- cloudwatch:insight-rule
- cloudwatch:metric-stream
- evidently:project

CloudWatch 很明显 Amazon

- evidently:project/experiment
- evidently:project/feature
- evidently:project/launch

Amazon CloudWatch 日志

- logs:destination
- logs:log-group

AWS CodeArtifact

- codeartifact:domain
- codeartifact:repository

AWS CodeBuild

- codebuild:project

AWS CodeCommit

- codecommit:repository

Amazon P CodeGuru rofiler

- codeguru-profiler:profilingGroup

AWS CodePipeline

- codepipeline:pipeline

AWS CodeConnections

- codestarconnections:connect

Amazon Cognito

- cognito:identitypool

- cognito:userpool

Amazon Connect

- appintegrations:eventintegration

Amazon Connect Wisdom

- wisdom:assistant
- wisdom:association
- wisdom:knowledge-base

Amazon Detective

- detective:graph

Amazon DynamoDB

- dynamodb:table

EC2 Image Builder

- imagebuilder:component
- imagebuilder:containerrecipe
- imagebuilder:distributionconfiguration
- imagebuilder:image
- imagebuilder:imagepipeline
- imagebuilder:imagerecipe
- imagebuilder:infrastructureconfiguration

Amazon ECR Public

- ecrpublic:repository

AWS Elastic Beanstalk

- elasticbeanstalk:application
- elasticbeanstalk:applicationversion
- elasticbeanstalk:configurationtemplate
- elasticbeanstalk:environment

Amazon ElastiCache

- elasticache:cluster
- elasticache:globalreplicationgroup
- elasticache:parametergroup
- elasticache:replicationgroup
- elasticache:reserved-instance
- elasticache:snapshot
- elasticache:subnetgroup
- elasticache:user
- elasticache:usergroup

Amazon Elastic Compute Cloud (Amazon EC2)

- ec2:capacity-reservation
- ec2:capacity-reservation-fleet
- ec2:client-vpn-endpoint
- ec2:customer-gateway
- ec2:dedicated-host
- ec2:dhcp-options
- ec2:egress-only-internet-gateway
- ec2:elastic-gpu
- ec2:elastic-ip

- ec2:fleet
- ec2:fpga-image
- ec2:host-reservation
- ec2:image
- ec2:instance
- ec2:instance-event-window
- ec2:internet-gateway
- ec2:ipam
- ec2:ipam-pool
- ec2:ipam-scope
- ec2:ipv4pool-ec2
- ec2:key-pair
- ec2:launch-template
- ec2:natgateway
- ec2:network-acl
- ec2:network-insights-access-scope
- ec2:network-insights-access-scope-analysis
- ec2:network-insights-analysis
- ec2:network-insights-path
- ec2:network-interface
- ec2:placement-group
- ec2:prefix-list
- ec2:reserved-instances
- ec2:route-table
- ec2:security-group
- ec2:security-group-rule
- ec2:snapshot
- ec2:spot-fleet-request
- ec2:spot-instances-request

- ec2:subnet
- ec2:subnet-cidr-reservation
- ec2:traffic-mirror-filter
- ec2:traffic-mirror-filter-rule
- ec2:traffic-mirror-session
- ec2:traffic-mirror-target
- ec2:transit-gateway
- ec2:transit-gateway-attachment
- ec2:transit-gateway-connect-peer
- ec2:transit-gateway-multicast-domain
- ec2:transit-gateway-policy-table
- ec2:transit-gateway-route-table
- ec2:transitgatewayroutetableannouncement
- ec2:volume
- ec2:vpc
- ec2:vpc-endpoint
- ec2:vpc-flow-log
- ec2:vpc-peering-connection
- ec2:vpn-connection
- ec2:vpn-gateway

Amazon Elastic Container Registry

- ecr:repository

Amazon Elastic Container Service

- ecs:cluster
- ecs:container-instance
- ecs:service

- ecs:task
- ecs:task-definition
- ecs:task-set

Amazon Elastic File System

- efs:filesystem
- efs:accesspoint

Elastic Load Balancing

- elasticloadbalancing:listener
- elasticloadbalancing:listener-rule
- elasticloadbalancing:listener-rule/app
- elasticloadbalancing:listener/app
- elasticloadbalancing:listener/net
- elasticloadbalancing:loadbalancer
- elasticloadbalancing:loadbalancer/app
- elasticloadbalancing:loadbalancer/net
- elasticloadbalancing:targetgroup

AWS Elemental MediaPackage

- mediapackage:channel
- mediapackage:originendpoint
- mediapackage-vod:packaging-configurations
- mediapackage-vod:packaging-groups

AWS Elemental MediaTailor

- mediatailor:playbackConfiguration

Amazon EMR Serverless

- emr-serverless:applications

Amazon EventBridge

- events:event-bus
- events:rule

AWS Fault Injection Service

- fis:experimenttemplate

Amazon Forecast

- forcast:dataset
- forcast:dataset-group

Amazon Fraud Detector

- frauddetector:detector
- frauddetector:entity-type
- frauddetector:event-type
- frauddetector:label
- frauddetector:outcome
- frauddetector:variable

Amazon GameLift

- gamelift:alias

AWS Global Accelerator

- globalaccelerator:accelerator
- globalaccelerator:accelerator/listener
- globalaccelerator:accelerator/listener/endpoint-group

AWS Glue

- glue:database
- glue:job
- glue:table
- glue:trigger

AWS Glue DataBrew

- databrew:dataset
- databrew:recipe
- databrew:ruleset

AWS Identity and Access Management

- iam:group
- iam:instance-profile
- iam:oidc-provider
- iam:policy
- iam:role
- iam:saml-provider
- iam:server-certificate
- iam:user
- iam:virtualmfadevice

Amazon Interactive Video Service

- ivs:channel
- ivs:streamkey

AWS IoT

- iot:authorizer
- iot:jobtemplate
- iot:mitigationaction
- iot:policy
- iot:provisioningtemplate
- iot:rolealias
- iot:securityprofile
- iot:thing
- iot:topicrule

AWS IoT Analytics

- iotanalytics:channel
- iotanalytics:dataset
- iotanalytics:datastore
- iotanalytics:pipeline

AWS IoT Events

- iotevents:alarmModel
- iotevents:detectorModel
- iotevents:input

AWS IoT Greengrass Version 1

- greengrass:components
- greengrass:groups

AWS IoT SiteWise

- iotsitewise:asset
- iotsitewise:assetmodel
- iotsitewise:gateway

AWS IoT TwinMaker

- iottwinmaker:workspace
- iottwinmaker:workspace/component-type
- iottwinmaker:workspace/entity

AWS Key Management Service

- kms:key

Amazon Kinesis

- kinesis:stream

Amazon Data Firehose

- kinesisfirehose:deliverystream

Amazon Kinesis Video Streams

- kinesisvideo:stream

AWS Lambda

- lambda:code-signing-config
- lambda:event-source-mapping
- lambda:function

Amazon Lex

- lex:bot

Amazon Location Service

- geo:place-index
- geo:tracker

Amazon Lookout for Metrics

- lookoutmetrics:Alert

Amazon Lookout for Vision

- lookoutvision:project

适用于 Apache Flink 的亚马逊托管服务

- kinesisanalytics:application

Amazon Managed Service for Prometheus

- aps:rulegroupsnamespace
- aps:workspace

Amazon Managed Service for Prometheus

- memorydb:cluster
- memorydb:parametergroup
- memorydb:user

Amazon Managed Streaming for Apache Kafka

- kafka:cluster
- kafka:configuration

AWS Migration Hub Refactor Spaces

- refactor-spaces:environment
- refactor-spaces:environment/application
- refactor-spaces:environment/application/route
- refactor-spaces:environment/application/service

AWS Network Firewall

- network-firewall:firewall-policy

AWS Network Manager

- networkmanager:core-network
- networkmanager:device
- networkmanager:global-network
- networkmanager:link

亚马逊 OpenSearch 服务

- es:domain

AWS Panorama

- panorama:package

Amazon Personalize

- personalize:dataset
- personalize:dataset-group
- personalize:schema

AWS Private Certificate Authority

- acmpca:certificateauthority

Amazon QLDB

- qldb:ledger
- qldb:stream

Amazon Redshift

- redshift:cluster
- redshift:eventsubscription
- redshift:parametergroup
- redshift:snapshot
- redshift:snapshotcopygrant
- redshift:snapshotschedule
- redshift:subnetgroup
- redshift:usagelimit

Amazon Rekognition

- rekognition:project

Amazon Relational Database Service (Amazon RDS)

- rds:auto-backup
- rds:cev
- rds:cluster
- rds:cluster-endpoint
- rds:cluster-pg
- rds:cluster-snapshot
- rds:db
- rds:db-proxy
- rds:db-proxy-endpoint
- rds:deployment
- rds:es
- rds:global-cluster
- rds:og
- rds:pg
- rds:ri
- rds:secgrp
- rds:snapshot
- rds:subgrp

AWS Resilience Hub

- resiliencehub:resiliencypolicy

AWS Resource Groups

- resourcegroups:group

AWS 资源探索器

- resource-explorer-2:index

- resource-explorer-2:view

Amazon Route 53

- route53:healthcheck
- route53:hostedzone

Amazon Route 53 Recovery 就绪性

- route53-recover-readiness:recovery-group
- route53-recover-readiness:resource-set

Amazon Route 53 Resolver

- route53resolver:firewalldomainlist
- route53resolver:firewallrulegroup
- route53resolver:resolverendpoint
- route53resolver:resolverrule

Amazon SageMaker

- sagemaker:model
- sagemaker:notebookinstance

AWS Secrets Manager

- secretsmanager:secret

AWS Service Catalog

- servicecatalog:applications
- servicecatalog:attribute-groups

Amazon Simple Notification Service

- sns:topic

Amazon Simple Queue Service

- sqs:queue

Amazon Simple Storage Service (Amazon S3)

- s3:accesspoint
- s3:bucket
- s3:storage-lens

AWS Step Functions

- states:statemachine
- stepfunctions:activity

AWS Systems Manager

- ssm:association
- ssm:automation-execution
- ssm:document
- ssm:maintenancewindow
- ssm:managed-instance
- ssm:parameter
- ssm:patchbaseline
- ssm:resourcedatasync
- ssm:windowtarget
- ssm:windowtask

AWS Verified Access

- ec2:verifiedaccessendpoint
- ec2:verifiedaccessgroup
- ec2:verifiedaccessinstance
- ec2:verifiedaccesstrustprovider

AWS Wavelength

- ec2:carriergateway

以编程方式访问受支持的资源类型的列表

要通过代码访问支持的资源类型列表，您可以从任何 AWS SDK 调用该ListSupportedResourceTypes操作。

例如，您可以运行 list-supported-resource-types AWS Command Line Interface (AWS CLI) 命令，如以下示例所示。

```
$ aws resource-explorer-2 list-supported-resource-types
{
    "ResourceTypes": [
        {
            "ResourceType": "acm-pca:certificate-authority",
            "Service": "acm-pca"
        },
        {
            "ResourceType": "airflow:environment",
            "Service": "airflow"
        },
        {
            "ResourceType": "amplify:branches",
            "Service": "amplify"
        },
... truncated for brevity ...
```

显示为其他类型的资源类型

某些资源类型由 Amazon 资源名称（ARN）字符串标识，这些字符串与其他资源类型共享通用格式。发生这种情况时，资源管理器可以将此类资源报告为其他资源类型。这将会影响下表中的资源类型。

实际资源类型	已报告为资源类型
ec2:securitygroupegress ec2:securitygroupingress	ec2:security-group-rule
elasticloadbalancingv2:loadbalancer	elasticloadbalancing:loadbalancer
docdb:dbcluster neptune:dbcluster rds:dbcluster	rds:cluster
docdb:dbclusterparametergroup neptune:dbclusterparametergroup rds:dbclusterparametergroup	rds:cluster-pg
docdb:clustersnapshot neptune:dbclustersnapshot rds:clustersnapshot	rds:cluster-snapshot
docdb:dbinstance neptune:dbinstance rds:dbinstance	rds:db
docdb:eventsubscription neptune:eventsubscription	rds:es

实际资源类型	已报告为资源类型
rds:eventsubscription	
docdb:globalcluster rds:globalcluster	rds:global-cluster
neptune:dbparametergroup rds:dbparametergroup	rds:pg
docdb:dbsubnetgroup neptune:dbsubnetgroup rds:dbsubnetgroup	rds:subgrp

资源管理器的配额

您的 AWS 账户 对每个 AWS 服务 都施加了默认限额。除非另有说明，否则每个限额都是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。

要查看 AWS 资源探索器 的限额，请打开服务限额控制台。在导航窗格中，选择 AWS 服务 并选择资源管理器。

要请求提高配额，请参阅 Service Quotas 用户指南中的请求增加配额。如果配额在 Service Quotas 中尚不可用，请使用提高限制表格。

以下限额是资源管理器的默认限额。

最大值限额	默认值
AWS 区域 中的视图数量	10

操作的速率限制	默认值
每秒最大搜索操作数	5
每秒最大非搜索操作数	3
聚合器区域中的每月最大搜索操作数	10000
本地区域中的每月最大搜索操作数	500

AWS 资源探索器 与 AWS SDK 一起使用

AWS 软件开发套件 (SDK) 可用于许多流行的编程语言。每个软件开发工具包都提供 API、代码示例和文档，使开发人员能够更轻松地以其首选语言构建应用程序。

SDK 文档	代码示例
AWS SDK for C++	AWS SDK for C++ 代码示例
AWS CLI	AWS CLI 代码示例
AWS SDK for Go	AWS SDK for Go 代码示例
AWS SDK for Java	AWS SDK for Java 代码示例
AWS SDK for JavaScript	AWS SDK for JavaScript 代码示例
AWS SDK for Kotlin	AWS SDK for Kotlin 代码示例
AWS SDK for .NET	AWS SDK for .NET 代码示例
AWS SDK for PHP	AWS SDK for PHP 代码示例
AWS Tools for PowerShell	PowerShell 代码示例工具
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 代码示例
AWS SDK for Ruby	AWS SDK for Ruby 代码示例
AWS SDK for Rust	AWS SDK for Rust 代码示例
适用于 SAP ABAP 的 AWS SDK	适用于 SAP ABAP 的 AWS SDK 代码示例
AWS SDK for Swift	AWS SDK for Swift 代码示例

示例可用性

找不到所需的内容？ 通过使用此页面底部的提供反馈链接请求代码示例。

《资源管理器用户指南》的文档历史记录

下表描述了的文档版本 AWS 资源探索器。要获得本文档的更新通知，您可以订阅 RSS 源。

变更	说明	日期
增加了对新资源类型的支持	Resource Explorer 增加了对来自 65 个新资源的支持 AWS Key Management Service， AWS 服务 包括亚马逊 Route 53 和 Amazon Fraud Detector。	2024 年 2 月 20 日
更新了托管式策略	资源浏览器增加了查看其他资源类型的支持。AWSResourceExplorerServiceRolePolicy AWS 托管策略已更新，授予资源浏览器查看其他资源类型的访问权限。	2023 年 12 月 12 日
添加了新的搜索筛选条件	资源管理器现在支持按应用程序搜索资源。	2023 年 11 月 16 日
增加了对新资源类型的支持	资源管理器增加了对来自 AWS 服务 AWS CloudFormation、和 Amazon 的 86 AWS Glue种新资源的支持 SageMaker。	2023 年 11 月 15 日
资源管理器支持多账户搜索	现在，您可以使用资源管理器在您的组织或组织单位内的 AWS 账户 中搜索和发现资源。有关更多信息，请参阅开启多账户搜索。	2023 年 11 月 14 日
新增和更新的托管式策略	资源管理器添加了对 AWS Organizations的支持。AWS 托管策略已添加和更新，可向您的组织、组织结构、账户和委	2023 年 11 月 14 日

	派管理员授予资源管理器访问权限。	
增加了对新资源类型的支持	资源管理器添加了对 AWS Organizations的支持。AWS 托管策略已更新，可向您的组织、组织结构、账户和委派管理员授予资源管理器访问权限。	2023 年 11 月 14 日
增加了对新资源类型的支持	资源管理器现在支持来自 Amazon Cognito、 AWS Elastic Beanstalk和 Amazon Elastic File System 等服务的 12 种新资源类型。	2023 年 10 月 18 日
增加了对新资源类型的支持	资源管理器增加了对 164 个资源的支持。授予资源管理器访问索引资源的 AWS 托管策略已更新，可包括这些新的资源类型。	2023 年 10 月 17 日
资源管理器现已在某些可选择加入的区域中可用	BAH 和 CGK 中的客户现在可以选择使用资源管理器。	2023 年 10 月 5 日
增加了对新资源类型的支持	资源管理器增加了对以下资源的支持 AWS 服务：AWS CodeBuild、、Amazon Cognito AWS CodePipeline、亚马逊弹性容器注册表、 AWS Elastic Beanstalk Amazon Elastic File System AWS IoT、和。 AWS Step Functions授予资源管理器访问索引资源的 AWS 托管策略已更新，可包括这些新的资源类型。	2023 年 8 月 1 日

资源管理器现在支持将搜索结果导出为 CSV	现在，您可以将资源搜索页面上的搜索结果导出为 CSV 格式的文件。	2023 年 4 月 4 日
AWS Chatbot 用于搜索和发现您的 AWS 资源	现在 AWS Chatbot ，您可以使用自然语言问题来搜索您的资源。有关更多信息，请参阅使用 AWS Chatbot 搜索资源。	2023 年 3 月 30 日
增加了对新资源类型的支持	资源管理器增加了对以下资源的支持 AWS 服务：亚马逊和亚马逊简单队列服务 (Amazon ElastiCache SQS) Simple Queue Service。 AWS Lambda授予资源管理器访问索引资源的 AWS 托管策略已更新，可包括这些新的资源类型。	2023 年 3 月 7 日
IAM 最佳实践更新	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践。	2022 年 12 月 6 日
新的 AWS 托管策略	资源管理器添加 AWSResourceExplorerFullAccess AWSResourceExplorerReadOnlyAccess、和 AWSResourceExplorerServiceRolePolicy 托管策略。	2022 年 11 月 7 日
初始版本	《资源管理器用户指南》的初始版本	2022 年 11 月 7 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。