aws

用户指南

AWS Resource Access Manager

AWS Resource Access Manager: 用户指南

Table of Contents

什么是 AWS Resource Access Manager？

AWS Resource Access Manager (AWS RAM) 可帮助您跨 AWS 账户、在组织或组织单位 (OU) 内以及与 AWS Identity and Access Management (IAM) 角色和用户针对受支持资源类型安全地共享资源。如果您有多个 AWS 账户，可以一次性创建一个资源，然后使用 AWS RAM 使该资源可供其他账户使用。如果您的账户由 AWS Organizations 管理，则您可以与组织中的所有其他账户共享资源，也可以仅与一个或多个指定组织单位 (OU) 所包含的账户共享资源。您还可以根据账户 ID 与特定 AWS 账户共享，而不管该账户是否属于组织。一些支持的资源类型还允许您与指定的 IAM 角色和用户进行共享。

目录

视频概述

以下视频简要介绍了 AWS RAM 并描述了如何创建资源共享。有关更多信息，请参阅???。

以下视频演示了如何对 AWS 资源应用 AWS 托管权限。有关更多信息，请参阅???。

此视频演示如何遵循最低权限的最佳实践，创建和关联客户托管权限。有关更多信息，请参阅???。

AWS RAM 的优势

为什么要使用 AWS RAM？ 它具备下列优点：

- 减少运营开销 - 只需创建一次资源，即可使用 AWS RAM 与其他账户共享该资源。这样您就不需要在每个账户中预置重复的资源，这可以减少运营开销。在拥有资源的账户中，无需使用基于身份的权限策略，AWS RAM 即可简化向该账户中的每个角色和用户授予访问权限。

- 提供安全性和一致性 - 使用一组策略和权限，简化共享资源的安全管理。如果您要在所有单独的账户中创建重复的资源，则您的任务是实施相同的策略和权限，然后必须使所有这些账户中的策略和权限保持相同。相反，AWS RAM 资源共享的所有用户都由一组策略和权限进行管理。AWS RAM 为共享不同类型的 AWS 资源提供一致的体验。
- 提供可见性和可审核性 - 通过将 AWS RAM 与 Amazon CloudWatch 和 AWS CloudTrail 集成，查看共享资源的使用详情。借助 AWS RAM，可全面深入地了解共享资源和账户。

如何使用基于资源的策略授予跨账户访问权限？

您可以通过附加基于资源的策略来识别您 AWS 账户之外的 AWS Identity and Access Management (IAM) 主体（IAM 角色和用户），从而与其他 AWS 账户共享某些类型的 AWS 资源。但是，通过附加策略共享资源并不能利用 AWS RAM 提供的额外好处。通过使用 AWS RAM，您将获得以下功能：

- 您可以与组织或组织单位 (OU) 共享，而不必列举每个 AWS 账户 ID。
- 用户可以直接在原始 AWS 服务控制台和 API 操作中看到与他们共享的资源，就好像这些资源直接存在于用户的账户中一样。例如，如果您使用 AWS RAM 与其他账户共享 Amazon VPC 子网，则该账户中的用户可以在 Amazon VPC 控制台中以及在该账户中执行的 Amazon VPC API 操作的结果中看到该子网。通过附加基于资源的策略共享的资源不可见；相反，您必须通过其 Amazon 资源名称 (ARN) 来发现并明确引用该资源。
- 资源的所有者可以看到哪些主体有权访问他们共享的每项资源。
- 如果您与不属于您组织的账户共享资源，则 AWS RAM 会启动邀请流程。收件人必须接受邀请，然后主体才能访问共享的资源。开启组织内共享功能后，与组织中的账户共享不需要邀请。

如果您使用基于资源的权限策略共享了资源，则可以通过执行以下任一操作将这些资源提升为完全 AWS RAM 托管资源：

- 使用 PromoteResourceShareCreatedFromPolicy API 操作。
- 使用 API 操作的等效项，即 AWS Command Line Interface (AWS CLI) promote-resource-share-created-from-policy 命令。

资源共享工作原理

当您与拥有账户中的另一个 AWS 账户（使用账户）共享资源时，您将授予使用账户中的主体对共享资源的访问权限。任何适用于使用账户中的角色和用户的策略和权限也适用于共享资源。共享中的资源看起来像是您与之共享的 AWS 账户中的原生资源。

您可以共享全球资源和区域资源。有关更多信息，请参阅共享区域资源（相较于全球资源）。

共享您的资源

利用 AWS RAM，您可通过创建资源共享来共享您拥有的资源。要创建资源共享，请指定以下内容：

- 要在其中创建资源共享的 AWS 区域。在控制台右上角，从区域下拉菜单中进行选择。在AWS CLI 中，使用 `--region` 参数。
  - 资源共享只能包含与资源共享位于相同 AWS 区域的区域资源。
  - 只有当资源共享位于全球资源的指定主区域美国东部（弗吉尼亚州北部）`us-east-1` 时，资源共享才能包含全球资源。
- 资源共享的名称。
- 您希望作为此资源共享的一部分授予访问权限的资源列表。
- 授予对资源共享访问权限的主体。主体可以是单独的 AWS 账户、AWS Organizations 中组织或组织单位 (OU) 的账户，或单独的 AWS Identity and Access Management (IAM) 角色或用户。

  > **Note**
  >
  > 并非所有资源类型都可以与 IAM 角色和用户共享。有关您可以与这些主体共享的资源的信息，请参阅可共享的资源 AWS。

- 与资源共享中包含的每种资源类型相关联的托管权限。托管权限决定了其他账户中的主体可以对资源共享中的资源执行哪些操作。

  权限的行为取决于主体的类型：

  - 如果主体所在的账户与拥有资源的账户不同，则附加到资源共享的权限是这些账户中的角色和用户可获得的最大权限。然后，这些账户的管理员必须使用基于 IAM 身份的策略向个人角色和用户授予对共享资源的访问权限。在这些策略中授予的权限不能超过附加到资源共享的权限中定义的权限。

资源拥有账户保留其共享资源的全部所有权。

使用共享资源

当资源的所有者将资源与您的账户共享时，您可以访问共享资源，就像该资源为您的账户所拥有一样。您可以使用相关服务的控制台、AWS CLI 命令和 API 操作来访问资源。允许您账户中的主体执行的

API 操作因资源类型而异，并由附加到资源共享的 AWS RAM 权限指定。此外，所有 IAM 策略以及在您的账户中配置的服务控制策略将继续适用，这使您能够利用在安全性和管理控制方面的现有投资。

当您使用该资源的服务访问共享资源时，您具有与拥有该资源的 AWS 账户相同的能力和限制。

- 如果资源是区域性资源，则您只能从其所属账户中存在的 AWS 区域访问它。
- 如果资源是全球性资源，则可以从该资源的服务控制台和工具支持的任何 AWS 区域访问它。您只能在指定的主区域美国东部（弗吉尼亚州北部）`us-east-1` 的 AWS RAM 控制台和工具中，查看和管理资源共享及其全球资源。

访问 AWS RAM

您可以通过以下任何方式使用 AWS RAM:

AWS RAM 控制台

AWS RAM 提供基于 Web 的用户界面，即 AWS RAM 控制台。如果您已注册 AWS 账户，可以通过登录 AWS Management Console并从控制台主页选择 AWS RAM，访问 AWS RAM 控制台。

您也可以在浏览器中直接导航到 AWS RAM 控制台。如果您尚未登录，则系统会要求您在控制台出现之前登录。

AWS CLI 和 Tools for Windows PowerShell

AWS CLI 和 AWS Tools for PowerShell 提供对 AWS RAM 公共 API 操作的直接访问权限。AWS 在 Windows、macOS 和 Linux 上支持这些工具。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 AWS RAM 命令的更多信息，请参阅 AWS CLI 命令参考或 AWS Tools for Windows PowerShell Cmdlet 参考。

AWS 软件开发工具包

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 软件开发工具包和工具参考指南。

查询 API

如果您不使用支持的编程语言之一，则 AWS RAM HTTPS 查询 API 将为您提供对 AWS RAM 和 AWS 的编程访问权限。借助 AWS RAM API，您可以直接向服务发出 HTTPS 请求。当您使用 AWS RAM API 时，必须添加代码，才能使用您的凭证对请求进行数字化签名。有关详细信息，请参阅 AWS RAM API 参考。

AWS RAM 定价

使用 AWS RAM 或创建资源共享并跨账户共享您的资源不额外收费。资源使用费因资源类型而异。有关 AWS 如何对可共享资源计费的更多信息，请参阅资源所属服务的文档。

合规性和国际标准

PCI DSS

AWS RAM 支持由商家或服务提供商处理、存储和传输信用卡数据，而且已经验证符合支付卡行业 (PCI) 数据安全标准 (DSS)。

有关 PCI DSS 的更多信息，包括如何请求 AWS PCI Compliance Package 的副本，请参阅 PCI DSS 第 1 级。

FedRAMP

AWS RAM 在以下 AWS 区域被授权为 FedRAMP 中等：美国东部（弗吉尼亚州北部）、美国东部（俄亥俄州）、美国西部（北加利福尼亚）和美国西部（俄勒冈州）。

AWS RAM 在以下 AWS 区域被授权为 FedRAMP 高：AWS GovCloud（美国西部）和 AWS GovCloud（美国东部）。

联邦风险与授权管理计划 (FedRAMP) 是一项美国政府层面的计划，它提供一种标准方法来对云产品和云服务进行安全性评估、授权以及持续监控。

有关 FedRAMP 合规性的更多信息，请参阅 FedRAMP。

SOC 和 ISO

AWS RAM 可用于符合以下要求的工作负载：服务组织控制 (SOC) 合规性和国际标准化组织 (ISO) ISO 9001、ISO 27001、ISO 27017、ISO 27018 和 ISO 27701 标准。金融、医疗保健和其他监管行业的客户可以深入了解保护客户数据的安全流程和控制措施，这些信息可通过 AWS Artifact 在 SOC 报告以及 AWS ISO 和 CSA STAR 证书中找到。

有关 SOC 合规性的更多信息，请参阅 SOC。

有关 ISO 合规性的更多信息，请参阅 ISO 9001、ISO 27001、ISO 27017、ISO 27018 和 ISO 27701。

AWS RAM 入门

使用 AWS Resource Access Manager，您可以与其他各 AWS 账户共享您拥有的资源。如果您的账户由 AWS Organizations 管理，您也可以与组织中的其他账户共享资源。您还可以使用通过其他 AWS 账户与您共享的资源。

如果您未启用 AWS Organizations 内的共享，则无法与您的组织或组织中的组织单位 (OU) 共享资源。但是，您仍可以与组织中的各 AWS 账户共享资源。对于支持的资源类型，您还可以与组织中的各 AWS Identity and Access Management (IAM) 角色或用户共享资源。在这种情况下，这些主体被视为外部账户，而不是您组织的一部分。他们会收到加入资源共享的邀请，且必须接受邀请后才能访问共享资源。

目录

的术语和概念 AWS RAM

以下概念有助于解释如何使用 AWS Resource Access Manager (AWS RAM) 共享资源。

资源共享

您可以 AWS RAM 通过创建资源共享来使用共享资源。资源共享包含以下三个要素：

- 要共享的一个或多个 AWS 资源的列表。
- 要向其授予资源访问权限的一个或多个主体的列表。
- 共享中包含的每种资源的托管权限。每项托管权限适用于该资源共享中该类型的所有资源。

在您使用创建资源共享之后，可以 AWS RAM 向在资源共享中指定的委托人授予访问该共享资源的权限。

- 如果您开启与 AWS RAM 共享 AWS Organizations，并且您与之共享的委托人与共享账户属于同一个组织，则只要他们的账户管理员使用 AWS Identity and Access Management (IAM) 权限策略向他们授予使用资源的权限，这些委托人就可以获得访问权限。

- 如果您未开启与 Or AWS RAM ganizations 共享，您仍然可以与组织中的个人 AWS 账户 共享资源。使用账户中的管理员会收到加入资源共享的邀请，且他们必须接受邀请，然后资源共享中指定的主体才能访问共享的资源。
- 如果资源类型支持，您也可以与组织外部的账户共享。使用账户中的管理员会收到加入资源共享的邀请，且他们必须接受邀请，然后资源共享中指定的主体才能访问共享的资源。有关哪些资源类型支持此类共享的信息，请参阅可共享的资源 AWS，并查看可以与其组织之外的账户共享列。

共享账户

共享帐户包含共享的资源， AWS RAM 管理员使用在其中创建 AWS 资源共享 AWS RAM。

AWS RAM 管理员是拥有在中创建和配置资源共享权限的IAM委托人 AWS 账户。由于通过将基于资源的策略附加到资源共享中的资源来起 AWS RAM 作用，因此 AWS RAM 管理员还必须有权对资源共享中包含 AWS 服务 的每种资源类型调用`PutResourcePolicy`操作。

使用主体

消费账户是 AWS 账户 共享资源的账户。资源共享可以将整个账户指定为主体，或者对于某些资源类型，可以指定账户中的单个角色或用户。有关哪些资源类型支持此类共享的信息，请参阅可共享的资源 AWS并查看 “可以与IAM角色和用户共享” 列。

AWS RAM 还支持服务主体作为资源共享的使用者。有关哪些资源类型支持此类共享的信息，请参阅可共享的资源 AWS，并查看可以与服务主体共享列。

使用账户中的主体只能执行以下两个 权限所允许的操作：

- 附加到资源共享的托管权限。它们指定了可以向使用账户中的主体授予的最大 权限。
- IAM管理员在使用者账户中附加到个人角色或用户的IAM基于身份的策略。这些策略必须授予`Allow`访问指定操作和共享账户中资源的 Amazon 资源名称 (ARN) 的权限。

AWS RAM 支持以下IAM主体类型作为资源共享的使用者：

- 另一个 AWS 账户 — 资源共享使共享账户中包含的资源可供使用者账户使用。
- 个人IAM角色或其他账户中的用户-某些资源类型支持直接与个人IAM角色或用户共享。按其指定此主体类型ARN。
  - IAM角色 — `arn:aws:iam::123456789012:role/rolename`
  - IAM用户 — `arn:aws:iam::123456789012:user/username`

- 服务主体-与 AWS 服务共享资源以授予该服务对资源共享的访问权限。服务主体共享允许 AWS 服务代表您采取行动，以减轻运营负担。

  要与服务主体共享，请选择允许与任何人共享，然后，在选择主体类型下，从下拉列表中选择服务主体。采用以下格式指定服务主体的名称：

  - *service-id*.amazonaws.com

  为了降低混淆代理人带来的风险，资源策略在 aws:SourceAccount 条件键中显示资源所有者的账户 ID。

- 组织中的帐户-如果共享帐户由管理 AWS Organizations，则资源共享可以指定要与组织中的所有帐户共享的组织 ID。资源共享也可以指定组织单位（OU）ID，以便与该 OU 中的所有账户共享。共享账户只能与自己的组织或其组织IDs内部的 OU 共享。按组织或 OU 指定组织中的帐户。ARN

  - 组织中的所有账户 — 以下是组织ARN中的一个示例 AWS Organizations：

    ```
    arn:aws:organizations::123456789012:organization/o-<orgid>
    ```

  - 组织单位中的所有账户 — 以下是 OU ID ARN 的示例：

    ```
    arn:aws:organizations::123456789012:organization/o-<orgid>/ou-<rootid>-<ouid>
    ```

> **Important**
>
> 当您与组织或 OU 共享，并且该范围包括拥有资源共享的账户时，共享账户中的所有主体都会自动获得对共享中资源的访问权限。授予的访问权限由与共享关联的托管权限定义。这是因为 AWS RAM 附加到共享中每个资源的基于资源的策略使用"Principal": "*"。有关更多信息，请参阅 使用的含义 "Principal": "*" 在基于资源的政策中。
> 其他所使用账户中的主体无法立即访问共享的资源。其他账户的管理员必须首先将基于身份的权限策略附加到相应的主体。这些策略必须授予ARNs对资源共享中各个资源的Allow访问权限。这些策略中的权限不能超过与资源共享关联的托管权限中指定的权限。

基于资源的策略

基于资源的策略是实现IAM策略语言的JSON文本文档。与您附加到委托人（例如IAM角色或用户）的基于身份的策略不同，您可以将基于资源的策略附加到资源。 AWS RAM 根据您为资源共享提供的信息，代表您制定基于资源的策略。您必须指定一个 Principal 策略元素来确定谁可以访问该资源。有关更多信息，请参阅《用户指南》中的基于身份的策略和基于资源的策略。IAM

将对生成的 AWS RAM 基于资源的策略以及所有其他IAM策略类型进行评估。这包括附加到尝试访问资源的委托人的任何IAM基于身份的策略，以及可能适用于该资源的服务控制策略 (SCPs)。 AWS Organizations AWS 账户由 AWS RAM 参与生成的基于资源的策略与所有其他IAM策略采用相同的策略评估逻辑。有关策略评估以及如何确定生成的权限的完整详细信息，请参阅《IAM用户指南》中的策略评估逻辑。

AWS RAM 通过提供基于 easy-to-use抽象资源的策略，提供简单安全的资源共享体验。

对于支持基于资源的策略的资源类型， AWS RAM 会自动为您构建和管理基于资源的策略。对于给定资源， AWS RAM 通过组合包含资源的所有资源共享中的信息，构建基于该资源的策略。例如，假设您通过使用 AWS RAM 并包含在两个不同的资源共享中共享的 SageMaker Amazon AI 管道。您可以使用一个资源共享为整个组织提供只读访问权限。然后，您可以使用其他资源共享仅向单个账户授予 SageMaker AI 执行权限。 AWS RAM 自动将这两组不同的权限组合成一个包含多个语句的资源策略。然后，它将组合的基于资源的策略附加到管道资源。您可以通过调用来查看此基础资源策略 GetResourcePolicy操作。 AWS 服务 然后使用该基于资源的策略来授权任何试图对共享资源执行操作的委托人。

尽管您可以手动创建基于资源的策略并通过调用 `PutResourcePolicy` 将其附加到您的资源，但我们建议您使用 AWS RAM ，因为它具有以下优点：

- 共享使用者的可发现性-如果您通过使用共享资源 AWS RAM，则用户可以直接在资源拥有服务的控制台和API操作中看到与他们共享的所有资源，就像这些资源直接存在于用户的账户中一样。例如，如果您与其他账户共享一个 AWS CodeBuild 项目，则使用者账户中的用户可以在 CodeBuild 控制台和所执行 CodeBuild API操作的结果中看到该项目。通过直接附加基于资源的策略共享的资源不可见。相反，您必须通过其发现资源并明确引用该资源ARN。
- 共享所有者的可管理性-如果您通过使用共享资源 AWS RAM，则共享账户中的资源所有者可以集中查看哪些其他账户有权访问其资源。如果您使用基于资源的策略共享资源，则只能通过在相关的服务控制台或API中查看各个资源的策略来查看使用账户。
- 效率 — 如果您通过使用共享资源 AWS RAM，则可以共享多个资源并将其作为一个单元进行管理。仅使用基于资源的策略共享的资源需要在您共享的每个资源上附加单独的策略。
- 简单 — 有了它 AWS RAM，您无需了解JSON基于IAM策略的语言。 AWS RAM 提供 ready-to-use AWS 托管权限，您可以选择将其附加到资源共享。

通过使用 AWS RAM，您甚至可以共享一些尚不支持基于资源的策略的资源类型。对于此类资源类型，会 AWS RAM 自动生成一个基于资源的策略来表示实际权限。用户可以通过致电查看此表示形式 GetResourcePolicy。 这包括以下资源类型：

- Amazon Aurora - DB 集群

- Amazon EC2 — 容量预留和专用主机
- AWS License Manager — 许可证配置
- AWS Outposts — 本地网关路由表、前哨基地和站点
- Amazon Route 53 - 转发规则
- Amazon Virtual Private Cloud — 客户拥有IPv4的地址、前缀列表、子网、流量镜像目标、传输网关和传输网关组播域

AWS RAM 生成的基于资源的策略示例

如果您与个人账户共享 Image Builder EC2 图像资源，则 AWS RAM 会生成如下例所示的策略，并将其附加到资源共享中包含的所有图像资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages",
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
        }
    ]
}
```

如果您与其他IAM角色或用户共享 Image Builder EC2 图像资源 AWS 账户，则 AWS RAM 会生成如下例所示的策略，并将其附加到资源共享中包含的所有图像资源。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/MySampleRole"
      },
```

```
      "Action": [
          "imagebuilder:GetImage",
          "imagebuilder:ListImages",
      ],
      "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
    }
  ]
}
```

如果您与组织中的所有账户或组织中的账户共享 Image Builder EC2 图像资源，则 AWS RAM 会生成如下例所示的策略，并将其附加到资源共享中包含的所有图像资源。

> **Note**
>
> 此策略使用 "Principal": "*"，然后使用 "Condition" 元素将权限限制为与指定 PrincipalOrgID 相匹配的身份。有关更多信息，请参阅 使用的含义 "Principal": "*" 在基于资源的政策中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages",
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-123456789"
                }
            }
        }
    ]
}
```

使用的含义 "Principal": "*" 在基于资源的政策中

当您在基于资源的策略"Principal": "*"中加入时，该策略会向包含该资源的账户中的所有IAM委托人授予访问权限，但须遵守Condition元素施加的任何限制（如果存在）。适用于调用主体的任何策略中的明确 Deny 语句将覆盖此策略授予的权限。但是，在任何适用的身份策略、权限边界策略或会话策略中，隐式 Deny（意味着缺少显式 Allow）不会 导致对由此类基于资源的策略授予对操作访问权限的主体进行 Deny。

如果您的场景不希望出现这种行为，则您可以通过向影响相关角色和用户的身份策略、权限边界或会话策略添加显式 Deny 语句，限制这种行为。

托管权限

托管权限定义了主体可以在哪些条件下对资源共享中支持的资源类型执行哪些操作。创建资源共享时，您必须指定要对资源共享中包含的每种资源类型使用哪种托管权限。托管权限列出了委托人可以使用AWS RAM共享的资源执行的一组actions和条件。

您只能为资源共享中的每种资源类型附加一个托管权限。如果某个类型的某些资源使用一种托管权限，而相同类型的其他资源使用不同的托管权限，则无法创建资源共享。为此，您需要创建两个不同的资源共享并在它们之间分配资源，以便为每个资源集提供不同的托管权限。有两种不同类型的托管权限：

AWS 托管权限

AWS 托管权限由常见客户场景创建、维护 AWS 和授予权限。 AWS RAM 为每种支持的资源类型定义至少一个 AWS 托管权限。某些资源类型支持多个 AWS 托管权限，其中一个托管权限被指定为 AWS 默认权限。除非您另行指定，否则将关联默认 AWS 托管权限。

客户托管权限

客户托管权限是您通过精确指定可以在哪些条件下使用 AWS RAM共享的资源执行哪些操作来创建和维护的托管权限。例如，您想限制您VPC的 Amazon IP 地址管理器 (IPAM) 池的读取权限，这有助于您大规模管理 IP 地址。您可以为开发人员创建客户托管权限来分配 IP 地址，但不能查看其他开发人员账户分配的 IP 地址范围。您可以遵循最低权限相关的最佳实践，仅授予在共享资源上执行任务所需的权限。

您可以为资源共享中的资源类型定义自己的权限，并可以选择添加诸如全局上下文键和服务特定键之类的条件，以指定主体访问资源的条件。这些权限可以在一个或多个 AWS RAM 共享中使用。客户托管权限为区域特定权限。

AWS RAM 将托管权限作为输入，为您共享的资源制定基于资源的策略。

托管权限版本

对托管权限的任何更改都表示为该托管权限的新版本。新版本是所有新资源共享的默认版本。每个托管权限始终有一个指定为默认版本的版本。当您或 AWS 创建新的托管权限版本时，必须明确更新每个现有资源共享的托管权限。在此步骤中，您可以先评估更改，然后再将其应用于您的资源共享。所有新的资源共享将自动使用相应资源类型的新版托管权限。

AWS 托管权限版本

AWS 处理对 AWS 托管权限的所有更改。此类更改可解决新功能或消除已发现的缺点。您只能将默认托管权限版本应用于您的资源共享。

客户托管权限版本

您负责处理对客户托管权限的所有更改。您可以创建新的默认版本，将旧版本设置为默认版本，或者删除不再与任何资源共享关联的版本。一个客户托管权限最多可以有五个版本。

创建或更新资源共享时，只能附加指定托管权限的默认版本。有关更多信息，请参阅 将 AWS 托管权限更新到较新版本。

共享您的 AWS 资源

要使用共享您拥有的资源 AWS RAM，请执行以下操作：

- 在 AWS Organizations中启用资源共享（可选）
- 创建资源共享

> **注意**
>
> - 与拥有 AWS 账户 该资源的以外的委托人共享资源不会更改适用于创建该资源的账户内的资源权限或配额。
> - AWS RAM 是一项区域服务。您与之共享的委托人只能访问创建资源共享时 AWS 区域 所在的资源共享。
> - 有些资源在共享方面有特殊的注意事项和先决条件。有关更多信息，请参阅 可共享的资源 AWS。

在 AWS Organizations中启用资源共享

当您的账户由管理时 AWS Organizations，您可以利用这一优势更轻松地共享资源。无论是否使用 Organizations，用户都可以与个人账户共享。但是，如果您的账户位于组织中，则您可以与个人账户、组织或 OU 中的所有账户共享，而不必枚举每个账户。

要在组织内共享资源，必须先使用 AWS RAM 控制台或 AWS Command Line Interface (AWS CLI) 启用与共享 AWS Organizations。当您在组织中共享资源时， AWS RAM 不会向委托人发送邀请。企业中的委托人获取对共享资源的访问权限，而无需交换邀请。

当您在组织内启用资源共享时， AWS RAM 会创建一个名**AWSServiceRoleForResourceAccessManager**为的服务相关角色。此角色只能由 AWS RAM 服务担任，并授予使用 AWS 托管策略检索有关其所属组织的信息的 AWS RAM 权限`AWSResourceAccessManagerServiceRolePolicy`。

如果您不再需要与整个组织共享资源OUs，或者可以禁用资源共享。有关更多信息，请参阅 禁用与 AWS Organizations 的资源共享。

最小权限

要运行以下步骤，您必须以拥有以下权限的组织管理账户中的主体身份登录：

- `ram:EnableSharingWithAwsOrganization`
- `iam:CreateServiceLinkedRole`
- `organizations:enableAWSServiceAccess`
- `organizations:DescribeOrganization`

要求

- 只有在组织管理账户中以主体身份登录时，才能执行这些步骤。
- 组织必须已启用所有功能。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。

> **Important**
>
> 您必须使用 AWS RAM 控制台或 enable-sharing-with-aws- organization AWS CLI 命令启用与 AWS Organizations 共享。这将确保创建与

AWSServiceRoleForResourceAccessManager 服务相关角色。如果您使用 AWS Organizations 控制台或 enable-aws-service-access AWS CLI 命令启用可信访问，则不会创建AWSServiceRoleForResourceAccessManager服务相关角色，也无法在组织内共享资源。 AWS Organizations

Console

要在组织内启用资源共享，请执行以下操作：

1. 在 AWS RAM 控制台中打开 “设置” 页面。
2. 选择 “启用与之共享” AWS Organizations，然后选择 “保存设置”。

AWS CLI

要在组织内启用资源共享，请执行以下操作：

使用 enable-sharing-with-aws-组织命令。

此命令可以在任何区域中使用 AWS 区域，并且允许 AWS Organizations 在所有支持的区域中 AWS RAM 与共享。

```
$ aws ram enable-sharing-with-aws-organization
{
    "returnValue": true
}
```

创建资源共享

要共享您拥有的资源，请创建资源共享。过程概览：

1. 添加您要共享的资源。
2. 对于共享中包含的每种资源类型，请指定要用于该资源类型的托管权限。
   - 您可以选择可用的 AWS 托管权限、现有客户托管权限或创建新的客户托管权限。
   - AWS 托管权限由创建 AWS ，以涵盖标准用例。
   - 客户托管权限允许您定制自己的托管权限，以满足您的安全和业务需求。

> **Note**
>
> 如果选定的托管权限有多个版本，则 AWS RAM 会自动附加默认版本。您只能 附加指定为默认版本的版本。

3. 指定要对资源拥有访问权限的主体。

注意事项

- 如果您以后需要删除共享中包含的 AWS 资源，我们建议您先从包含该资源的任何资源共享中移除该资源，或者删除该资源共享。
- 您可以在资源共享中包含的资源类型列在了可共享的资源 AWS中。
- 仅当您拥有某个资源时，您才可以共享此资源。您无法共享与您共享的资源。
- AWS RAM 是一项区域服务。当您与其他 AWS 账户中的主体共享资源时，这些主体必须从创建每个资源时所在的 AWS 区域 访问这些资源。对于支持的全局资源，您可以从 AWS 区域 该资源的服务控制台和工具支持的任何资源访问这些资源。您只能在指定的主区域美国东部（弗吉尼亚州北部）us-east-1 的 AWS RAM 控制台和工具中，查看此类资源共享及其全球资源。有关 AWS RAM 和全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。
- 如果您共享的账户是组织中组织的一员， AWS Organizations 并且启用了在组织内共享，那么与您共享的组织中的任何委托人将自动获得访问资源共享的权限，而无需使用邀请。您在组织环境之外与之共享的账户中的主体会收到加入资源共享的邀请，并且只有在他们接受邀请后才能获得对所共享资源的访问权限。
- 如果您与服务主体共享，则无法将任何其他主体与该资源共享关联。
- 如果共享是在属于某个组织的账户或主体之间进行的，则组织成员资格的任何更改都会动态影响对资源共享的访问权限。
  - 如果您 AWS 账户 向组织或有权访问资源共享的 OU 中添加，则该新成员账户将自动获得对资源共享的访问权限。然后，您与之共享的账户的管理员 可以授予该账户中的个人主体访问该共享中的资源的权限。
  - 如果您从组织或有权访问资源共享的 OU 中移除某个账户，则该账户中的所有主体将自动失去对通过该资源共享访问的资源的访问权限。
  - 如果您直接与成员账户或成员账户中的IAM角色或用户共享，然后将该账户从组织中移除，则该账户中的任何委托人将无法访问通过该资源共享访问的资源。

> **Important**
>
> 当您与组织或 OU 共享，并且该范围包括拥有资源共享的账户时，共享账户中的所有主体都会自动获得对共享中资源的访问权限。授予的访问权限由与共享关联的托管权限定义。这是因为 AWS RAM 附加到共享中每个资源的基于资源的策略使用`"Principal": "*"`。有关更多信息，请参阅 使用的含义 "Principal": "*" 在基于资源的政策中。
> 其他所使用账户中的主体无法立即访问共享的资源。其他账户的管理员必须首先将基于身份的权限策略附加到相应的主体。这些策略必须授予ARNs对资源共享中各个资源的`Allow`访问权限。这些策略中的权限不能超过与资源共享关联的托管权限中指定的权限。

- 您只能将您的账户所属的组织以及OUs该组织添加到您的资源共享中。您不能将组织外部的组织作为委托人添加到OUs资源共享中。但是，对于支持的服务，您可以将组织外部的个人 AWS 账户 IAM角色和用户添加为资源共享的委托人。

> **Note**
>
> 并非所有资源类型都可以与IAM角色和用户共享。有关您可以与这些主体共享的资源的信息，请参阅可共享的资源 AWS。

- 对于以下资源类型，您有七天的时间接受邀请加入以下资源类型的共享。如果您在邀请到期之前未接受邀请，则系统会自动拒绝邀请。

> **Important**
>
> 对于不 在以下列表中的共享资源类型，您有 12 小时的时间 接受加入资源共享的邀请。12 小时后，邀请过期，资源共享中的最终用户主体将解除关联。最终用户无法再接受邀请。

  - Amazon Aurora - DB 集群
  - Amazon EC2 — 容量预留和专用主机
  - AWS License Manager — 许可证配置
  - AWS Outposts — 本地网关路由表、前哨基地和站点
  - Amazon Route 53 - 转发规则
  - Amazon VPC — 客户拥有IPv4的地址、前缀列表、子网、流量镜像目标、中转网关、中转网关组播域

Console

要创建资源共享，请执行以下操作：

1. 打开AWS RAM 控制台。
2. 由于 AWS RAM 资源共享是特定的 AWS 区域，因此请 AWS 区域 从控制台右上角的下拉列表中选择相应的资源共享。要查看包含全球资源的资源共享，必须将设置 AWS 区域 为美国东部（弗吉尼亚北部）、(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。如果要在资源共享中包含全球资源，则必须选择指定的主区域，即美国东部（弗吉尼亚州北部）us-east-1。
3. 如果您不熟悉 AWS RAM，请从主页上选择 “创建资源共享”。否则，请从由我共享：资源共享页面选择创建资源共享。
4. 在步骤 1：指定资源共享详细信息中，执行以下操作：

   a. 对于名称，键入资源共享的描述性名称。

   b. 在资源下，选择要添加到资源共享的资源，如下所示：

      - 对于选择资源类型，选择要共享的资源的类型。这会将可共享资源的列表筛选为仅所选类型的资源。
      - 在生成的资源列表中，选中要共享的各个资源旁边的复选框。所选资源将移至选定资源下。

        如果您要共享与特定可用区关联的资源，则使用可用区 ID（AZ ID）可帮助您跨账户确定这些资源的相对位置。有关更多信息，请参阅 AWS 资源的可用区 ID。

   c. （可选）要将标签附加到资源共享，请在标签下输入标签键和值。通过选择添加新标签，添加其他标签。根据需要重复上述步骤。这些标签仅适用于资源共享本身，不适用于资源共享中的资源。
5. 选择下一步。
6. 在步骤 2：将托管权限与每种资源类型关联中，您可以选择将创建的托管权限 AWS 与资源类型相关联，选择现有的客户托管权限，也可以为支持的资源类型创建自己的客户托管权限。有关更多信息，请参阅 托管权限的类型。

   选择创建客户托管权限，以构建符合共享使用案例要求的客户托管权限。有关更多信息，请参阅创建客户托管权限。完成该过程后，选择

   ，

   然后您可以从托管权限下拉列表中选择新的客户托管权限。

> **Note**
>
> 如果选定的托管权限有多个版本，则 AWS RAM 会自动附加默认版本。您只能 附加指定为默认版本的版本。

要显示托管权限允许的操作，请展开查看该托管权限的策略模板。

7. 选择下一步。
8. 在步骤 3：向主体授予访问权限中，执行以下操作：

   a. 默认情况下，“允许与任何人共享” 处于选中状态，这意味着，对于支持共享的资源类型，您可以与 AWS 账户 组织外部的资源共享资源。这不会影响只能在组织内部共享的资源类型，例如 Amazon VPC 子网。您还可以与IAM角色和用户共享一些支持的资源类型。

   要将资源共享限制为仅组织中的账户和主体，请选择仅允许在组织内共享。

   b. 对于主体，请执行以下操作：

   - 要添加组织、组织单位 (OU) 或组织的一部分 AWS 账户 ，请打开 “显示组织结构”。这将显示组织的树视图。然后，选中要添加的每个委托人旁边的复选框。

     > **Important**
     >
     > 当您与组织或 OU 共享，并且该范围包括拥有资源共享的账户时，共享账户中的所有主体都会自动获得对共享中资源的访问权限。授予的访问权限由与共享关联的托管权限定义。这是因为 AWS RAM 附加到共享中每个资源的基于资源的策略使用`"Principal": "*"`。有关更多信息，请参阅 使用的含义 "Principal": "*" 在基于资源的政策中。
     > 其他所使用账户中的主体无法立即访问共享的资源。其他账户的管理员必须首先将基于身份的权限策略附加到相应的主体。这些策略必须授予ARNs对资源共享中各个资源的`Allow`访问权限。这些策略中的权限不能超过与资源共享关联的托管权限中指定的权限。

   - 如果您选择组织（ID 以 o- 开头），则组织中所有 AWS 账户 的主体都可以访问资源共享。

- 如果您选择一个 OU（ID 以开头ou-），则该 OU AWS 账户 中的所有委托人及其子级OUs都可以访问该资源共享。
- 如果您选择个人 AWS 账户，则只有该账户中的委托人才能访问资源共享。

> **Note**
>
> 仅当启用与 AWS Organizations 的共享功能并且您已登录到该组织的管理账户时，才会显示显示组织结构切换开关。
> 您不能使用此方法来指定组织 AWS 账户 外部人员、IAM角色或用户。相反，您必须关闭 “显示组织结构”，然后使用下拉列表和文本框输入 ID 或ARN。

- 要通过 ID 指定委托人ARN，或者包括组织外部的委托人，请为每位委托人选择委托人类型。接下来，输入 ID（对于 AWS 账户、组织或 OU）或ARN（IAM角色或用户），然后选择 “添加”。可用的主体类型、ID 和ARN格式如下所示：
  - AWS 账户— 要添加 AWS 账户，请输入 12 位数的账户 ID。例如：

    ```
    123456789012
    ```

  - 组织-要添加组织 AWS 账户 中的所有组织，请输入组织的 ID。例如：

    ```
    o-abcd1234
    ```

  - 组织单位（OU）- 要添加 OU，请输入 OU 的 ID。例如：

    ```
    ou-abcd-1234efgh
    ```

  - IAM角色-要添加IAM角色，请输入ARN该角色的。使用以下语法：

    ```
    arn:partition:iam::account:role/role-name
    ```

    例如：

    ```
    arn:aws:iam::123456789012:role/MyS3AccessRole
    ```

    > **Note**
    >
    > 要获取IAM角色ARN的唯一性，请在IAM控制台中查看角色列表，使用 get-role AWS CLI 命令或操作。GetRoleAPI

  - IAM用户-要添加IAM用户，请输入ARN该用户的。使用以下语法：

```
arn:partition:iam::account:user/user-name
```

例如：

```
arn:aws:iam::123456789012:user/bob
```

> **Note**
>
> 要获取IAM用户的唯一ARN值，请在IAM控制台中查看用户列表，使用 get-user AWS CLI 命令，或者 GetUserAPI行动。

- 服务主体 - 要添加服务主体，请从选择主体类型下拉列表中选择服务主体。输入 AWS 服务主体的名称。使用以下语法：
  - `service-id.amazonaws.com`

  例如：

  ```
  pca-connector-ad.amazonaws.com
  ```

c. 对于所选的主体，请验证您指定的主体是否显示在列表中。

9. 选择下一步。
10. 在步骤 4：查看和创建中，查看资源共享的配置详细信息。要更改任何步骤的配置，请选择与您要返回的步骤对应的链接，然后进行所需的更改。
11. 查看完资源共享后，选择创建资源共享。

    可能需要花几分钟时间，才能完成资源和委托人关联。在尝试使用资源共享之前，允许此过程完成。
12. 您可以随时添加和删除资源与主体，或将自定义标签应用于资源共享。您可以更改资源共享中包含的资源类型的托管权限，以及支持超过默认托管权限的资源类型的托管权限。您不再希望共享资源时，可以将其删除。有关更多信息，请参阅 共享您拥有的 AWS 资源。

AWS CLI

要创建资源共享，请执行以下操作：

使用 create-resource-share命令。以下命令创建与组织 AWS 账户 中的所有人共享的资源共享。该共享包含 AWS License Manager 许可证配置，并授予该资源类型的默认托管权限。

> **Note**
>
> 如果您想将客户托管权限与该资源共享中的资源类型一起使用，则可以使用现有的客户托管权限，也可以创建新的客户托管权限。记下ARN客户的托管权限，然后创建资源共享。有关更多信息，请参阅 创建客户托管权限。

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

使用共享 AWS 资源

要开始使用通过 AWS Resource Access Manager 与您的账户共享的资源，请完成以下任务。

任务

- 回复资源共享邀请
- 使用与您共享的资源

回复资源共享邀请

如果您收到加入资源共享的邀请，您必须接受它才能访问共享资源。

以下情形不使用邀请：

- 如果您是 AWS Organizations 中组织的一部分，且已在您的组织中启用共享，则组织中的主体将自动获得对共享资源的访问权限，而不会收到这些邀请。
- 如果您与拥有资源的 AWS 账户共享，则该账户中的主体无需邀请即可自动访问共享资源。

Console

要响应邀请，请执行以下操作：

1. 在 AWS RAM 控制台中，打开与我共享：资源共享页面。

   > **Note**
   >
   > 资源共享仅在创建资源共享的 AWS 区域可见。如果控制台未显示预期的资源共享，则您可能需要使用右上角的下拉控件切换到其他 AWS 区域。

2. 查看您已获得访问权限的资源共享列表。

   状态列显示您当前对资源共享的参与状态。Pending 状态表示您已被添加到资源共享，但尚未接受或拒绝邀请。

3. 要回复资源共享邀请，请选择资源共享 ID，然后选择接受资源共享以接受邀请，或者选择拒绝资源共享以拒绝邀请。如果您拒绝邀请，则无法访问资源。如果您接受邀请，则可以访问资源。

AWS CLI

首先，获取可供您使用的资源共享邀请的列表。以下示例命令在 us-west-2 区域中运行，显示 PENDING 状态下有一个资源共享可用。

```
$ aws ram get-resource-share-invitations
{
    "resourceShareInvitations": [
        {
```

```
            "resourceShareInvitationArn": "arn:aws:ram:us-
west-2:111122223333:resource-share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
            "resourceShareName": "MyNewResourceShare",
            "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
            "senderAccountId": "111122223333",
            "receiverAccountId": "444455556666",
            "invitationTimestamp": "2021-09-15T15:00:32.568000-07:00",
            "status": "PENDING"
        }
    ]
}
```

您可以使用上一个命令中邀请的 Amazon 资源名称 (ARN) 作为下一个命令中的参数来接受该邀请。

```
$ aws ram accept-resource-share-invitation \
    --resource-share-invitation-arn arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
        "resourceShareName": "MyNewResourceShare",
        "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
        "senderAccountId": "111122223333",
        "receiverAccountId": "444455556666",
        "invitationTimestamp": "2021-09-15T15:14:12.580000-07:00",
        "status": "ACCEPTED"
    }
}
```

输出显示 `status` 已更改为 ACCEPTED。该资源共享中包含的资源现在可供接受账户中的主体使用。

使用与您共享的资源

在您接受加入资源共享的邀请后，您可以对共享资源执行特定的操作。这些操作因资源类型而异。有关更多信息，请参阅可共享的资源 AWS。这些资源可直接在每个资源的服务控制台和 API/CLI 操作中使用。如果资源是区域性资源，则您必须在服务控制台或 API/CLI 命令中使用正确的 AWS 区域。如果资

源是全球性资源，则您必须使用指定的主区域美国东部（弗吉尼亚州北部）us-east-1。要查看 AWS RAM 中的资源，您必须打开创建资源共享所在 AWS 区域的 AWS RAM 控制台。

使用共享 AWS 资源

您可以使用 AWS Resource Access Manager (AWS RAM) 共享您拥有的 AWS 资源和访问与您共享的 AWS 资源。

目录

共享区域资源（相较于全球资源）

本主题将讨论 AWS Resource Access Manager (AWS RAM) 处理区域资源和全球资源方式的差异。

资源要么是区域资源，要么是全球资源。您可以使用 Amazon 资源名称 (ARN) 中的第四个字段来识别资源是区域资源还是全球资源。区域资源显示 AWS 区域。如果为空，则表明资源为全球资源。

区域资源和全球资源有什么区别？

区域资源

您可以与 AWS RAM 共享的大多数资源都是区域资源。您在指定 AWS 区域中创建它们，然后它们就存在于该区域中。要查看这些资源或与之交互，您必须将操作定向到该区域。例如，要使用 AWS Management Console创建 Amazon Elastic Compute Cloud (Amazon EC2) 实例，您应选择要创建实例的 AWS 区域。如果您使用 AWS Command Line Interface (AWS CLI) 创建实例，则需要包含 `--region` 参数。每个 AWS SDK 都有自己的等效机制来指定操作所用的区域。

使用区域资源有几个原因。一个不错的原因是，要确保资源以及您用来访问资源的服务端点尽可能靠近客户。这样可通过最大限度减少延迟来提高性能。另一个原因是为了提供隔离边界。这样，您可以在多个区域中创建独立的资源副本，以分配负载并提高可扩展性。同时，它可以将资源相互隔离，以提高可用性。

如果您在控制台或 AWS CLI 命令中指定不同的 AWS 区域，则无法再查看在前一个区域中可以看到的资源或与之交互。

当您查看区域资源的 Amazon 资源名称 (ARN) 时，包含该资源的区域被指定为 ARN 中的第四个字段。例如，Amazon EC2 实例是一种区域资源。此类资源的 ARN 与 `us-east-1` 区域中存在的 VPC 的以下示例类似。

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

全球资源

有些 AWS 服务支持可以全球 访问的资源，这意味着您可以从任何地方 使用该资源。您无需在全局服务的控制台中指定 AWS 区域。要访问全球资源，在使用服务的 AWS CLI 和 AWS SDK 操作时请勿指定 `--region` 参数。

全球资源支持这种情况：在关键时刻某一特定资源只能存在一个实例。在这种情况下，在不同区域的副本之间进行复制或同步是不够的。为了确保资源使用者能即时看到任何变化，访问单一全局端点被认为是可以接受的，虽然可能会增加延迟。例如，当您创建 AWS Cloud WAN 核心网络作为全球资源时，它对所有用户都是一致的。它以单个连续的全局网络形式出现在所有区域。

全球资源的 Amazon 资源名称 (ARN) 不包括区域。此类 ARN 的第四个字段为空，例如以下示例 Cloud WAN 核心网络的 ARN。

```
arn:aws:networkmanager::123456789012:core-network/core-network-0514d38fa6f796cea
```

资源共享及其区域

AWS RAM 是一项区域服务，资源共享是区域性共享。因此，资源共享可以包含与该资源共享相同的 AWS 区域的资源以及任何支持的全球资源。您创建资源共享的区域是资源共享的主区域。

> **Important**
>
> 目前，您只能在指定主区域美国东部（弗吉尼亚州北部）区域 us-east-1 中创建全球资源的资源共享。尽管您只能在该单一主区域创建资源共享，但在该服务的控制台或 CLI 和 SDK 操作中查看时，任何共享的全球资源都将显示为标准全球资源。对主区域的限制仅适用于资源共享，不适用于其包含的资源。

要共享您在 us-west-2 区域创建的区域资源，您必须将 AWS RAM 控制台配置为使用 us-west-2 并在那里创建资源共享。您不能创建包含不同 AWS 区域的区域资源的资源共享。这意味着，要共享来自 us-west-2 和 eu-north-1 的资源，必须创建两个不同的资源共享。您不能将来自两个不同区域的资源合并到一个资源共享中。

要在 AWS RAM 控制台中共享全球资源，必须将 AWS RAM 控制台配置为使用指定的主区域，即美国东部（弗吉尼亚州北部）us-east-1。然后，在指定的主区域创建资源共享。您只能将资源共享中的全球资源与 us-east-1 区域的资源混合使用。

尽管全球资源只能在指定主区域的 AWS RAM 资源共享中查看，但在您共享后它仍然是全球资源。您可以从可在原始 AWS 账户访问全球资源的任何区域访问共享 AWS 账户中的全球资源。

注意事项

- 要在 AWS RAM 控制台创建资源共享，您必须使用包含要共享的资源的区域。如果要包含全球资源，则必须使用指定的主区域来创建共享。例如，要共享 AWS Cloud WAN 核心网络，您必须在 us-east-1 区域中创建资源共享。
- 要在 AWS RAM 控制台查看或修改资源共享，您必须使用包含资源共享的区域。同样，AWS RAM AWS CLI 和 SDK 操作仅允许您与您在操作中指定的区域中的资源共享进行交互。要查看或修改包含全球资源的资源共享，您必须使用指定的主区域，即美国东部（弗吉尼亚州北部）us-east-1。
- 要在 AWS RAM 控制台查看要包含在资源共享的区域资源，您必须使用包含区域资源的区域。
- 要在 AWS RAM 控制台中查看要包含在资源共享的全球资源，您必须使用指定的主区域，即美国东部（弗吉尼亚州北部）us-east-1。
- 您只能在指定主区域美国东部（弗吉尼亚州北部）us-east-1 中，同时 创建区域资源和全球资源的资源共享。

共享您拥有的 AWS 资源

您可以使用 AWS Resource Access Manager (AWS RAM)，与您指定的主体共享您指定的资源。本节介绍如何创建新的资源共享、修改现有资源共享以及删除不再需要的资源共享。

主题

查看您在 AWS RAM 中创建的资源共享

您可以查看您已创建的资源共享的列表。您可以查看您共享了哪些资源以及与哪些主体共享了这些资源。

Console

要查看资源共享，请执行以下操作：

1. 在 AWS RAM 控制台中，打开由我共享：资源共享页面。
2. 由于 AWS RAM 资源共享存在于特定 AWS 区域，因此，请从控制台右上角的下拉列表中选择相应的 AWS 区域。要查看包含全球资源的资源共享，您必须将 AWS 区域设置为美国东部（弗吉尼亚州北部）(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。
3. 如果结果中资源共享使用的任何托管权限具有指定为默认权限的新版托管权限，则页面会显示一条横幅来提醒您。您可以选择一次性更新所有托管权限版本，方法是：在页面顶部选择查看并全部更新。

   或者，对于具有一个或多个新版托管权限的单个资源共享，状态列会显示更新可用。选择该链接将开始查看更新的托管权限版本的过程，并允许您将其分配为该资源共享中相关资源类型的版本。
4. （可选）应用筛选条件以查找特定资源共享。您可以应用多个筛选条件来缩小搜索范围。您可以键入关键字（例如资源共享名称的一部分），仅列出名称中包含该文本的资源共享。选择文

本框可查看建议属性字段的下拉列表。选择一个字段后，您可以从该字段的可用值列表中进行选择。在找到所需资源之前，您可以添加其他属性或关键字。

5. 选择要查看的资源共享的名称。控制台显示以下有关资源共享的信息：

   - 摘要 - 列出资源共享名称、ID、所有者、Amazon 资源名称 (ARN)、创建日期、是否允许与外部账户共享及其当前状态。
   - 托管权限 - 列出附加到此资源共享的托管权限。资源共享中包含的每种资源类型最多可以有一个托管权限。每个托管权限都显示与资源共享关联的托管权限的版本。如果不是默认版本，则控制台会显示更新到默认版本链接。如果您选择该链接，则可以更新资源共享以使用默认版本。
   - 共享资源 - 列出资源共享中包含的各资源。选择资源的 ID，打开新的浏览器选项卡，以便在其本机服务的控制台中查看该资源。
   - 共享主体 - 列出共享资源的主体。
   - 标签 - 列出附加到资源共享本身的标签键值对；这些不是附加到资源共享中包含的各资源的标签。

AWS CLI

要查看资源共享，请执行以下操作：

您可以使用将参数 `--resource-owner` 设置为 SELF 的 get-resource-shares 命令，来显示在 AWS 账户中创建的资源共享的详细信息。

以下示例显示了在当前 AWS 区域 (us-east-1) 中为调用 AWS 账户共享的资源共享。要获取在其他区域创建的资源共享，请使用 `--region` *<region-code>* 参数。要加入包含全球资源的资源共享，您必须指定区域美国东部（弗吉尼亚州北部）us-east-1。

```
$  aws ram get-resource-shares \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
```

```
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        },
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
            "name": "MyLicenseConfigShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```


在中创建资源共享 AWS RAM

要共享您拥有的资源，请创建资源共享。过程概览：

1. 添加您要共享的资源。
2. 对于共享中包含的每种资源类型，请指定要用于该资源类型的托管权限。
   - 您可以从可用的 AWS 托管权限、现有客户托管权限中进行选择，也可以创建新的客户托管权限。
   - AWS 托管权限由创建 AWS ，以涵盖标准用例。
   - 客户托管权限允许您定制自己的托管权限，以满足您的安全和业务需求。

> **Note**
>
> 如果选定的托管权限有多个版本，则 AWS RAM 会自动附加默认版本。您只能 附加指定为默认版本的版本。

3. 指定要对资源拥有访问权限的主体。

注意事项

- 如果您以后需要删除共享中包含的 AWS 资源，我们建议您先从包含该资源的任何资源共享中移除该资源，或者删除该资源共享。
- 您可以在资源共享中包含的资源类型列在了可共享的资源 AWS中。
- 仅当您拥有某个资源时，您才可以共享此资源。您无法共享与您共享的资源。
- AWS RAM 是一项区域服务。当您与其他 AWS 账户中的主体共享资源时，这些主体必须从创建每个资源时所在的 AWS 区域 访问这些资源。对于支持的全局资源，您可以从 AWS 区域 该资源的服务控制台和工具支持的任何资源访问这些资源。您只能在指定的主区域美国东部（弗吉尼亚州北部）us-east-1 的 AWS RAM 控制台和工具中，查看此类资源共享及其全球资源。有关 AWS RAM 和全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。
- 如果您共享的账户是组织中组织的一员， AWS Organizations 并且启用了在组织内共享，那么与您共享的组织中的任何委托人将自动获得访问资源共享的权限，而无需使用邀请。您在组织环境之外与之共享的账户中的主体会收到加入资源共享的邀请，并且只有在他们接受邀请后才能获得对所共享资源的访问权限。
- 如果您与服务主体共享，则无法将任何其他主体与该资源共享关联。
- 如果共享是在属于某个组织的账户或主体之间进行的，则组织成员资格的任何更改都会动态影响对资源共享的访问权限。
  - 如果您 AWS 账户 向组织或有权访问资源共享的 OU 中添加，则该新成员账户将自动获得对资源共享的访问权限。然后，您与之共享的账户的管理员可以授予该账户中的个人主体访问该共享中的资源的权限。
  - 如果您从组织或有权访问资源共享的 OU 中移除某个账户，则该账户中的所有主体将自动失去对通过该资源共享访问的资源的访问权限。
  - 如果您直接与成员账户或成员账户中的IAM角色或用户共享，然后将该账户从组织中移除，则该账户中的任何委托人将无法访问通过该资源共享访问的资源。

> **Important**
>
> 当您与组织或 OU 共享，并且该范围包括拥有资源共享的账户时，共享账户中的所有主体都会自动获得对共享中资源的访问权限。授予的访问权限由与共享关联的托管权限定义。这是因为 AWS RAM 附加到共享中每个资源的基于资源的策略使用"Principal": "*"。有关更多信息，请参阅 使用的含义 "Principal": "*" 在基于资源的政策中。
> 其他所使用账户中的主体无法立即访问共享的资源。其他账户的管理员必须首先将基于身份的权限策略附加到相应的主体。这些策略必须授予ARNs对资源共享中各个资源的Allow访问权限。这些策略中的权限不能超过与资源共享关联的托管权限中指定的权限。

- 您只能将您的账户所属的组织以及OUs该组织添加到您的资源共享中。您不能将组织外部的组织作为委托人添加到OUs资源共享中。但是，对于支持的服务，您可以将组织外部的个人 AWS 账户 IAM角色和用户添加为资源共享的委托人。

> **Note**
>
> 并非所有资源类型都可以与IAM角色和用户共享。有关您可以与这些主体共享的资源的信息，请参阅可共享的资源 AWS。

- 对于以下资源类型，您有七天的时间接受邀请加入以下资源类型的共享。如果您在邀请到期之前未接受邀请，则系统会自动拒绝邀请。

> **Important**
>
> 对于不 在以下列表中的共享资源类型，您有 12 小时的时间 接受加入资源共享的邀请。12 小时后，邀请过期，资源共享中的最终用户主体将解除关联。最终用户无法再接受邀请。

  - Amazon Aurora - DB 集群
  - Amazon EC2 — 容量预留和专用主机
  - AWS License Manager — 许可证配置
  - AWS Outposts — 本地网关路由表、前哨基地和站点
  - Amazon Route 53 - 转发规则
  - Amazon VPC — 客户拥有IPv4的地址、前缀列表、子网、流量镜像目标、中转网关、中转网关组播域

Console

要创建资源共享，请执行以下操作：

1. 打开AWS RAM 控制台。
2. 由于 AWS RAM 资源共享是特定的 AWS 区域，因此请 AWS 区域 从控制台右上角的下拉列表中选择相应的资源共享。要查看包含全球资源的资源共享，必须将设置 AWS 区域 为美国东部（弗吉尼亚北部）、(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。如果要在资源共享中包含全球资源，则必须选择指定的主区域，即美国东部（弗吉尼亚州北部）us-east-1。

3. 如果您不熟悉 AWS RAM，请从主页上选择 “创建资源共享”。否则，请从由我共享：资源共享页面选择创建资源共享。
4. 在步骤 1：指定资源共享详细信息中，执行以下操作：

   a. 对于名称，键入资源共享的描述性名称。

   b. 在资源下，选择要添加到资源共享的资源，如下所示：

      - 对于选择资源类型，选择要共享的资源的类型。这会将可共享资源的列表筛选为仅所选类型的资源。
      - 在生成的资源列表中，选中要共享的各个资源旁边的复选框。所选资源将移至选定资源下。

        如果您要共享与特定可用区关联的资源，则使用可用区 ID（AZ ID）可帮助您跨账户确定这些资源的相对位置。有关更多信息，请参阅 AWS 资源的可用区 ID。

   c. （可选）要将标签附加到资源共享，请在标签下输入标签键和值。通过选择添加新标签，添加其他标签。根据需要重复上述步骤。这些标签仅适用于资源共享本身，不适用于资源共享中的资源。
5. 选择下一步。
6. 在步骤 2：将托管权限与每种资源类型关联中，您可以选择将创建的托管权限 AWS 与资源类型相关联，选择现有的客户托管权限，也可以为支持的资源类型创建自己的客户托管权限。有关更多信息，请参阅 托管权限的类型。

   选择创建客户托管权限，以构建符合共享使用案例要求的客户托管权限。有关更多信息，请参阅创建客户托管权限。完成该过程后，选择

   ，

   然后您可以从托管权限下拉列表中选择新的客户托管权限。

   > **Note**
   >
   > 如果选定的托管权限有多个版本，则 AWS RAM 会自动附加默认版本。您只能 附加指定为默认版本的版本。

   要显示托管权限允许的操作，请展开查看该托管权限的策略模板。
7. 选择下一步。
8. 在步骤 3：向主体授予访问权限中，执行以下操作：

a. 默认情况下，“允许与任何人共享” 处于选中状态，这意味着，对于支持共享的资源类型，您可以与 AWS 账户 组织外部的资源共享资源。这不会影响只能在组织内部共享的资源类型，例如 Amazon VPC 子网。您还可以与IAM角色和用户共享一些支持的资源类型。

要将资源共享限制为仅组织中的账户和主体，请选择仅允许在组织内共享。

b. 对于主体，请执行以下操作：

- 要添加组织、组织单位 (OU) 或组织的一部分 AWS 账户 ，请打开 “显示组织结构”。这将显示组织的树视图。然后，选中要添加的每个委托人旁边的复选框。

> **Important**
>
> 当您与组织或 OU 共享，并且该范围包括拥有资源共享的账户时，共享账户中的所有主体都会自动获得对共享中资源的访问权限。授予的访问权限由与共享关联的托管权限定义。这是因为 AWS RAM 附加到共享中每个资源的基于资源的策略使用`"Principal": "*"`。有关更多信息，请参阅 使用的含义 "Principal": "*" 在基于资源的政策中。
> 其他所使用账户中的主体无法立即访问共享的资源。其他账户的管理员必须首先将基于身份的权限策略附加到相应的主体。这些策略必须授予ARNs对资源共享中各个资源的`Allow`访问权限。这些策略中的权限不能超过与资源共享关联的托管权限中指定的权限。

- 如果您选择组织（ID 以 `o-` 开头），则组织中所有 AWS 账户 的主体都可以访问资源共享。
- 如果您选择一个 OU（ID 以开头`ou-`），则该 OU AWS 账户 中的所有委托人及其子级OUs都可以访问该资源共享。
- 如果您选择个人 AWS 账户，则只有该账户中的委托人才能访问资源共享。

> **Note**
>
> 仅当启用与 AWS Organizations 的共享功能并且您已登录到该组织的管理账户时，才会显示显示组织结构切换开关。
> 您不能使用此方法来指定组织 AWS 账户 外部人员、IAM角色或用户。相反，您必须关闭 “显示组织结构”，然后使用下拉列表和文本框输入 ID 或ARN。

- 要通过 ID 指定委托人ARN，或者包括组织外部的委托人，请为每位委托人选择委托人类型。接下来，输入 ID（对于 AWS 账户、组织或 OU）或ARN（IAM角色或用户），然后选择 “添加”。可用的主体类型、ID 和ARN格式如下所示：
  - AWS 账户— 要添加 AWS 账户，请输入 12 位数的账户 ID。例如：

    ```
    123456789012
    ```

  - 组织-要添加组织 AWS 账户 中的所有组织，请输入组织的 ID。例如：

    ```
    o-abcd1234
    ```

  - 组织单位（OU）- 要添加 OU，请输入 OU 的 ID。例如：

    ```
    ou-abcd-1234efgh
    ```

  - IAM角色-要添加IAM角色，请输入ARN该角色的。使用以下语法：

    ```
    arn:partition:iam::account:role/role-name
    ```

    例如：

    ```
    arn:aws:iam::123456789012:role/MyS3AccessRole
    ```

    > **Note**
    >
    > 要获取IAM角色ARN的唯一性，请在IAM控制台中查看角色列表，使用 get-role AWS CLI 命令或操作。GetRoleAPI

  - IAM用户-要添加IAM用户，请输入ARN该用户的。使用以下语法：

    ```
    arn:partition:iam::account:user/user-name
    ```

    例如：

    ```
    arn:aws:iam::123456789012:user/bob
    ```

    > **Note**
    >
    > 要获取IAM用户的唯一ARN值，请在IAM控制台中查看用户列表，使用 get-user AWS CLI 命令，或者 GetUserAPI行动。

- 服务主体 - 要添加服务主体，请从选择主体类型下拉列表中选择服务主体。输入 AWS 服务主体的名称。使用以下语法：
  - *service-id*.amazonaws.com

    例如：

    pca-connector-ad.amazonaws.com

c. 对于所选的主体，请验证您指定的主体是否显示在列表中。

9. 选择下一步。
10. 在步骤 4：查看和创建中，查看资源共享的配置详细信息。要更改任何步骤的配置，请选择与您要返回的步骤对应的链接，然后进行所需的更改。
11. 查看完资源共享后，选择创建资源共享。

    可能需要花几分钟时间，才能完成资源和委托人关联。在尝试使用资源共享之前，允许此过程完成。
12. 您可以随时添加和删除资源与主体，或将自定义标签应用于资源共享。您可以更改资源共享中包含的资源类型的托管权限，以及支持超过默认托管权限的资源类型的托管权限。您不再希望共享资源时，可以将其删除。有关更多信息，请参阅 共享您拥有的 AWS 资源。

AWS CLI

要创建资源共享，请执行以下操作：

使用 create-resource-share命令。以下命令创建与组织 AWS 账户 中的所有人共享的资源共享。该共享包含 AWS License Manager 许可证配置，并授予该资源类型的默认托管权限。

> **Note**
>
> 如果您想将客户托管权限与该资源共享中的资源类型一起使用，则可以使用现有的客户托管权限，也可以创建新的客户托管权限。记下ARN客户的托管权限，然后创建资源共享。有关更多信息，请参阅 创建客户托管权限。

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
```

```
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

更新中的资源共享 AWS RAM

您可以通过以下方式 AWS RAM 随时更新中的资源共享：

- 您可以向您创建的资源共享添加主体、资源或标签。
- 对于支持超过默认 AWS 托管权限的资源类型，您可以选择将哪种托管权限应用于每种类型的资源。
- 当附加到资源共享的托管权限具有新的默认版本时，您可以更新托管权限以使用新版本。
- 您可以通过从资源共享中删除主体或资源，撤消对共享资源的访问权限。如果您撤消访问权限，则主体不再对共享资源具有访问权限。

> **Note**
>
> 如果资源共享为空或仅包含支持退出资源共享的资源类型，则您与之共享资源的主体可以退出该共享。如果资源共享包含不支持退出的资源类型，则会显示一条消息，告知主体他们必须联系共享所有者。在这种情况下，作为资源共享的所有者，您必须从资源共享中移除主体。有关不支持此操作的资源类型的列表，请参阅退出资源共享的先决条件。

Console

要更新资源共享，请执行以下操作：

1. 导航到 AWS RAM 控制台中的由我共享：资源共享页面。
2. 由于 AWS RAM 资源共享是特定的 AWS 区域，因此请 AWS 区域 从控制台右上角的下拉列表中选择相应的资源共享。要查看包含全球资源的资源共享，必须将设置 AWS 区域 为美国东部（弗吉尼亚北部）、(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。
3. 选择资源共享，然后选择修改。
4. 在步骤 1：指定资源共享详细信息中，查看资源共享详细信息，并在需要时更新以下任意内容：

   a. （可选）要更改资源共享的名称，请编辑名称。

   b. （可选）要将资源添加到资源共享，请在资源下选择资源类型，然后选中资源旁边的复选框将其添加到资源共享中。仅当您在 AWS Management Console中将区域设置为美国东部（弗吉尼亚州北部）（us-east-1）时，全球资源才会显示。

   c. （可选）要从资源共享中移除资源，请在选定资源下找到该资源，然后选择资源 ID 旁边的 X。

   d. （可选）要向资源共享添加标签，请在标签下方的空白文本框中，输入标签键和值。要添加多个标签键和值对，请选择添加新标签。最多可以添加 50 个标签。

   e. 要从资源共享中移除标签，请在标签下，找到该标签并选择其旁边的移除。
5. 选择下一步。
6. （可选）在步骤 2：将托管权限与每种资源类型关联中，您可以选择将创建的托管权限 AWS 与资源类型相关联，选择现有的客户托管权限，也可以创建自己的客户托管权限。有关更多信息，请参阅 托管权限的类型。

   您也可以选择创建客户托管权限，以构建符合共享使用案例要求的客户托管权限。有关更多信息，请参阅 创建客户托管权限。完成该过程后，选择

   ，

   然后您可以从托管权限下拉列表中选择新的客户托管权限。

   要显示托管权限允许的操作，请展开查看该托管权限的策略模板。
7. 如果当前分配给资源共享的托管权限版本不是当前默认版本，则您可以通过选择更新到默认版本，更新到默认版本。

> **Note**
>
> 在完成最后一步之后保存对资源共享所做的更改之前，您可以通过选择还原到以前的版本，取消版本更新。但是，对于 AWS 托管权限，保存资源共享后，更改即为最终更改，您无法再返回到以前的版本。

8. 选择下一步。
9. 在步骤 3：选择允许访问的主体中，查看选定的主体，并在需要时更新以下任一内容：

   a. （可选）要更改是否启用与组织内部或外部的主体共享，请选择以下选项之一：

      - 要与 AWS 账户 组织外部的个人IAM角色或用户共享资源，请选择 “允许与外部委托人共享”。
      - 要在中将资源共享限制为仅限组织中的委托人 AWS Organizations，请选择 “仅允许与组织中的委托人共享”。

   b. 对于主体，请执行以下操作：

      - （可选）要在组织 AWS 账户 内部添加组织、组织单位 (OU) 或成员，请打开显示组织结构以显示组织的树视图。然后选中要添加的每个委托人旁边的复选框。

> **Important**
>
> 当您与组织或 OU 共享，并且该范围包括拥有资源共享的账户时，共享账户中的所有主体都会自动获得对共享中资源的访问权限。授予的访问权限由与共享关联的托管权限定义。这是因为 AWS RAM 附加到共享中每个资源的基于资源的策略使用`"Principal": "*"`。有关更多信息，请参阅 使用的含义 "Principal": "*" 在基于资源的政策中。
>
> 其他所使用账户中的主体无法立即访问共享的资源。其他账户的管理员必须首先将基于身份的权限策略附加到相应的主体。这些策略必须授予ARNs对资源共享中各个资源的`Allow`访问权限。这些策略中的权限不能超过与资源共享关联的托管权限中指定的权限。

> **Note**
>
> 仅当启用与 AWS Organizations 的共享功能并且您以组织管理账户的主体身份登录时，才会显示显示组织结构切换开关。

您不能使用此方法来指定组织 AWS 账户 外部人员、IAM角色或用户。相反，您必须通过输入其标识符来添加这些主体，这些标识符显示在显示组织结构切换开关下方的文本框中。请参见下一个要点。

- （可选）要按标识符添加委托人，请从下拉列表中选择委托人类型，然后输入委托人ARN的 ID 或。最后，选择添加。

  如果您选择个人 AWS 账户，则只有该帐户可以访问资源共享。您可以选择以下任一选项。

  - 其他 AWS 账户 （资源所有者除外）-使资源可供其他账户使用。该账户的管理员必须使用基于身份的权限策略向个人角色和用户授予对共享资源的访问权限，以完成该过程。这些权限不能超过附加到资源共享的托管权限中定义的权限。
  - 此 AWS 账户 （资源所有者）— 资源拥有者账户中的所有角色和用户都将自动获得由附加到资源共享的托管权限所定义的访问权限。
- 添加的内容会立即显示在选定的主体列表中。

  然后，您可以通过重复此步骤来添加其他帐户或您的组织。OUs
- （可选）要删除委托人，请在 “选定的委托人” 下找到该委托人，选中其复选框，然后选择取消选择。

10. 选择下一步。
11. 在步骤 4：查看和更新中，查看资源共享的配置详细信息。
12. 要更改任何步骤的配置，请选择与要返回的步骤对应的链接，然后进行所需的更改。

    如果任何托管权限仍在使用默认版本以外的版本，则您可以选择更新到默认版本来解决这个问题。
13. 完成更改后，选择更新资源共享。

AWS CLI

要更新资源共享，请执行以下操作：

您可以使用以下 AWS CLI 命令修改资源共享：

- 要重命名资源共享或更改是否允许使用外部委托人，请使用命令 update-resource-share。 以下示例重命名了指定的资源共享，并将其设置为仅允许来自其组织的委托人。您必须使用包含资源共享的 AWS 区域 所对应的服务端点。

```
$ aws ram update-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
    --name "my-renamed-resource-share" \
    --no-allow-external-principals
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "name": "my-renamed-resource-share",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": false,
        "status": "ACTIVE",
        "creationTime": 1565295733.282,
        "lastUpdatedTime": 1565303080.023
    }
}
```

- 要将资源添加到资源共享，请使用命令 associate-resource-share。 以下示例将子网添加到指定的资源共享。

```
$ aws ram associate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "associatedEntity": "arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235",
        "associationType": "RESOURCE",
        "status": "ASSOCIATING",
        "external": false
    ]
}
```

- 要为资源共享中的资源类型添加或替换托管权限，请使用以下命令 list-permissions 和 associate-resource-share-permission。 在一个资源共享中，您只能为每种资源类型分配一个托管权限。如

果您尝试向已具有托管权限的资源类型添加托管权限，则必须包含 `--replace` 选项，否则命令将失败并出现错误。

以下示例命令列出了亚马逊弹性计算云 (AmazonEC2) 子网可用的托管权限，然后使用其中ARNs一个命令替换当前为指定资源共享中该资源类型分配的 AWS 托管权限。ARNs

```
$ aws ram list-permissions \
    --resource-type ec2:Subnet
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMDefaultPermissionSubnet",
            "resourceType": "ec2:Subnet",
            "creationTime": "2020-02-27T11:38:26.727000-08:00",
            "lastUpdatedTime": "2020-02-27T11:38:26.727000-08:00"
        }
    ]
}
$ aws ram associate-resource-share-permission \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --permission-arn arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet
{
    "returnValue": true
}
```

- 要从资源共享中移除资源，请使用命令 disassociate-resource-share。 以下示例ARN从指定的资源共享中移除具有指定的 Amazon EC2 子网。

```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
```

```
        "associatedEntity": "arn:aws:ec2:us-east-1:ubnet/
subnet-0250c25a1f4e15235",
        "associationType": "RESOURCE",
        "status": "DISASSOCIATING",
        "external": false
    ]
}
```

- 要修改附加到资源共享的标签，请使用以下命令 tag-resource 和 untag-resource。 以下示例将标签project=lima添加到指定的资源共享。

```
$ aws ram tag-resource \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tags key=project,value=lima
```

以下示例从指定的资源共享中移除键为 project 的标签。

```
$ aws ram untag-resource \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tag-keys=project
```

如果成功，标记命令不会产生任何输出。

查看您在 AWS RAM 中共享的资源

您可以查看所有资源共享中您共享的单个资源列表。该列表有助于您确定您当前共享了哪些资源、包含这些资源的资源共享数量，以及有权访问这些资源的主体的数量。

Console

要查看您当前正在共享的资源，请执行以下操作：

1. 在 AWS RAM 控制台中，打开由我共享：共享资源页面。
2. 由于 AWS RAM 资源共享存在于特定 AWS 区域，因此，请从控制台右上角的下拉列表中选择相应的 AWS 区域。要查看包含全球资源的资源共享，您必须将 AWS 区域设置为美国东部

（弗吉尼亚州北部）(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。

3. 对于每个共享资源，可获得以下信息：

   - 资源 ID - 资源的 ID。选择资源的 ID，打开新的浏览器选项卡，以便在其本机服务控制台中查看该资源。
   - 资源类型 - 资源的类型。
   - 上次共享日期 - 上次共享资源的日期。
   - 资源共享 - 包含资源的资源共享的数量。要查看资源共享列表，请选择该数字。
   - 主体 - 可以访问资源的主体数量。选择此值以查看主体。

AWS CLI

要查看您当前正在共享的资源，请执行以下操作：

您可以使用将参数 `--resource-owner` 设置为 SELF 的 list-resources 命令，显示您当前共享的资源的详细信息。

以下示例显示了 AWS 区域 (us-east-1) 调用 AWS 账户内资源共享中所包括的资源。要获取在其他区域共享的资源，请使用 `--region` *<region-code>* 参数。

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner SELF
{
    "resources": [
        {
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:41.081000-07:00"
        },
        {
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
```

```
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-07-22T11:48:11.104000-07:00",
            "lastUpdatedTime": "2021-07-22T11:48:11.971000-07:00"
        }
    ]
}
```

在 AWS RAM 中查看您共享资源的主体

您可以查看所有资源共享中您共享资源的主体。查看此主体列表，可帮助您确定谁有权访问您的共享资源。

Console

要查看您共享资源的主体，请执行以下操作：

1. 导航到 AWS RAM 控制台中的由我共享：主体页面。
2. 由于 AWS RAM 资源共享存在于特定 AWS 区域，因此，请从控制台右上角的下拉列表中选择相应的 AWS 区域。要查看包含全球资源的资源共享，您必须将 AWS 区域设置为美国东部（弗吉尼亚州北部）(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。
3. 应用筛选条件以查找特定主体。您可以应用多个筛选条件来缩小搜索范围。选择文本框可查看建议属性字段的下拉列表。选择一个字段后，您可以从该字段的可用值列表中进行选择。在找到所需资源之前，您可以添加其他属性或关键字。
4. 对于列表中的每个主体，控制台都会显示以下信息：
   - 主体 ID - 主体的 ID。选择 ID 以打开新的浏览器选项卡，以便在其本机控制台中查看主体。
   - 资源共享 - 您与指定主体共享的资源共享数量。选择该数字以查看资源共享列表。
   - 资源 - 您与主体共享的资源数量。选择该数字以查看共享资源列表。

AWS CLI

要查看您共享资源的主体，请执行以下操作：

您可以使用 list-principals 命令，获取您在当前 AWS 区域中为调用账户创建的资源共享中引用的主体列表。

以下示例列出了有权访问在默认区域中为调用账户创建的共享的主体。在此示例中，主体是调用账户的组织和单独的 AWS 账户，作为两个不同资源共享的一部分。您必须使用包含资源共享的 AWS 区域所对应的服务端点。

```
$ aws ram list-principals \
    --region us-east-1 \
    --resource-owner SELF
{
    "principals": [
        {
            "id": "arn:aws:organizations::123456789012:organization/o-a1b2c3dr",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-09-14T20:40:58.532000-07:00",
            "lastUpdatedTime": "2021-09-14T20:40:59.610000-07:00",
            "external": false
        },
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/6405fa7c-0786-4e15-8c9f-8aec02802f18",
            "creationTime": "2021-09-15T15:00:31.601000-07:00",
            "lastUpdatedTime": "2021-09-15T15:14:13.618000-07:00",
            "external": true
        }
    ]
}
```

在 AWS RAM 中删除资源共享

您可以随时删除资源共享。当您删除资源共享时，与资源共享关联的所有主体都将失去对共享资源的访问权限。删除资源共享不会删除共享的资源。

> **删除 AWS 资源**
>
> 如果您需要删除包含在资源共享中的 AWS 资源，AWS 建议您首先确保从包含该资源的任何资源共享中移除该资源，或者删除该资源共享。

删除的资源共享在删除后仍在 AWS RAM 控制台中保留显示一小段时间，但其状态更改为 `Deleted`。

Console

要删除资源共享，请执行以下操作：

1. 在 AWS RAM 控制台中，打开由我共享：资源共享页面。
2. 由于 AWS RAM 资源共享存在于特定 AWS 区域，因此，请从控制台右上角的下拉列表中选择相应的 AWS 区域。要查看包含全球资源的资源共享，您必须将 AWS 区域设置为美国东部（弗吉尼亚州北部）(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。
3. 选择要删除的资源共享。

> **Warning**
>
> 务必选择正确的资源共享。您无法在删除后恢复资源共享。

4. 选择删除，然后在确认消息中，选择删除。
5. 两个小时后，已删除的资源共享将消失。在此之前，它仍在控制台中可见，且状态为已删除。

AWS CLI

要删除资源共享，请执行以下操作：

您可以使用 delete-resource-share 命令删除不再需要的资源共享。

以下示例首先使用 get-resource-shares 命令，获取要删除的资源共享的 Amazon 资源名称 (ARN)。然后，它使用 delete-resource-share 来删除指定的资源共享。

```
$  aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
```

```
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
$ aws ram delete-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425
{
    "returnValue": true
}
```

访问与您共享的 AWS 资源

使用 AWS Resource Access Manager (AWS RAM)，您可以查看已添加的资源共享、您可以访问的共享资源以及与您共享资源的共享资源。 AWS 账户 当您不再需要访问共享资源时，您也可以退出资源共享。

内容

- 接受和拒绝资源共享邀请
- 查看与您共享的资源共享
- 查看与您共享的资源
- 查看与您共享的主体
- 退出资源共享

接受和拒绝资源共享邀请

要访问共享资源，资源共享的所有者必须将您添加为主体。所有者可以将以下任一项作为主体添加到资源共享中。

- 您的账户所属的组织
- 包含您账户的组织单位（OU）
- 您的单个账户
- 对于支持的资源类型，您的特定 IAM 角色或用户

如果您通过属于中组织成员的 AWS 账户 添加到资源共享 AWS Organizations，并且启用了组织内部共享，则无需接受邀请即可自动访问共享资源。服务委托人还可以在不接受邀请的情况下自动访问共享资源。如果您获得访问权限的账户后来被从组织中删除，则该账户中的所有主体将自动失去对通过该资源共享访问的资源的访问权限。

如果通过以下一种方式将您添加到资源共享中，则您将收到加入资源共享的邀请：

- 您所在组织之外的账户 AWS Organizations
- 与之共享时组织内部的帐户 AWS Organizations 未启用

如果您收到加入资源共享的邀请，您必须接受它才能访问共享的资源。如果您拒绝邀请，则无法访问共享的资源。

对于以下资源类型，您有七天的时间接受邀请加入以下资源类型的共享。如果您在邀请到期之前未接受邀请，则系统会自动拒绝邀请。

> **Important**
>
> 对于不 在以下列表中的共享资源类型，您有 12 小时的时间 接受加入资源共享的邀请。12 小时后，邀请过期，资源共享中的最终用户主体将解除关联。最终用户无法再接受邀请。

- Amazon Aurora - DB 集群
- Amazon EC2 - 容量预留和专用主机
- AWS License Manager — 许可证配置
- AWS Outposts — 本地网关路由表、前哨基地和站点
- Amazon Route 53 - 转发规则
- Amazon VPC - 客户拥有的 IPv4 地址、前缀列表、子网、流量镜像目标、中转网关、传输网关组播域

Console

要回复资源共享的邀请，请执行以下操作：

1. 导航到 AWS RAM 控制台中的 “与我共享：资源共享” 页面。
2. 由于 AWS RAM 资源共享是特定的 AWS 区域，因此请 AWS 区域 从控制台右上角的下拉列表中选择相应的资源共享。要查看包含全球资源的资源共享，必须将设置 AWS 区域 为美国东部

（弗吉尼亚北部）、(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。

3. 查看您已添加到的资源共享列表。

   状态列显示您当前对资源共享的参与状态。Pending 状态表示您已被添加到资源共享，但尚未接受或拒绝邀请。

4. 要回复资源共享邀请，请选择资源共享 ID，然后选择接受资源共享以接受邀请，或者选择拒绝资源共享以拒绝邀请。如果您拒绝邀请，则无法访问资源。如果您接受邀请，则可以访问资源。

AWS CLI

要回复资源共享的邀请，请执行以下操作：

您可以使用以下命令接受或拒绝资源共享的邀请：

- get-resource-share-invitations
- accept-resource-share-invitation
- reject-resource-share-invitation

1. 以下示例首先使用get-resource-share-invitations命令检索用户可用的所有邀请的列表 AWS 账户。使用该 AWS CLI query参数，您可以将输出限制为仅显示那些status设置为的邀请PENDING。此示例显示了来自账户 111111111111 的一个邀请，对于指定 AWS 区域中的当前账户 123456789012，该邀请目前处于 PENDING。

```
$ aws ram get-resource-share-invitations \
    --region us-east-1 \
    --query 'resourceShareInvitations[?status==`PENDING`]'
{
    "resourceShareInvitations": [
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
            "resourceShareName": "Test TrngAcct Resource Share",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/c4506c70-df75-4e6c-ac30-42ca03295a37",
            "senderAccountId": "111111111111",
            "receiverAccountId": "123456789012",
```

```
            "invitationTimestamp": "2021-09-21T08:56:24.977000-07:00",
            "status": "PENDING"
        }
    ]
}
```

2. 找到要接受的邀请后，记下输出中的 resourceShareInvitationArn，以便在下一个命令中使用来接受邀请。

```
$ aws ram accept-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "ACCEPTED"
    }
}
```

如果成功，请注意，响应显示 status 已从 PENDING 变为 ACCEPTED。

如果您想拒绝邀请，请使用相同的参数运行reject-resource-share-invitation命令。

```
$ aws ram reject-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
```

```
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "REJECTED"
    }
}
```

查看与您共享的资源共享

您可以查看您有权访问的资源共享。您可以查看哪些主体与您共享了资源和他们共享了哪些资源。

Console

要查看资源共享，请执行以下操作：

1. 导航到 AWS RAM 控制台中的与我共享：资源共享页面。
2. 由于 AWS RAM 资源共享存在于特定 AWS 区域，因此，请从控制台右上角的下拉列表中选择相应的 AWS 区域。要查看包含全球资源的资源共享，您必须将 AWS 区域设置为美国东部（弗吉尼亚州北部）(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。
3. （可选）应用筛选条件以查找特定资源共享。您可以应用多个筛选条件来缩小搜索范围。您可以键入关键字（例如资源共享名称的一部分），仅列出名称中包含该文本的资源共享。选择文本框可查看建议属性字段的下拉列表。选择一个字段后，您可以从该字段的可用值列表中进行选择。在找到所需资源之前，您可以添加其他属性或关键字。
4. AWS RAM 控制台将显示以下信息：
   - 名称 - 资源共享的名称。
   - ID - 资源共享的 ID。选择 ID 来查看资源共享的详细信息页面。
   - 所有者 - 创建资源共享的 AWS 账户 的 ID。
   - 状态 – 资源共享的当前状态。可能的值包括：
     - `Active` - 资源共享处于活动状态并且可供使用。
     - `Deleted` - 资源共享已删除并且不再可用。
     - `Pending` - 资源共享接受邀请正在等待响应。

AWS CLI

要查看资源共享，请执行以下操作：

使用 get-resource-shares 命令，将 `--resource-owner` 参数设置为 `OTHER-ACCOUNTS`。

以下示例显示了指定 AWS 区域内其他 AWS 账户与调用账户共享的资源共享列表。

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Env Shared Licenses",
            "owningAccountId": "111111111111",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
        },
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:222222222222:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
            "name": "Prod Env Shared Subnets",
            "owningAccountId": "222222222222",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:56:24.737000-07:00",
            "lastUpdatedTime": "2021-09-21T08:56:24.737000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```

查看与您共享的资源

您可以查看您可以访问的共享资源。您可以查看哪些主体与您共享了资源和哪些资源共享包括这些资源。

Console

要查看与您共享的资源，请执行以下操作：

1. 导航到 AWS RAM 控制台中的与我共享：共享资源页面。
2. 由于 AWS RAM 资源共享存在于特定 AWS 区域，因此，请从控制台右上角的下拉列表中选择相应的 AWS 区域。要查看包含全球资源的资源共享，您必须将 AWS 区域设置为美国东部（弗吉尼亚州北部）(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。
3. 应用筛选条件以查找特定的共享资源。您可以应用多个筛选条件来缩小搜索范围。
4. 界面中会提供以下信息：
   - 资源 ID - 资源的 ID。选择资源的 ID 以在其服务控制台查看此资源。
   - 资源类型 - 资源的类型。
   - 上次共享日期 - 与您共享资源的日期。
   - 资源共享 - 包含资源的资源共享的数量。选择此值以查看资源共享。
   - 所有者 ID - 拥有资源的主体的 ID。

AWS CLI

要查看与您共享的资源，请执行以下操作：

您可以使用 list-resources 命令查看与您共享的资源。

以下示例命令显示了有关可在指定 AWS 区域内其他 AWS 账户中通过资源共享访问的资源的详细信息。

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resources": [
        {
            "arn": "arn:aws:license-manager:us-east-1:111111111111:license-
configuration:lic-36be0485f5ae379cc74cf8e9242ab143",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "status": "AVAILABLE",
```

```
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:42.517000-07:00"
        }
    ]
}
```

查看与您共享的主体

您可以查看与您共享资源的所有主体的列表。您可以查看他们与您共享的资源和资源共享。

Console

要查看与您共享资源的主体，请执行以下操作：

1. 通过以下网址打开 AWS RAM 控制台：https://console.aws.amazon.com/ram。
2. 由于 AWS RAM 资源共享存在于特定 AWS 区域，因此，请从控制台右上角的下拉列表中选择相应的 AWS 区域。要查看包含全球资源的资源共享，您必须将 AWS 区域设置为美国东部（弗吉尼亚州北部）(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。
3. 在导航窗格中，选择与我共享和委托人。
4. （可选）您可以应用筛选器以查找特定主体。您可以应用多个筛选条件来缩小搜索范围。
5. 控制台将显示以下信息：
   - 主体 ID - 与您共享的主体的 ID。
   - 资源共享 - 主体已添加您的资源共享数量。选择该数字以查看资源共享列表。
   - 资源 - 主体与您共享的资源数量。选择此值以查看资源列表。

AWS CLI

要查看与您共享资源的主体，请执行以下操作：

您可以使用 list-principals 命令来检索与您的 AWS 账户共享资源的主体列表。

以下示例命令显示了有关与指定 AWS 区域中用于调用该操作的账户共享资源共享的 AWS 账户的详细信息。

```
$  aws ram list-principals \
    --region us-east-1 \
```

```
    --resource-owner OTHER-ACCOUNTS
{
    "principals": [
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T09:06:25.545000-07:00",
            "external": true
        }
    ]
}
```

退出资源共享

如果您不再需要访问与您共享的资源，您可以随时退出资源共享。当您退出资源共享时，您将失去对共享资源的访问权限。

退出资源共享的先决条件

- 只有资源共享是以个人 AWS 账户与您共享的，而不是在组织环境中共享的，您才能退出该共享。如果您由组织内的 AWS 账户添加到了资源共享并且启用了与 AWS Organizations 的共享，则您不能退出该资源共享。自动访问组织内的资源共享。
- 要退出资源共享，请验证资源共享是否为空或是否仅包含支持退出共享的资源类型。

  以下是唯一支持退出资源共享的资源类型。

服务	资源类型
Amazon Aurora	`rds:Cluster`
Amazon EC2	`ec2:CapacityReservation` `ec2:DedicatedHost`
AWS License Manager	`license-manager:LicenseConfiguration`
AWS Outposts	`ec2:LocalGatewayRouteTable`

服务	资源类型
	outposts:Outpost outposts:Site
Amazon Route 53	route53resolver:ResolverRule
Amazon VPC	ec2:CoipPool ec2:PrefixList ec2:Subnet ec2:TrafficMirrorTarget ec2:TransitGateway ec2:TransitGatewayMulticast Domain

如何退出资源共享

Console

要退出资源共享，请执行以下操作：

1. 导航到 AWS RAM 控制台中的与我共享：资源共享页面。
2. 由于 AWS RAM 资源共享存在于特定 AWS 区域，因此，请从控制台右上角的下拉列表中选择相应的 AWS 区域。要查看包含全球资源的资源共享，您必须将 AWS 区域设置为美国东部（弗吉尼亚州北部）(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。
3. 选择要退出的资源共享。
4. 选择退出资源共享，然后在确认对话框中，选择退出。

AWS CLI

要退出资源共享，请执行以下操作：

您可以使用 disassociate-resource-share 命令退出资源共享。

以下示例命令会导致调用命令的 AWS 账户无法访问由 ARN 指定的资源共享所共享的资源。您必须将请求定向到 AWS 区域中包含您要退出的资源共享的服务端点。

1. 首先，检索资源共享列表以检索要退出的资源共享的 ARN。

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Environment Shared Licenses",
            "owningAccountId": "111111111111",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```

2. 然后，您可以运行命令来退出该资源共享。请注意，您还必须将您的账户 ID 123456789012 指定为主体，以取消与指定资源共享（由账户 111111111111 共享）的关联。

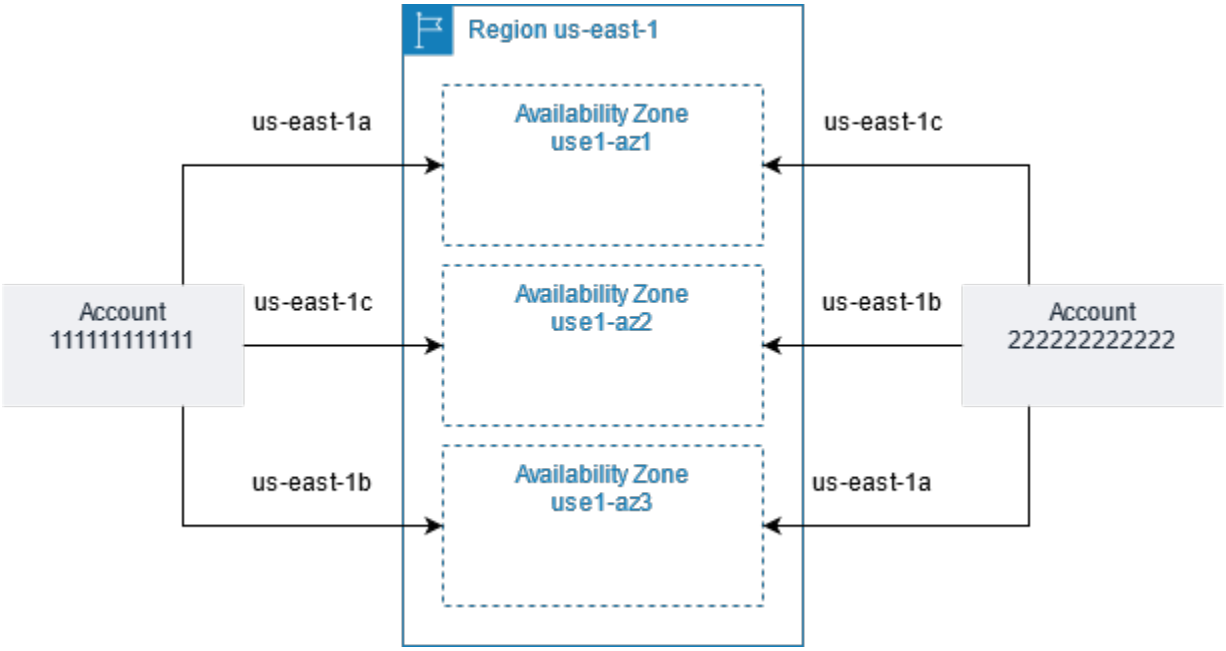
```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e \
    --principals 123456789012
                        {
    "resourceShareAssociations": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "associatedEntity": "123456789012",
            "associationType": "PRINCIPAL",
            "status": "DISASSOCIATING",
            "external": false
```

```
        }
    ]
}
```

AWS 资源的可用区 ID

AWS 将物理可用区随机 映射到每个 AWS 账户的可用区名称。这种方法有助于在 AWS 区域的可用区之间分配资源，而不是将资源集中在每个区域的可用区“a”中。因此，您的 AWS 账户的可用区 `us-east-1a` 可能与其他 AWS 账户的 `us-east-1a` 表示的物理位置不同。有关更多信息，请参阅《Amazon EC2 用户指南》中的区域和可用区。

下图显示了每个账户的 AZ ID 如何相同，尽管每个账户的可用区名称映射可能不同。



对于某些资源，您不仅必须要确定 AWS 区域，还必须要确定可用区。例如，Amazon VPC 子网。在单个账户中，可用区与特定名称的映射并不重要。但是，当您使用 AWS RAM 与其他 AWS 账户共享这样的资源时，映射很 重要。这种随机映射使访问共享资源的账户知道要引用哪个可用区的能力变得复杂。为了帮助解决这个问题，此类资源还允许您使用 AZ ID 来识别您的资源相对于账户的实际位置。AZ ID 是跨所有 AWS 账户的可用区的唯一且一致的标识符。例如，`use1-az1` 是 `us-east-1` 区域的可用区 AZ ID，它在每个 AWS 账户中的物理位置均相同。

您可以使用 AZ ID，以确定一个账户中的资源相对于另一个账户中的资源所在的位置。例如，如果您在 AZ ID 为 `use1-az2` 的可用区中与另一个账户共享一个子网，则在 AZ ID 也为 `use1-az2` 的可用区中该账户便可使用这一子网。每个子网的 AZ ID 均显示在 Amazon VPC 控制台中，且可以使用 AWS CLI 进行查询。

Console

查看账户中的可用区的 AZ ID

1. 在 AWS RAM 控制台中，导航到 AWS RAM 控制台页面。
2. 您可以在您的 AZ ID 下查看当前 AWS 区域的 AZ ID。

AWS CLI

查看账户中的可用区的 AZ ID

以下示例命令显示了 us-west-2 区域中可用区的 AZ ID 以及如何映射这些可用区以调用 AWS 账户。

```
$ aws ec2 describe-availability-zones \
    --region us-west-2
{
    "AvailabilityZones": [
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2a",
            "ZoneId": "usw2-az2",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2b",
            "ZoneId": "usw2-az1",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
```

```
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2c",
            "ZoneId": "usw2-az3",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2d",
            "ZoneId": "usw2-az4",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        }
    ]
}
```

可共享的资源 AWS

使用 AWS Resource Access Manager (AWS RAM)，您可以共享其他人创建和管理的资源 AWS 服务。您可以与个人共享资源 AWS 账户。您还可以与组织中的账户或组织单位 (OUs) 共享资源 AWS Organizations。某些支持的资源类型还允许您与个人 AWS Identity and Access Management (IAM) 角色和用户共享资源。

以下各节按 AWS 服务分组列出了您可以使用共享的资源类型 AWS RAM。表中的列指定了每种资源类型支持的功能：

可以与IAM用户和角色共享	 — 除了账户之外，您还可以与个人 AWS Identity and Access Management (IAM) 角色和用户共享此类资源。  - 您只能与账户共享此类资源。	是 否
可以与组织外部的账户共享	 – 您只能与企业内部或外部的任何个人账户共享此类资源。有关更多信息，请参阅注意事项。  - 您只能与属于同一组织成员的账户共享此类资源。	是 否
可以使用客户托管权限	支持的所有资源类型都 AWS RAM 支持 AWS 托管权限，但此列中的 “是” 表示该资源类型也支持客户托管权限。	

	 - 此类资源支持使用客户托管权限。  - 此类资源不支持使用客户托管权限。	是 否
可以与服务主体共享	 - 您可以与 AWS 服务共享此类资源。  - 您不能与 AWS 服务共享此类资源。	是 否

亚马逊API网关

您可以使用共享以下 Amazon API Gateway 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
域名 apigateway:Domainnames	集中创建和管理域名，并与其他人 AWS 账户 或您的组织共享。这样，多个账户就可以调用映射到私有域名的域名APIs。有关更多信息，请参阅 Amazon	 否	 是 可以与任何 AWS	 否	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	Gateway 开发者指南APIs中的 API Gatew API a y 中的私有自定义域名。		账户共享。		

AWS App Mesh

您可以通过使用共享以下 AWS App Mesh 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
Mesh `appmesh:Mesh`	集中创建和管理网格，并与其他 AWS 账户 或您的组织共享此类网格。共享网格允许不同 AWS 账户 网格创建的资源在同一个网格中相互通信。有关更多信息，请参阅《AWS App Mesh 用户指南》中的使用共享网格。	 是	 是 可以与任何 AWS 账户共享。	 否	 否

AWS AppSync GraphQL API

您可以使用共享以下 AWS AppSync GraphQL API 资源。 AWS RAM

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
GraphyQL API `appsync:APIs`	APIs集中管理 AWS AppSync GraphQL，并与其他人 AWS 账户或您的组织共享。这允许多个账户共享 AWS AppSync APIs作为创建统一 AWS AppSync 合并账户的一部分，API该合并账户可以访问同一区域中不同账户的多个子架构APIs中的数据。有关更多信息，请参阅《 AWS AppSync 开发者指南》APIs中的合并。	 是	 是 可以与任何 AWS 账户共享。	 是	 否

Amazon Aurora

您可以使用 AWS RAM共享以下 Amazon Aurora 资源。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
数据库集群 `rds:Cluster`	集中创建和管理 DB 集群，并与其他 AWS 账户 或您的组织共享此类集群。这允许多个 AWS 账户 克隆一个共享的、	 否	 是 可以与任何 AWS	 否	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	集中管理的 DB 集群。有关更多信息，请参阅亚马逊 A urora 用户指南中的使用跨账户克隆 AWS RAM 和 A mazon Aurora。		账户共享。		

AWS Backup

您可以通过使用共享以下 AWS Backup 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
BackupVault `backup:BackupVault`	集中创建和管理逻辑上存在气隙的保管库，并与其他人 AWS 账户 或您的组织共享。此选项允许多个账户访问和恢复保管库中的备份。有关更多信息，请参阅《AWS Backup 开发人员指南》中的逻辑气隙保管库概述。	是	是 可以与任何 AWS 账户共享。	是	否

Amazon Bedrock

您可以使用共享以下 Amazon Bedrock 资源。 AWS RAM

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
自定义模型 `bedrock:CustomModel`	集中创建和管理自定义模型，并与其他人 AWS 账户 或您的组织共享。这允许多个账户对生成式 AI 应用程序使用相同的自定义模型。有关更多信息，请参阅 Amazon Bedrock 用户指南中的共享其他账户的模型。	 是	 否 只能 与自己组织内的 AWS 账户 共享。	 是	 否

AWS Billing 查看服务

您可以使用共享 AWS Billing 以下 View 服务资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
账单视图 `billing:billingview`	集中创建和管理自定义账单视图，并与其他人 AWS 账户 或您的组织共享。这样，应用程序和业务部门所有者就可以通过成员账户访问业务部门级别的 AWS 支出。有关更多信息，请参阅AWS Cost Management 用户指南中的使用账单视图控	 否	 否 只能 与自己组织内的 AWS 账户 共享。	 是	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	制成本管理数据的访问权限。				

AWS Private Certificate Authority

您可以通过使用共享以下 AWS 私有 CA 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
Private Certificate Authority（CA） `acm-pca:CertificateAuthority`	为组织的内部公钥基础架构 (CAs) 创建和管理私有证书颁发机构 (PKI)，并CAs与其他人 AWS 账户 或您的组织共享这些机构。这允许其他账户中的 AWS Certificate Manager 用户颁发由您的共享 CA 签名的 X.509 证书。有关更多信息，请参阅《AWS Private Certificate Authority 用户指南》中的控制对私有 CA 的访问权限。	 是	 是 可以与任何 AWS 账户共享。	 否	 是

Amazon DataZone

您可以通过使用共享以下 DataZone 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
DataZone 域 `datazone:Domain`	集中创建和管理域，并与其他 AWS 账户 或您的组织共享此类域。这允许多个账户创建 Amazon DataZone 域名。有关更多信息，请参阅《亚马逊 DataZone 用户指南》 DataZone中的 “什么是亚马逊”。	 否	 是 可以与任何 AWS 账户共享。	 否	 否

AWS CloudHSM

您可以通过使用共享以下 AWS CloudHSM 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
AWS CloudHSM Backup `cloudhsm:Backup`	集中管理 AWS CloudHSM 备份，并与其他人 AWS 账户 或您的组织共享。这样，多个 AWS 账户 用户就可以查看有关 Backup 的信息并使用它来恢复集 AWS CloudHSM 群。	 是	 是	 是	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	有关更多信息，请参阅《AWS CloudHSM 用户指南》中的管理 AWS CloudHSM 备份。				

AWS CodeBuild

您可以通过使用共享以下 AWS CodeBuild 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
项目 codebuild:Project	创建一个项目，然后用它来运行构建。与其他人 AWS 账户 或您的组织共享项目。这允许多个 AWS 账户 和用户查看有关项目的信息并分析其构建。有关更多信息，请参阅《 AWS CodeBuild 用户指南》中的使用共享的项目。	 是	 是 可以与任何 AWS 账户共享。	 是	 否
报告组 codebuild:ReportGroup	创建一个报告组，然后在构建项目时使用它来创建报告。与其他人 AWS 账户 或您的组织共享报告组。这	 是	 是 可以与任何 AWS	 是	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	样，多个 AWS 账户 用户就可以查看报告组及其报告，以及每个报告的测试用例结果。报告可以在创建后的 30 天内进行查看，然后报告过期，无法再查看。有关更多信息，请参阅《AWS CodeBuild 用户指南》中的使用共享的项目。		账户共享。		

Amazon EC2

您可以使用共享以下 Amazon EC2 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
容量预留 `ec2:CapacityReservation`	集中创建和管理容量预留，并与其他人 AWS 账户 或您的组织共享预留容量。这样，多个用户就可以将其的 Amazon EC2 实例 AWS 账户 启动到集中管理的预留容量中。有关更多信息，请参阅 Amazon EC2 用户指	否	是 可以与任何 AWS 账户共享。	否	否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	南中的使用共享容量预留。 **Important** 如果您不满足共享容量预留的所有先决条件，则共享操作可能会失败。如果发生这种情况，并且用户尝试将某个 Amazon EC2 实例启动到该容量预留中，则该实例将作为按需实例启动，从而产生更高的成本。我们建议您尝试在 Amazon EC2 控制台中查看共享容量预留，以验证自己是否可以访问共享容量预留。您还可以监控资源共享是否出现故障，这样您就可以在用户启动实例之前采取纠正措施，从而降低成本。有关更多信息，				

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	请参阅 示例：在资源共享失败时发出警报。				
专属主机 `ec2:DedicatedHost`	集中分配和管理 Amazon EC2 专用主机，并与其他人 AWS 账户 或您的组织共享该主机的实例容量。这允许多个用户在集中管理的专用主机上 AWS 账户 启动他们的 Amazon EC2 实例。有关更多信息，请参阅 Amazon EC2 用户指南中的使用共享专用主机。	否	是 可以与任何 AWS 账户共享。	否	否
置放群组 `ec2:PlacementGroup`	在组织内外共享您在组织内外拥有的置放群组。 AWS 账户您可以将与之共享的任何账户启动到共享置放群组中的 Amazon 实EC2例。有关更多信息，请参阅 Amazon EC2 用户指南中的共享置放群组。	是	是 可以与任何 AWS 账户共享。	否	否

EC2Image Builder

您可以使用共享以下 EC2 Image Builder 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
组件 `imagebuilder:Component`	集中创建和管理组件，并与其他 AWS 账户 或您的组织共享此类组件。管理谁可以在其镜像配方中使用预定义的构建和测试组件。有关更多信息，请参阅 EC2Image Builder 用户指南中的共享 EC2 Image Builder 资源。	 是	 是 可以与任何 AWS 账户共享。	 是	 否
容器配方数 `imagebuilder:ContainerRecipe`	集中创建和管理您的容器配方，并与其他人 AWS 账户 或您的组织共享。这样，您可以管理谁能使用预定义的文档来复制容器映像构建。有关更多信息，请参阅 EC2Image Builder 用户指南中的共享 EC2 Image Builder 资源。	 是	 是 可以与任何 AWS 账户共享。	 是	 否
映像 `imagebuilder:Image`	集中创建和管理您的黄金映像，并与其他人 AWS 账户 或您的组织共享。管理谁可以在整个组织中使用使用 EC2 Image Builder 创建的图像。有关更多信息，请参阅 EC2Image Builder	 是	 是 可以与任何 AWS 账户共享。	 是	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	用户指南中的共享 EC2 Image Builder 资源。				
映像配方 `imagebuilder:ImageRecipe`	集中创建和管理您的图像配方，并与其他人 AWS 账户 或您的组织共享。这使您可以管理谁可以使用预定义的文档来复制AMI构建。有关更多信息，请参阅EC2Image Builder 用户指南中的共享 EC2 Image Builder 资源。	是	是 可以与任何 AWS 账户共享。	是	否

AWS End User Messaging SMS

您可以使用共享以下 AWS End User Messaging SMS 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
OptOutList `sms-voice:opt-out-list`	创建 OptOutList 并与组织 AWS 账户 中的其他人共享。您可以共享， OptOutList 以便其他应用程序可以从其他应用程序中选择退出用户的电话号码， AWS 账户 或者他们可以查看用户电话号码的状	否	是 可以与任何 AWS 账户共享。	是	否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	态。有关更多信息，请参阅《 AWS End User Messaging SMS 用户指南》中的 “使用共享资源”。				
PhoneNumber `sms-voice:phone-number`	创建和管理电话号码，以便与其他人 AWS 账户 或您的组织共享。这允许多人使用共享的电话号码 AWS 账户 发送消息。有关更多信息，请参阅《 AWS End User Messaging SMS 用户指南》中的 “使用共享资源”。	 否	 是 可以与任何 AWS 账户共享。	 是	 是
池 `sms-voice:pool`	创建和管理资源池，以便与其他人 AWS 账户 或您的组织共享。这允许多人使用共享池 AWS 账户 发送消息。有关更多信息，请参阅《 AWS End User Messaging SMS 用户指南》中的 “使用共享资源”。	 否	 是 可以与任何 AWS 账户共享。	 是	 是

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
SenderId `sms-voice:sender-id`	创建和管理 SenderId，并与其他人 AWS 账户或您的组织共享。这允许多人使用共享的消息 AWS 账户 发送消息 SenderId。有关更多信息，请参阅《 AWS End User Messaging SMS 用户指南》中的 “使用共享资源”。	否	是 可以与任何 AWS 账户共享。	是	是

Amaz FSx on 公开版 ZFS

您可以使用共享以下 Amazon f FSx or Open ZFS 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
FSx 卷 `fsx:Volume`	集中创建和管理 FSx Open ZFS 卷，并与其他人 AWS 账户 或您的组织共享。这允许多个账户通过FSxAPIsCreateVolume 或使用共享卷下的 OpenZfs 快照执行数据复制CopySnapshotAndUpdateVolume 。有	是	是 可以与任何 AWS 账户共享。	是	否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	关更多信息，请参阅《Amazon FSx 开放ZFS用户指南》中的按需数据复制。				

AWS Glue

您可以通过使用共享以下 AWS Glue 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
数据目录 `glue:Catalog`	管理中央数据目录，并与您的组织共享有关数据库和表 AWS 账户 的元数据。这使用户能够对多个账户的数据运行查询。有关更多信息，请参阅《AWS Lake Formation 开发人员指南》中的跨 AWS 账户共享数据目录表和数据库。	 否	 是 可以与任何 AWS 账户共享。	 否	 否
数据库 `glue:Database`	集中创建和管理数据目录数据库，并与 AWS 账户 您的组织共享。数据库是数据目录表的集合。这使用户能够运行	 否	 是 可以与任何 AWS	 否	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	查询以及提取、转换和加载 (ETL) 作业，这些作业可以跨多个账户联接和查询数据。有关更多信息，请参阅《AWS Lake Formation 开发人员指南》中的跨 AWS 账户共享数据目录表和数据库。		账户共享。		
表 `glue:Table`	集中创建和管理数据目录表，并与 AWS 账户您的组织共享。数据目录表包含有关 Amazon S3 中数据表、JDBC 数据源、Amazon Redshift、流媒体源和其他数据存储的元数据。这使用户能够运行可以跨多个账户加入和查询数据的查询和ETL作业。有关更多信息，请参阅《AWS Lake Formation 开发人员指南》中的跨 AWS 账户共享数据目录表和数据库。	 否	 是 可以与任何 AWS 账户共享。	 否	 否

AWS License Manager

您可以通过使用共享以下 AWS License Manager 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
许可证配置 `license-manager:LicenseConfiguration`	集中创建和管理许可证配置，并与其他人 AWS 账户 或您的组织共享。这使您可以在多个 AWS 账户中执行基于企业协议条款的集中管理许可规则。有关更多信息，请参阅《License Manager 用户指南》中的 License Manager 中的许可证配置。	 否	 是 可以与任何 AWS 账户共享。	 否	 否

AWS Marketplace

您可以通过使用共享以下 AWS Marketplace 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
Marketplace 目录实体 `aws-marketplace:Entity`	在中创建、管理和共享组织内部 AWS 账户 或组织内的实体 AWS Marketplace。有关更多信息，请参阅《AWS Marketplace Catalog API 参考》中的 AWS RAM中的资源共享。	 是	 是 可以与任何 AWS 账户共享。	 否	 否

AWS Migration Hub Refactor Spaces

您可以通过使用共享以下 AWS Migration Hub Refactor Spaces 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
Refactor Spaces 环境 `refactor-spaces:Environment`	创建 Refactor Spaces 环境，并使用它来包含您的 Refactor Spaces 应用程序。与组织中的其他 AWS 账户 或所有账户共享环境。这样 AWS 账户 ，多个用户就可以查看有关环境及其中的应用程序的信息。有关更多信息，请参阅《AWS Migration Hub Refactor Spaces 用户指南》中的使用 AWS RAM共享 Refactor Spaces 环境。	 是	 是 可以与任何 AWS 账户共享。	 是	 否

AWS Network Firewall

您可以通过使用共享以下 AWS Network Firewall 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
防火墙策略 network-firewall:FirewallPolicy	集中创建和管理防火墙策略，并与其他人 AWS 账户 或您的组织共享这些策略。这使组织中的多个账户可以共享一组通用的网络监控、保护和筛选行为。有关更多信息，请参阅《AWS Network Firewall 开发人员指南》中的共享防火墙策略和规则组。	 是	 是 可以与任何 AWS 账户共享。	 否	 否
规则组 network-firewall:StatefulRuleGroup network-firewall:StatelessRuleGroup	集中创建和管理无状态规则组和有状态规则组，并与其他人 AWS 账户 或您的组织共享。这使组织中的 AWS Organizations 多个帐户可以共享一组检查和处理网络流量的标准。有关更多信息，请参阅《AWS Network Firewall 开发人员指南》中的共享防火墙策略和规则组。	 是	 是 可以与任何 AWS 账户共享。	 否	 否

AWS Outposts

您可以通过使用共享以下 AWS Outposts 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
Outposts `outposts:Outpost`	集中创建和管理Outposts，并与组织中的其他 AWS 账户 共享此类 Outposts。这允许多个账户在共享的、集中管理的 Outposts 上创建子网和EBS卷。有关更多信息，请参阅AWS Outposts 用户指南中的使用共享的 AWS Outposts 资源。	 否	 否 只能 与自己组织内的 AWS 账户 共享。	 是	 否
本地网关路由表 `ec2:LocalGatewayRouteTable`	集中创建和管理与本地网关的关VPC联，并与组织 AWS 账户 中的其他人共享。这允许多个账户创建与本地网关的关VPC联，并查看路由表和虚拟接口配置。有关更多信息，请参阅《AWS Outposts 用户指南》中的可共享的 Outpost 资源。	 否	 否 只能 与自己组织内的 AWS 账户 共享。	 否	 否
站点 `outposts:Site`	创建和管理 Outpost 站点，并与组织中的其他 AWS 账户 共享此类站点。这允许多个账户在共享站点上创建和管理 Outposts，并支持在 Outpost 资源和站点之间进行分割控	 否	 是 可以与任何 AWS 账户共享。	 否	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	制。有关更多信息，请参阅AWS Outposts 用户指南中的使用共享的 AWS Outposts 资源。				

Amazon S3 on Outposts

您可以使用 AWS RAM共享以下 Amazon S3 on Outposts 资源。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
S3 on Outposts `s3-outposts:Outpost`	在 Outpost 上创建和管理 Amazon S3 存储桶、接入点和端点。这允许多个账户在共享站点上创建和管理 Outposts，并支持在 Outpost 资源和站点之间进行分割控制。有关更多信息，请参阅AWS Outposts 用户指南中的使用共享的 AWS Outposts 资源。	否	否 只能 与自己组织内的 AWS 账户 共享。	是	否

AWS 资源探索器

您可以通过使用共享以下 AWS 资源探索器 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
视图 `resource-explorer-2:View`	集中创建和配置资源浏览器视图，并与组织 AWS 账户 中的其他人共享。这样，多个角色和用户就可以 AWS 账户 搜索和发现可通过视图访问的资源。有关更多信息，请参阅《AWS 资源探索器用户指南》中的共享 Resource Explorer 视图。	 否	 否 只能 与自己组织内的 AWS 账户 共享。	 否	 否

AWS Resource Groups

您可以通过使用共享以下 AWS Resource Groups 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
资源组 `resource-groups:Group`	集中创建和管理主机资源组，并与组织 AWS 账户 中的其他人共享。这允许多人 AWS 账户 共享使用创建的一组 Amazon EC2 专用主机 AWS License Manager。有关更多信息，请参阅《AWS	 否	 是 可以与任何 AWS 账户共享。	 否	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	License Manager 用户指南》中的 AWS License Manager中的主机资源组。				

Amazon Route 53

您可以使用 AWS RAM共享以下 Amazon Route 53 资源。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
Route 53 解析器DNS防火墙规则组 `route53resolver:FirewallRuleGroup`	集中创建和管理 Route 53 Resolver DNS 防火墙规则组，并与其他人 AWS 账户 或您的组织共享这些规则。这使多个账户可以共享一组标准，用于检查和处理通过 Route 53 Resolver 的出站DNS查询。有关更多信息，请参阅《Amazon Route 53 开发者指南》 AWS 账户 中的 “在之间共享 Route 53 解析器DNS防火墙规则组”。	是	是 可以与任何 AWS 账户共享。	否	否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
Route 53 Profiles `route53profiles:Profile`	创建和管理 53 号公路 Profiles 集中管理，并与其他人 AWS 账户 或您的组织共享。这允许多个账户应用 Route 53 中指定的DNS配置 Profiles 变为多个VPCs。有关更多信息，请参阅 Amazon Route 53 Profiles在《亚马逊 Route 53 开发者指南》中。	 是	 是 可以与任何 AWS 账户共享。	 是	 否
Resolver 规则 `route53resolver:ResolverRule`	集中创建和管理 Resolver 规则，并与其他人 AWS 账户 或您的组织共享这些规则。这允许多个账户将DNS查询从其虚拟私有云 (VPCs) 转发到共享的集中管理的 Resolver 规则中定义的目标 IP 地址。有关更多信息，请参阅 Amazon Route 53 开发者指南中的与他人共享解析器规则 AWS 账户和使用共享规则。	 否	 是 可以与任何 AWS 账户共享。	 否	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
查询日志 `route53resolver:ResolverQueryLogConfig`	集中创建和管理查询日志，并与其他 AWS 账户 或您的组织共享这些日志。这 AWS 账户使多人可以将源自他们的DNS查询记录VPCs到集中管理的查询日志中。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的与其他 AWS 账户共享 Resolver 查询日志记录配置。	 是	 是 可以与任何 AWS 账户共享。	 是	 否

Amazon 应用程序恢复控制器 (ARC)

您可以使用共享以下 Amazon 应用程序恢复控制器 (ARC) 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
ARC 集群 `route53-recovery-control:Cluster`	集中创建和管理ARC集群，并与其他人 AWS 账户 或您的组织共享。这允许多个账户在单个共享集群中创建控制面板和路由控制，从而降低复杂性和组织所需	 是	 是 可以与任何 AWS 账户共享。	 是	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	的集群总数。有关更多信息，请参阅 Amazon 应用程序恢复控制器 (ARC) 开发者指南中的跨账户共享集群。				

Amazon Simple Storage Service

您可以通过使用共享以下 Amazon Simple Storage Service 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
Access Grants `s3:AccessGrants`	集中创建和管理 S3 访问权限授予实例，并与其他人 AWS 账户 或您的组织共享。这使得多个账户可以查看和删除共享资源。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的 S3 访问权限授予跨账户访问权限。	是	是 可以与任何 AWS 账户共享。	是	是

亚马逊 SageMaker AI

您可以使用共享以下 Amazon SageMaker AI 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
SageMaker AI 目录 `sagemaker:SagemakerCatalog`	为了便于发现 — 允许账户所有者向其他账户授予 SageMaker AI 目录中所有功能组资源的可发现性权限。一旦获得访问权限，这些账户的用户就可以从目录中查看与他们共享的功能组。有关更多信息，请参阅 A mazon A SageMaker I 开发者指南中的跨账户功能组可发现性和访问权限。 **Note** 在 SageMaker AI 中，可发现性和访问权限是单独的权限。	否	是 可以与任何 AWS 账户共享。	是	否
SageMaker AI 功能组 `sagemaker:FeatureGroup`	对于访问权限 - 允许账户所有者向其他账户授予特定功能组资源的访问权限。一旦获得访问权限，这些账户的用户就可以使用与他们共享的功能组。有关更多信息，请参阅 A mazon A SageMaker I 开发者指	是	是 可以与任何 AWS 账户共享。	是	否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	南中的跨账户功能组可发现性和访问权限。 Note 在 SageMaker AI 中，可发现性和访问权限是单独的权限。				
SageMaker AI JumpStart sagemaker:Hub	借助 SageMaker Amazon AI JumpStart，您可以sagemaker:Hub 集中创建和管理，并与同一组织 AWS 账户 中的其他人共享。有关更多信息，请参阅 Amazon AI 开发者指南中的在 Amazon A SageMaker I JumpStart 中使用私有策划中心控制基础模型访问权限。SageMaker	 是	 是 可以与任何 AWS 账户共享。	 是	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
谱系组 `sagemaker:LineageGroup`	Amazon SageMaker AI 允许您创建管道元数据的血统组，以便更深入地了解其历史和关系。与组织中的其他账户 AWS 账户 或账户共享血统组。这样，多个 AWS 账户 用户就可以查看有关世系组的信息并查询其中的跟踪实体。有关更多信息，请参阅 A mazon A SageMaker I 开发者指南中的跨账户血统跟踪。	 是	 是 可以与任何 AWS 账户共享。	 否	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
SageMaker AI 模型卡片 `sagemaker:ModelCard`	Amazon SageMaker AI 创建模型卡，将机器学习 (ML) 模型的关键细节集中在一个地方记录下来，从而简化管理和报告。与组织中的其他 AWS 账户 或账户共享您的模型卡，以实现机器学习操作的多账户策略。这 AWS 账户 允许将模型卡片的机器学习活动访问权限共享给其他账户。有关更多信息，请参阅亚马逊 A SageMaker I 开发者指南中的亚马逊 SageMaker AI 模型卡。	 是	 是 可以与任何 AWS 账户共享。	 否	 否
SageMaker AI 模型注册表模型 Package Group `sagemaker:model-package-group`	借助 SageMaker Amazon AI 模型注册表，您可以`sagemaker:model-package-group` 集中创建和管理，并与其他人共享 AWS 账户 以注册模型版本。有关更多信息，请参阅《亚马逊 A SageMaker I 开发者指南》中的 Amazon SageMaker AI 模型注册表。	 是	 是	 是	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
SageMaker 人工智能管道 `sagemaker:Pipeline`	借助 SageMaker Amazon AI 模型构建管道，您可以大规模创建、自动化和管理 end-to-end机器学习工作流程。与组织中的其他客户 AWS 账户 或账户共享您的渠道，为您的机器学习操作实现多账户策略。这允许多个 AWS 账户 用户查看有关管道及其执行的信息，并可选择访问其他账户的启动、停止和重试管道。有关更多信息，请参阅 A mazon SageMaker AI 开发者指南中的 SageMaker AI Pipelines 跨账户支持。	是	是 可以与任何 AWS 账户共享。	是	否

AWS Service Catalog AppRegistry

您可以通过使用共享以下 AWS Service Catalog AppRegistry 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
应用程序 servicecatalog:Application	创建应用程序，并使用它来跟踪整个 AWS 环境中属于该应用程序的资源。与其他人 AWS 账户 或您的组织共享该应用程序。这允许多个 AWS 账户 用户在本地查看有关应用程序及其关联资源的信息。有关更多信息，请参阅《服务目录用户指南》中的创建应用程序。	 否	 否 只能 与自己组织内的 AWS 账户 共享。	 是	 否
属性组 servicecatalog:AttributeGroup	创建属性组，并使用它来存储与您的应用程序相关的元数据。与其他 AWS 账户 或您的组织共享该属性组。这样，多个 AWS 账户 和用户就可以查看有关属性组的信息。有关更多信息，请参阅《服务目录用户指南》中的创建属性组。	 否	 否 只能 与自己组织内的 AWS 账户 共享。	 是	 否

AWS Systems Manager Incident Manager

您可以通过使用共享以下 AWS Systems Manager Incident Manager 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
联系人 `ssm-contacts:Contact`	集中创建和管理联系人和升级计划，并与其他人 AWS 账户 或您的组织共享联系人详细信息。这使许多人可以 AWS 账户 查看事件期间发生的互动。有关更多信息，请参阅《AWS Systems Manager Incident Manager 用户指南》中的使用共享的联系人和响应计划。	 是	 是 可以与任何 AWS 账户共享。	 是	 否
响应计划 `ssm-incidents:ResponsePlan`	集中创建和管理响应计划，并与其他人 AWS 账户 或您的组织共享。这使这些人能够 AWS 账户 将亚马逊 CloudWatch 警报和亚马逊 EventBridge 事件规则与响应计划联系起来，在检测到事件时自动创建事件。事件还可以访问这些其他 AWS 账户的指标。有关更多信息，请参阅《AWS Systems Manager Incident Manager 用户指南》中的使用共享的联系人和响应计划。	 是	 是 可以与任何 AWS 账户共享。	 是	 否

AWS Systems Manager 参数存储

您可以使用共享以下 AWS Systems Manager 参数存储资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
参数 `ssm:Parameter`	创建参数，并使用它来存储可在脚本、命令、SSM文档以及配置和自动化工作流程中引用的配置数据。与其他人 AWS 账户 或您的组织共享该参数。这允许多个 AWS 账户 用户查看有关字符串的信息，并通过将您的数据与代码分开来提高安全性。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的使用共享参数。	 是	 是 可以与任何 AWS 账户共享。	 是	 否

Amazon VPC

您可以使用共享以下亚马逊虚拟私有云 (AmazonVPC) 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
客户拥有的地址 IPv4 `ec2:CoipPool`	在 AWS Outposts 安装过程中，根据您提供的有关本地网络的信息，AWS 创建一个地址池，称为客户拥有的 IP 地址池。 客户拥有的 IP 地址通过您的本地网络提供连接到 Outposts 子网中资源的本地或外部连接。您可以使用弹性 IP 地址或使用自动分配客户拥有的 IP 地址的子网设置，将这些地址分配给 Outpost 上的资源，例如EC2实例。有关更多信息，请参阅《AWS Outposts 用户指南》中的客户拥有的 IP 地址。	否	否 只能 与自己组织内的 AWS 账户 共享。	否	否
IP 地址管理器 (IPAM) 池 `ec2:IpamPool`	与其他IAM角色 AWS 账户、用户或中的整个组织或组织单位 (OU) 集中共享 Amazon 资源VPCIPAM池 AWS Organizations。这使这些委托人可以CIDRs从资金池中分配给 AWS 资源VPCs，例如各自账户中的资源。有关更多信息，请参阅 Amazon	是	是 可以与任何 AWS 账户共享。	是	否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	VPC IP 地址管理器用户指南 AWS RAM中的使用共享IPAM池。				
IP 地址管理器 (IPAM) 资源发现 `ec2:IpamResourceDiscovery`	与其他人共享资源发现 AWS 账户。资源发现是一个 Amazon VPC IPAM 组件IPAM，用于管理和监控属于拥有者账户的资源。有关更多信息，请参阅 Amazon VPC IPAM 用户指南中的使用资源发现。	否	是 可以与任何 AWS 账户共享。	否	否
前缀列表 `ec2:PrefixList`	集中创建和管理前缀列表，并与其他人 AWS 账户 或您的组织共享。这允许在其资源中使用多个 AWS 账户 引用前缀列表，例如VPC 安全组和子网路由表。有关更多信息，请参阅 Amazon VPC 用户指南中的使用共享前缀列表。	否	是 可以与任何 AWS 账户共享。	否	否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
子网 `ec2:Subnet`	集中创建和管理子网，并与组织内的 AWS 账户 共享这些子网。这样，多个用户就可以将其应用程序资源 AWS 账户 启动到集中管理状态VPCs。这些资源包括亚马逊EC2实例、亚马逊关系数据库服务 (RDS) 数据库、Amazon Redshift 集群和 AWS Lambda 函数。有关更多信息，请参阅 Amazon VPC 用户指南中的使用VPC共享。 **Note** 要在创建资源共享时包含子网，除 `ram:CreateResourceShare` 之外，您还必须拥有 `ec2:DescribeSubnets` 和 `ec2:DescribeVpcs` 权限。 默认子网不可共享。您只能共享	否	只能 与自己组织内的 AWS 账户 共享。	否	否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
	自己创建的子网。				
安全组 `ec2:SecurityGroup`	集中创建和管理安全组，并与其他人 AWS 账户 或您的组织共享。这允许多人将安全组与其弹性网络接口 AWS 账户 相关联。有关更多信息，请参阅 Amazon VPC 用户指南中的共享安全组。	 是	 否 只能 与自己组织内的 AWS 账户 共享。	 是	 否
流量镜像目标 `ec2:TrafficMirrorTarget`	集中创建和管理流量镜像目标，并与其他人 AWS 账户 或您的组织共享。这允许多个 AWS 账户 将镜像网络流量从其账户中的流量镜像源发送到共享的、集中管理的流量镜像目标。有关更多信息，请参阅《流量镜像指南》中的跨账户流量镜像目标。	 否	 是 可以与任何 AWS 账户共享。	 否	 否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
中转网关 `ec2:TransitGateway`	集中创建和管理公交网关，并与其他人 AWS 账户 或您的组织共享。这允许多人通过共享的集中管理的传输网关在他们的网络VPCs和本地网络之间 AWS 账户路由流量。有关更多信息，请参阅在 Amazon 公交网关中共享VPC公交网关。 **Note** 要在创建资源共享时包含中转网关，除 `ram:CreateResourceShare` 之外，您还必须拥有 `ec2:DescribeTransitGateway` 权限。	否	是 可以与任何 AWS 账户共享。	否	否

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
中转网关组播域 `ec2:TransitGatewayMulticastDomain`	集中创建和管理传输网关组播域，并与其他人 AWS 账户 或您的组织共享这些域。这允许多个成员在组播域中 AWS 账户 注册和取消注册群组成员或群组源。有关更多信息，请参阅《中转网关指南》中的使用共享组播域。	 否	 是 可以与任何 AWS 账户共享。	 否	 否
AWS Verified Access 组 `ec2:VerifiedAccessGroup`	集中创建和管理 AWS Verified Access 群组，然后与其他人 AWS 账户 或您的组织共享。这允许多个账户中的应用程序使用一组共享的 AWS Verified Access 端点。有关更多信息，请参阅《AWS Verified Access 用户指南》AWS Resource Access Manager中的通过共享您的 AWS Verified Access 群组。	 是	 是 可以与任何 AWS 账户共享。	 否	 否

Amazon VPC Lattice

您可以使用共享以下 Amazon VPC Lattice AWS RAM资源。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
Amazon VPC Lattice 服务 `vpc-lattice:Service`	集中创建和管理 Amazon VPC Lattice 服务，并与个人 AWS 账户 或您的组织共享。这允许服务所有者在多账户环境中连接、保护和观察 service-to-service 通信。有关更多信息，请参阅《VPC莱迪思用户指南》中的使用共享资源。	 否	 是 可以与任何 AWS 账户共享。	 是	 否
Amazon VPC Lattice 服务网络 `vpc-lattice:ServiceNetwork`	集中创建和管理 Amazon VPC Lattice 服务网络，并与个人 AWS 账户 或您的组织共享。这允许服务网络所有者在多账户环境中连接、保护和观察 service-to-service通信。有关更多信息，请参阅 Amazon VPC Lattice 用户指南中的使用共享资源。	 否	 是 可以与任何 AWS 账户共享。	 是	 否

AWS 云 WAN

您可以使用共享以下 AWS Cloud WAN 资源 AWS RAM。

资源类型和代码	应用场景	可以与IAM用户和角色共享	可以与组织外部的账户共享	可以使用客户托管权限	可以与服务主体共享
云WAN核心网 networkmanager:CoreNetwork	集中创建和管理云WAN核心网络，并与其他人共享 AWS 账户。这允许在单个 Cloud WAN 核心网络上 AWS 账户访问和配置多台主机。有关更多信息，请参阅《AWS 云WAN用户指南》中的共享核心网络。	 是	 是 可以与任何 AWS 账户共享。	 否	 否

在 AWS RAM 中管理权限

在 AWS RAM 中，有两种类型的托管权限，即 AWS 托管权限和客户托管权限。

托管权限定义了使用者如何对资源共享中的资源进行操作。创建资源共享时，您必须指定要对资源共享中包含的每种资源类型使用哪种托管权限。托管权限中的策略模板包含基于资源的策略所需的所有内容，但主体和资源除外。资源的 Amazon 资源名称 (ARN) 和与资源共享关联的主体的 ARN 构成了基于资源的策略的要素。然后，AWS RAM 创建基于资源的策略，并将其附加到该资源共享中的所有资源。

每个托管权限可以有一个或多个版本。该托管权限的一个版本被指定为默认 版本。有时，AWS 通过创建新版本并将该新版本指定为默认版本，更新资源类型的 AWS 托管权限。您还可以通过创建新版本，更新您的客户托管权限。已附加到资源共享的托管权限不会 自动更新。AWS RAM 控制台会显示新的默认版本何时可用，您可以查看新默认版本与前一个版本相比后的变化。

> **Note**
>
> 我们建议您尽快更新到新版 AWS 托管权限。这些更新通常会增加对新的或更新的 AWS 服务的支持，这些更新可以使用 AWS RAM 共享其他资源类型。新的默认版本还可以解决和更正安全漏洞。

> **Important**
>
> 您只能将默认版托管权限附加到新资源共享。

您可以随时检索可用托管权限的列表。有关更多信息，请参阅查看托管权限。

主题

查看托管权限

您可以查看有关可分配给资源共享中资源类型的托管权限的详细信息。您可以识别分配给资源共享的托管权限。要查看这些详细信息，请使用 AWS RAM 控制台中的托管权限库。

Console

要查看有关 AWS RAM 中可用的托管权限的详细信息，请执行以下操作：

1. 在 AWS RAM 控制台中导航到托管权限库页面。
2. 由于 AWS RAM 资源共享存在于特定 AWS 区域，因此，请从控制台右上角的下拉列表中选择相应的 AWS 区域。要查看包含全球资源的资源共享，您必须将 AWS 区域设置为美国东部（弗吉尼亚州北部）(us-east-1)。有关共享全球资源的更多信息，请参阅共享区域资源（相较于全球资源）。尽管所有区域共享相同的可用 AWS 托管权限，但这会影响Step 5 中为每个托管权限显示的关联资源共享数量。客户托管权限仅在创建这些权限的区域中可用。
3. 在托管权限列表中，选择要查看其详细信息的托管权限。您可以使用搜索框筛选托管权限列表，方法是：输入部分名称或资源类型，或从下拉列表中选择托管权限类型。
4. （可选）要更改显示首选项，请选择托管权限面板右上角的齿轮图标。您可以更改以下首选项：

   - 页面大小 - 每页上显示的资源数量。
   - 换行 - 是否在表格行中换行。
   - 列 - 是显示还是隐藏有关资源类型和关联共享的信息。

   设置完显示首选项后，选择确认。
5. 对于每个托管权限，列表将显示以下信息：

   - 托管权限名称 - 托管权限的名称。
   - 资源类型 - 与托管权限关联的资源类型。
   - 托管权限类型 - 托管权限是 AWS 托管权限还是客户托管权限。
   - 关联共享 - 与托管权限关联的资源共享数量。如果显示数字，则您可以选择该数字以显示包含以下信息的资源共享表：
     - 资源共享名称 - 与托管权限关联的资源共享名称。
     - 托管权限版本 - 附加到此资源共享的托管权限的版本。
     - 所有者 - 资源共享所有者的 AWS 账户号。

    - 允许外部主体 - 该资源共享是否允许与 AWS Organizations 中组织外部的主体共享。
    - 状态 - 资源共享和托管权限之间关联的当前状态。
- 状态 - 描述托管权限是否为：
    - 可附加 - 您可以将托管权限附加到您的资源共享。
    - 不可附加 - 您无法将托管权限附加到您的资源共享。
    - 正在删除 - 托管权限已失效，很快就会被删除。
    - 已删除 - 托管权限已被删除。它会在两个小时内保持可见状态，然后才会从托管权限库中消失。

您可以选择托管权限的名称以显示有关该托管权限的更多信息。托管权限的详细信息页面将显示以下信息：

- 资源类型 - 此托管权限适用的 AWS 资源类型。
- 版本数量 - 一个客户托管权限最多可以有五个版本。
- 默认版本 - 指定哪个版本是默认版本，因此会将其自动分配给使用此托管权限的所有新资源共享。任何使用不同版本的现有资源共享都会显示一条提示，要求您将资源共享更新为默认版本。
- ARN - 托管权限的 Amazon 资源名称 (ARN)。AWS 托管权限的 ARN 使用以下格式：

  ```
  arn:aws:ram::aws:permission/
  AWSRAM[DefaultPermission]ShareableResourceType
  ```

  子字符串 *[DefaultPermission]*（实际的 ARN 中不带方括号）只存在于指定为默认值的资源类型的一个托管权限的名称中。
- 托管权限版本 - 您可以选择要在此下拉列表下方的选项卡中显示哪个版本的信息。
    - 详细信息选项卡：
        - 创建时间 - 创建此版托管权限的日期和时间。
        - 上次更新时间 - 上次更新此版托管权限的日期和时间。
    - 策略模板选项卡 - 此版托管权限允许主体对关联的资源类型执行的服务操作和条件列表（如果适用）。
    - 关联的资源共享 - 使用此版托管权限的资源共享列表。

AWS CLI

要查看有关 AWS RAM 中可用的托管权限的详细信息，请执行以下操作：

您可以使用 list-permissions 命令，获取可用于当前 AWS 区域中调用账户的资源共享的托管权限列表。

```
$ aws ram list-permissions
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:31.732000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:31.732000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-11-18T07:05:46.976000-08:00",
            "lastUpdatedTime": "2022-11-18T07:05:46.976000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },

        ... TRUNCATED FOR BREVITY ... RUN COMMAND TO SEE COMPLETE LIST OF
 PERMISSIONS ...

        {
```

```
            "arn": "arn:aws:ram::aws:permission/
AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
            "resourceType": "networkmanager:CoreNetwork",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:46.557000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:46.557000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },       {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
            "version": "1",
            "defaultVersion": true,
            "name": "My-Test-CMP",
            "resourceType": "ec2:IpamPool",
            "status": "ATTACHABLE",
            "creationTime": "2023-03-08T06:54:10.038000-08:00",
            "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "CUSTOMER_MANAGED"
        }
    ]
}
```

您还可以在 `list-permissions` AWS CLI 命令的 `--query` 参数中按名称查找特定托管权限的 ARN。以下示例筛选输出，以便仅包含与指定名称匹配的 `permissions` 数组结果中的元素。我们还指定只希望在结果中看到 ARN 字段，并且以纯文本格式而不是默认 JSON 格式显示。

```
$ aws ram list-permissions \
    --query "permissions[?name == 'My-Test-CMP'].arn \
    --output text
arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
```

找到您感兴趣的特定托管权限的 ARN 后，您可以运行命令 get-permission，检索其详细信息，包括其 JSON 策略文本。

```
$ aws ram get-permission \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
{
    "permission": {
```

```
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
        "version": "1",
        "defaultVersion": true,
        "name": "My-Test-CMP",
        "resourceType": "ec2:IpamPool",
        "permission": "{\n\t\"Effect\": \"Allow\",\n\t\"Action\": [\n
\t\t\"ec2:GetIpamPoolAllocations\",\n\t\t\"ec2:GetIpamPoolCidrs\",\n\t
\t\"ec2:AllocateIpamPoolCidr\",\n\t\t\"ec2:AssociateVpcCidrBlock\",\n
\t\t\"ec2:CreateVpc\",\n\t\t\"ec2:ProvisionPublicIpv4PoolCidr\",\n\t\t
\"ec2:ReleaseIpamPoolAllocation\"\n\t]\n}",
        "creationTime": "2023-03-08T06:54:10.038000-08:00",
        "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
        "isResourceTypeDefault": false,
        "permissionType": "CUSTOMER_MANAGED",
        "featureSet": "STANDARD",
        "status": "ATTACHABLE"
    }
}
```


在 AWS RAM 中创建和使用客户托管权限

AWS Resource Access Manager (AWS RAM) 为您可以共享的每种资源类型提供至少一种 AWS 托管权限。但是，这些托管权限可能不会为您的共享使用案例提供最低权限访问。当提供的其中一种 AWS 托管权限不起作用时，您可以创建自己的客户托管权限。

客户托管权限是您通过精确指定可以在哪些条件下使用 AWS RAM 共享的资源执行哪些操作来创建和维护的托管权限。例如，您想限制 Amazon VPC IP 地址管理器 (IPAM) 池的读取权限，这有助于您大规模管理 IP 地址。您可以为开发人员创建客户托管权限来分配 IP 地址，但不能查看其他开发人员账户分配的 IP 地址范围。您可以遵循最低权限相关的最佳实践，仅授予在共享资源上执行任务所需的权限。

此外，您可以根据需要更新或删除客户托管权限。

主题

创建客户托管权限

客户托管权限特定于 AWS 区域。确保在相应的区域创建此客户托管权限。

Console

要创建客户托管权限，请执行以下操作：

1. 请执行下列操作之一：
   - 导航到托管权限库，然后选择创建客户托管权限。
   - 直接导航到控制台中的创建客户托管权限页面。
2. 对于客户托管权限详细信息，请输入客户托管权限名称。
3. 选择此托管权限适用的资源类型。
4. 对于策略模板，定义允许对此资源类型执行哪些操作。
   - 您可以选择导入托管权限，以使用现有托管权限中的操作。
   - 在可视化编辑器中，选择或取消选择访问级别信息以满足您的要求。
   - 使用 JSON 编辑器添加或修改条件。
5. （可选）要将标签附加到托管权限，请为标签输入标签键和值。要添加其他标签，请选择添加新标签。根据需要重复上述步骤。
6. 完成后，选择创建客户托管权限。

AWS CLI

要创建客户托管权限，请执行以下操作：

- 运行 create-permission 命令，并指定名称、客户托管权限适用的资源类型以及策略模板正文文本。

  以下示例命令为 `imagebuilder:Component` 资源类型创建托管权限。

```
$ aws ram create-permission \
    --name TestCMP \
    --resource-type imagebuilder:Component \
    --policy-template "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}"
{
```

```
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
        "version": "1",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "resourceType": "imagebuilder:Component",
        "status": "ATTACHABLE",
        "creationTime": 1680033769.401,
        "lastUpdatedTime": 1680033769.401
    }
}
```

创建新版客户托管权限

如果客户托管权限的使用案例发生变化，则您可以创建新版托管权限。这不会影响您现有的资源共享，只会影响未来使用此客户托管权限的新资源共享。

每个托管权限最多可以有五个版本，但您只能关联默认版本。

Console

要创建客户托管权限的新版本，请执行以下操作：

1. 导航到托管权限库。
2. 按客户托管筛选托管权限列表，或搜索要更改的客户托管权限的名称。
3. 在托管权限详细信息页面的托管权限版本部分下，选择创建版本。
4. 对于策略模板，您可以使用可视化编辑器或 JSON 编辑器，添加或删除操作和条件。

   您还可以选择导入托管权限以使用现有的策略模板。
5. 完成后，在页面底部选择创建版本。

AWS CLI

要创建客户托管权限的新版本，请执行以下操作：

1. 找到要创建新版本的托管权限的 Amazon 资源名称 (ARN)。为此，使用 `--permission-type CUSTOMER_MANAGED` 参数调用 list-permissions，以便仅包含客户托管权限。

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. 获得 ARN 后，您可以调用 create-permission-version 操作并提供更新的策略模板。

```
$ aws ram create-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --policy-template {"Effect":"Allow","Action":
["imagebuilder:ListComponents"]}
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
        "version": "2",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "status": "ATTACHABLE",
        "resourceType": "imagebuilder:Component",
        "permission": "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}",
        "creationTime": 1680038973.79,
        "lastUpdatedTime": 1680038973.79
    }
}
```

输出包括新版本的版本号。

选择其他版本作为客户托管权限的默认版本

您可以将其他客户托管权限版本设置为新的默认版本。

Console

要为客户托管权限设置新的默认版本，请执行以下操作：

1. 导航到托管权限库。
2. 按客户托管筛选托管权限列表，或搜索要更改的客户托管权限的名称。
3. 在客户托管权限详细信息页面的托管权限版本部分下，使用下拉列表选择要设置为新默认版本的版本。
4. 选择设置为默认版本。
5. 显示对话框时，确认您希望此版本成为所有使用此客户托管权限的新资源共享的默认版本。如果您同意，请选择设置为默认版本。

AWS CLI

要为客户托管权限设置新的默认版本，请执行以下操作：

1. 通过调用 list-permission-versions，找到要设置为默认版本的版本号。

   以下示例命令将检索指定的托管权限的当前版本。

```
$ aws ram list-permission-versions \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "1",
            "defaultVersion": false,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "UNATTACHABLE",
            "creationTime": 1680033769.401,
```

```
            "lastUpdatedTime": 1680035597.345
        },
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. 将版本号设置为默认版本号后，您可以调用 set-default-permission-version 操作。

```
$ aws ram-cmp set-default-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 2
```

如果成功，该命令不返回任何输出。您可以再次运行 list-permission-versions，并验证所选版本的 `defaultVersion` 字段现在是否设置为 `true`。

删除客户托管权限版本

一个客户托管权限最多可以有五个版本。当您不再需要或不使用版本时，可以将其删除。您无法删除客户托管权限的默认版本。已删除的版本在控制台中最多可显示两个小时，并且处于已删除状态，然后系统才会将其完全删除。

Console

要删除客户托管权限版本，请执行以下操作：

1. 导航到托管权限库。
2. 按客户托管筛选托管权限列表，或者搜索包含您要删除的版本的客户托管权限的名称。
3. 确保要删除的版本不是当前默认版本。

4. 对于页面的版本部分，选择关联的资源共享选项卡，查看是否有共享使用此版本。

   如果有任何关联共享，则您必须先更改客户托管权限版本，然后才能删除此版本。
5. 选择版本部分右侧的删除版本。
6. 在确认对话框中，选择删除，确认您要删除此版本的客户托管权限。

   如果您不想删除此版本的客户托管权限，请选择取消。

AWS CLI

要删除客户托管权限的一个版本，请执行以下操作：

1. 调用 list-permission-versions 操作来检索可用的版本号。
2. 获得版本号后，将其作为参数提供给 delete-permission-version。

```
$ aws ram-cmp delete-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 1
```

   如果成功，该命令不返回任何输出。您可以再次运行 list-permission-versions，并验证输出中是否不再包含该版本。

删除客户托管权限

如果不再需要或不使用客户托管权限，可以将其删除。您无法删除与资源共享关联的客户托管权限。已删除的客户托管权限将在两小时后消失。在此之前，它仍在托管权限库中可见，且状态为已删除。

Console

要删除客户托管权限，请执行以下操作：

1. 导航到托管权限库。
2. 按客户托管筛选托管权限列表，或搜索要删除的客户托管权限的名称。
3. 在选择客户托管权限之前，确认托管权限列表中有 0 个关联共享。

   如果仍有与托管权限关联的资源共享，则您必须先为所有资源共享分配另一个托管权限，然后才能继续。
4. 在客户托管权限详细信息页面右上角，选择删除托管权限。

5. 显示确认对话框时，选择删除以删除托管权限。

AWS CLI

要删除客户托管权限，请执行以下操作：

1. 通过 `--permission-type CUSTOMER_MANAGED` 参数调用 list-permissions，以便仅包含客户托管权限，从而查找要删除的托管权限的 ARN。

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. 获得要删除的托管权限的 ARN 后，将其作为参数提供给 delete-permission。

```
$ aws ram delete-permission \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "returnValue": true,
    "permissionStatus": "DELETING"
}
```

将 AWS 托管权限更新到较新版本

有时，AWS 会更新可用于附加到特定资源类型的资源共享的 AWS 托管权限。AWS 执行此操作时，它会创建新版 AWS 托管权限。包含指定资源类型的资源共享不会自动更新为使用最新版托管权限。您必

须明确更新每个资源共享的托管权限。必须执行这一额外步骤，以便您先评估更改，然后再将其应用于您的资源共享。

Console

每当控制台显示列出与资源共享关联的权限的页面，并且其中一个或多个权限使用的版本不是默认权限版本时，控制台都会在控制台页面的顶部显示横幅。横幅表示您的资源共享使用的版本不是默认版本。

此外，当当前版本不是默认版本时，各权限可以在该当前版本号旁边显示更新到默认版本按钮。

选择该按钮将启动更新资源共享向导。在该向导的步骤 2 中，您可以更新任何非默认权限的版本以使用其默认版本。

在向导的最后一页上选择提交，完成向导后，更改才会保存。

> **Note**
>
> 您只能附加默认版本，并且无法恢复到其他版本。
> 对于客户托管权限，在将权限更新为默认版本后，除非先将其他版本设置为默认版本，否则无法将其他版本应用于资源共享。例如，如果您将权限更新为默认版本，然后发现要回滚的错误，则可以将以前的版本指定为默认版本。或者，您可以创建一个不同的新版本，然后将其指定为默认版本。执行其中一个选项后，您将更新资源共享以使用现在的默认版本。

AWS CLI

要更新 AWS 托管权限的版本，请执行以下操作：

1. 运行带 `--permission-arn` 参数的 get-resource-shares 命令，以指定要更新的托管权限的 Amazon 资源名称 (ARN)。这会导致该命令仅返回使用该托管权限的资源共享。

   例如，以下示例命令返回有关使用 Amazon EC2 容量预留的默认 AWS 托管权限的每个资源共享的详细信息。

   ```
   $ aws ram get-resource-shares \
       --resource-owner SELF \
       --permission-arn arn:aws:ram::aws:permission/
   AWSRAMDefaultPermissionCapacityReservation
   ```

   输出包括每个资源共享的 ARN，其中至少有一个资源的访问权限由该托管权限控制。

2. 对于上一个命令中指定的每个资源共享，运行命令 associate-resource-share-permission。包括用于指定要更新的资源共享的 `--resource-share-arn`、用于指定要更新的 AWS 托管权限的 `--permission-arn`，以及用于指定要更新共享以使用该托管权限最新版本的 `--replace` 参数。您无需指定版本号；系统会自动使用默认版本。

```
$ aws ram associate-resource-share-permission \
    --resource-share-arn < ARN of one of the shares from the output of the
 previous command > \
    --permission-arn arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionCapacityReservation \
    --replace
```

3. 对步骤 1 中命令的结果中收到的每个 `ResourceShareArn`，重复上一步中的命令。

在中使用客户托管权限的注意事项 AWS RAM

客户管理的权限仅在您创建 AWS 区域 的权限中可用。并非所有资源类型都支持客户托管权限。有关中支持的资源类型的列表 AWS Resource Access Manager，请参阅可共享的资源 AWS。

不支持包含多个语句的客户托管权限。在客户托管权限中，您只能使用单个非否定运算符。

客户托管权限不支持以下条件：

- 用于匹配主体属性的条件键：
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- 用于限制服务主体访问的条件密钥：
  - `aws:SourceArn`
  - `aws:SourceAccount`
  - `aws:SourceOrgPaths`
  - `aws:SourceOrgID`
- 系统标签：
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`

- aws:RequestTag/aws:

> **Note**
>
> 共享给服务委托人时，会自动填充该aws:SourceAccount值。

托管权限的工作原理

如需快速概览，请观看以下视频，该视频演示了托管权限如何允许您对 AWS 资源应用最低权限访问的最佳实践。

此视频演示如何遵循最低权限的最佳实践，创建和关联客户托管权限。有关更多信息，请参阅???。

创建资源共享时，您可以将 AWS 托管权限与要共享的每种资源类型相关联。如果托管权限有多个版本，则新的资源共享将始终使用指定为默认版本的版本。

创建资源共享后，AWS RAM 使用托管权限生成附加到每个共享资源的基于资源的策略。

托管权限中的策略模板指定了以下内容：

效果

表示是 Allow 还是 Deny 主体对共享资源执行操作的权限。对于托管权限，效果始终是 Allow。有关更多信息，请参阅《IAM 用户指南》中的效果。

操作

主体有权执行的操作列表。这可以是 AWS Management Console中的操作，也可以是 AWS Command Line Interface (AWS CLI) 或 AWS API 中的操作。操作由 AWS 权限定义。有关更多信息，请参阅《IAM 用户指南》中的操作。

条件

主体何时以及如何与资源共享中的资源进行交互。条件为您的共享资源增加了一层额外安全保障。使用它们来限制对共享资源的敏感操作的访问权限。例如，您可以包括一些条件，要求操作必须来自特定的公司 IP 地址范围，或者这些操作必须由经过多因素身份验证的用户执行。有关条件的更多信息，请参阅《IAM 用户指南》中的 AWS 全局条件上下文键。有关特定于服务的条件的更多信息，请参阅《服务授权参考》中的 AWS 服务的操作、资源和条件键。

> **Note**
>
> 客户托管权限和 AWS 托管权限支持的资源类型都有条件。
> 有关不适用于客户托管权限的条件的信息，请参阅在中使用客户托管权限的注意事项 AWS RAM。

托管权限的类型

创建资源共享时，您可以选择一个托管权限以与资源共享中包含的每种资源类型相关联。AWS 托管权限由 AWS 资源所属服务定义，并由 AWS RAM 管理。您可以创建和维护自己的客户托管权限。

- AWS 托管权限 - AWS RAM 支持的每种资源类型都有一个可用的默认托管权限。除非您明确选择其他托管权限之一，否则默认托管权限是用于资源类型的权限。默认托管权限旨在支持共享指定类型资源的最常见客户场景。默认托管权限允许主体执行由服务为资源类型定义的特定操作。例如，对于 Amazon VPC `ec2:Subnet` 资源类型，默认托管权限允许主体执行以下操作：
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:DescribeSubnets`

  默认 AWS 托管权限的名称使用以下格式：`AWSRAMDefaultPermission`*`ShareableResourceType`*。例如，对于 `ec2:Subnet` 资源类型，默认 AWS 托管权限的名称为 `AWSRAMDefaultPermissionSubnet`。

  > **Note**
  >
  > 默认托管权限与托管权限的默认版本 是分开的。所有托管权限，无论是默认权限还是某些资源类型支持的其他托管权限之一，都是独立的、完整的权限，具有不同的效果和操作，支持不同的共享场景，例如读写权限和只读权限。任何托管权限，无论是 AWS 托管权限还是客户托管权限，都可以有多个版本，其中一个版本是该权限的默认版本。

  例如，当您共享同时支持完全访问（`Read` 和 `Write`）托管权限和只读托管权限的资源类型时，您可以为具有完全访问托管权限的管理员创建一个资源共享。然后，您可以使用只读托管权限为其他开发人员创建单独的资源共享，以遵循授予最低权限的实践。

> **Note**
>
> 所有使用 AWS RAM 的 AWS 服务都至少支持一种默认托管权限。您可以在托管权限库页面上，查看每个 AWS 服务可用的权限。此页面提供有关每个可用托管权限的详细信息，包括当前与该权限关联的所有资源共享，以及是否允许与外部主体共享（如果适用）。有关更多信息，请参阅查看托管权限。
>
> 对于不支持其他托管权限的服务，在创建资源共享时，AWS RAM 会自动应用为所选资源类型定义的默认权限。如果支持，您还可以选择在关联托管权限页面上，选择创建客户托管权限。

- 客户托管权限 - 客户托管权限是您通过精确指定可以在哪些条件下对使用 AWS RAM 共享的资源执行哪些操作来创建和维护的托管权限。例如，您想限制 Amazon VPC IP 地址管理器 (IPAM) 池的读取权限，这有助于您大规模管理 IP 地址。您可以为开发人员创建客户托管权限来分配 IP 地址，但不能查看其他开发人员账户分配的 IP 地址范围。您可以遵循最低权限相关的最佳实践，仅授予在共享资源上执行任务所需的权限。

安全性 AWS RAM

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 AWS Resource Access Manager （ AWS RAM ）的合规性计划，请参阅合规性计划范围内的AWS 服务。
- 云端安全-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。

本文档可帮助您了解在使用时如何应用分担责任模型 AWS RAM。以下主题向您介绍如何进行配置 AWS RAM 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 AWS RAM 资源。

主题

- 中的数据保护 AWS RAM
- 的身份和访问管理 AWS RAM
- 登录和监控 AWS RAM
- AWS RAM 中的故障恢复能力
- 中的基础设施安全 AWS RAM
- 访问 AWS Resource Access Manager 使用接口端点 (AWS PrivateLink)

中的数据保护 AWS RAM

分 AWS 担责任模型适用于中的数据保护 AWS Resource Access Manager。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础架构上的内容的控制。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 FAQ。 有关欧洲数据保护的信息，请参阅责任AWS 共担模型和AWS安全GDPR博客上的博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭据并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。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 资源通信。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 使用API进行设置和用户活动记录 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或访问时需要 FIPS 140-3 经过验证的加密模块API，请使用端点。FIPS有关可用FIPS端点的更多信息，请参阅联邦信息处理标准 (FIPS) 140-3。

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

的身份和访问管理 AWS RAM

AWS Identity and Access Management (IAM) 是一项可帮助管理员安全地控制对 AWS 资源的访问的 AWS 服务。管理员IAM控制谁可以进行身份验证（登录）和授权（拥有权限）使用 AWS 资源。通过使用IAM，您可以在中创建委托人，例如角色、用户和群组。 AWS 账户您可以控制这些委托人使用 AWS 资源执行任务所拥有的权限。您无需IAM支付额外费用即可使用。有关管理和创建自定义IAM策略的更多信息，请参阅《IAM用户指南》中的管理IAM策略。

主题

- AWS RAM 如何使用 IAM
- AWS适用于 AWS RAM 的托管策略
- 对 AWS RAM 使用服务相关角色
- AWS RAM 的 IAM 策略示例
- AWS Organizations 和的服务控制策略示例 AWS RAM

- 禁用与 AWS Organizations 的资源共享

AWS RAM 如何使用 IAM

默认情况下，IAM委托人无权创建或修改 AWS RAM 资源。要允许IAM委托人创建或修改资源并执行任务，请执行以下步骤之一。这些操作授予使用特定资源和API操作的权限。

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

  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。
- IAM通过身份提供商管理的用户：

  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）中的说明进行操作。
- IAM用户：
  - 创建您的用户可以担任的角色。按照《用户指南》中为IAM用户创建角色中的IAM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《用户指南》中向用户（控制台）添加权限中的IAM说明进行操作。

AWS RAM 提供了多种 AWS 托管策略，您可以使用这些策略来满足许多用户的需求。有关这些规则组的更多信息，请参阅 AWS适用于 AWS RAM 的托管策略。

如果您需要对授予用户的权限进行更精细的控制，可以在IAM控制台中构建自己的策略。有关创建策略并将其附加到您的IAM角色和用户的信息，请参阅《AWS Identity and Access Management 用户指南》IAM中的策略和权限。

以下各节提供了构建IAM权限策略的 AWS RAM 具体细节。

目录

策略结构

IAM权限策略是一个包含以下语句的JSON文档：效果、操作、资源和条件。IAM政策通常采用以下形式。

```
{
    "Statement":[{
        "Effect":"<effect>",
        "Action":"<action>",
        "Resource":"<arn>",
        "Condition":{
            "<comparison-operator>":{
                "<key>":"<value>"
            }
        }
    }]
}
```

效果

Effect 语句指定策略是允许还是拒绝主体执行操作的权限。可能的值包括：`Allow` 和 `Deny`。

操作

Acti on 语句指定了策略允许或拒绝权限的 AWS RAM API操作。有关允许的操作的完整列表，请参阅《IAM用户指南》 AWS Resource Access Manager中定义的操作。

资源

R esou rce 语句指定了受策略影响的 AWS RAM 资源。要在语句中指定资源，您需要使用其唯一的 Amazon 资源名称 (ARN)。有关允许的资源的完整列表，请参阅《IAM用户指南》 AWS Resource Access Manager中定义的资源。

状况

Condition 语句是可选语句。它们可以用来进一步完善政策的适用条件。 AWS RAM 支持以下条件键：

- `aws:RequestTag/${TagKey}` - 测试服务请求是否包含具有指定标签键的标签并具有指定值。
- `aws:ResourceTag/${TagKey}` - 测试服务请求处理的资源是否附加了标签（其中包含您在策略中指定的标签键）。

  以下示例条件检查服务请求中引用的资源是否附加键名称为“Owner”、值为“Dev Team”的标签。

```
"Condition" : {
    "StringEquals" : {
        "aws:ResourceTag/Owner" : "Dev Team"
    }
}
```

- `aws:TagKeys` - 指定在创建或标记资源共享时必须使用的标签键。
- `ram:AllowsExternalPrincipals` - 测试服务请求中的资源共享是否允许与外部主体共享。外部委托人是指您的组织 AWS 账户 外部 AWS Organizations。如果其评估结果为 `False`，则您只能与同一组织中的账户共享此资源共享。
- `ram:PermissionArn`— 测试在服务请求中ARN指定的权限是否与您在策略中指定的ARN字符串相匹配。
- `ram:PermissionResourceType` - 测试在服务请求中指定的权限是否对您在策略中指定的资源类型有效。使用可共享资源类型列表中显示的格式指定资源类型。
- `ram:Principal`— 测试服务请求中指定的委托人是否与您在策略中指定的ARN字符串相匹配。ARN
- `ram:RequestedAllowsExternalPrincipals` - 测试服务请求是否包含 `allowExternalPrincipals` 参数以及其参数是否与您在策略中指定的值相匹配。
- `ram:RequestedResourceType` - 测试正在处理的资源的资源类型是否与您在策略中指定的资源类型字符串相匹配。使用可共享资源类型列表中显示的格式指定资源类型。
- `ram:ResourceArn`— 测试服务请求所处理ARN的资源是否与您在策略中指定的资源相匹配。ARN
- `ram:ResourceShareName` - 测试服务请求正在处理的资源共享的名称是否与您在策略中指定的字符串相匹配。
- `ram:ShareOwnerAccountId` - 测试服务请求正在处理的资源共享的账户 ID 编号是否与您在策略中指定的字符串相匹配。

AWS适用于 AWS RAM 的托管策略

AWS Resource Access Manager 目前提供了几个 AWS RAM 托管策略，本主题将对此进行介绍。

AWS 托管策略

- AWS 托管策略：AWSResourceAccessManagerReadOnlyAccess
- AWS 托管策略：AWSResourceAccessManagerFullAccess
- AWS 托管策略：AWSResourceAccessManagerResourceShareParticipantAccess

- AWS 托管策略：AWSResourceAccessManagerServiceRolePolicy
- 对 AWS 托管式策略的 AWS RAM 更新

在上面的列表中，您可以将前三个策略附加到您的 IAM 角色、组和用户以授予权限。列表中的最后一个策略是为 AWS RAM 服务的服务相关角色保留的。

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

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

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

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略：AWSResourceAccessManagerReadOnlyAccess

您可以将 `AWSResourceAccessManagerReadOnlyAccess` 策略附加得到 IAM 身份。

此策略为您的 AWS 账户所拥有的资源共享提供只读权限。

方法为：授予运行任何 `Get*` 或 `List*` 操作的权限。它不提供修改任何资源共享的任何功能。

权限详细信息

此策略包含以下权限。

- `ram` - 允许主体查看有关账户拥有的资源共享的详细信息。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:Get*",
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "*"
```

```
        }
    ]
}
```

AWS 托管策略：AWSResourceAccessManagerFullAccess

您可以将 AWSResourceAccessManagerFullAccess 策略附加得到 IAM 身份。

此策略提供查看或修改您拥有的资源共享的完全管理权限AWS 账户。

方法为：授予运行任何 ram 操作的权限。

权限详细信息

此策略包含以下权限。

- ram - 允许主体查看或修改有关 AWS 账户所拥有的资源共享的任何信息。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 托管策略：AWSResourceAccessManagerResourceShareParticipantAccess

您可以将 AWSResourceAccessManagerResourceShareParticipantAccess 策略附加得到 IAM 身份。

该策略使主体能够接受或拒绝与此 AWS 账户共享的资源共享，以及查看有关这些资源共享的详细信息。它不提供修改这些资源共享的任何功能。

方法为：授予运行一些 ram 操作的权限。

权限详细信息

此策略包含以下权限。

- ram - 允许主体接受或拒绝资源共享邀请，以及查看有关与账户共享的资源共享的详细信息。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:GetResourcePolicies",
                "ram:GetResourceShareInvitations",
                "ram:GetResourceShares",
                "ram:ListPendingInvitationResources",
                "ram:ListPrincipals",
                "ram:ListResources",
                "ram:RejectResourceShareInvitation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 托管策略：AWSResourceAccessManagerServiceRolePolicy

AWS 托管策略 AWSResourceAccessManagerServiceRolePolicy 只能与 AWS RAM 的服务相关角色一起使用。您不能附加、分离、修改或删除此策略。

此策略向 AWS RAM 提供对组织结构的只读访问权限。启用 AWS RAM 和 AWS Organizations 之间的集成后，AWS RAM 会自动创建一个名为 AWSServiceRoleForResourceAccessManager 的服务相关角色，服务会在需要查找有关您的组织及其账户的信息（例如，在 AWS RAM 控制台中查看组织结构时）时使用该角色。

方法为：授予只读权限来运行 organizations:Describe 和 organizations:List 操作，以提供组织结构和账户的详细信息。

权限详细信息

此策略包含以下权限。

- organizations - 允许主体查看有关组织结构的信息，包括组织单位及其包含的 AWS 账户。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListRoots"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
            ]
        }
    ]
}
```

对 AWS 托管式策略的 AWS RAM 更新

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

更改	说明	日期
AWS Resource Access Manager 已开启跟踪更改	AWS RAM 记录了其现有的托管策略并开始跟踪更改。	2021 年 9 月 16 日

对 AWS RAM 使用服务相关角色

AWS Resource Access Manager 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 AWS RAM 服务直接相关。服务相关角色由 AWS 预定义，并包含 AWS RAM 代表您调用其他 AWS 服务所需的一切权限。

服务相关角色使 AWS RAM 的配置更轻松，因为您不必手动添加必要的权限。AWS RAM 定义其服务相关角色的权限，除非另行定义，否则仅 AWS RAM 可以代入其服务相关角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的 AWS 服务并查找 Service-Linked Role（服务相关角色）列中显示为 Yes（是）的服务。请选择 Yes 与查看该服务的服务相关角色文档的链接。

适用于 AWS RAM 的服务相关角色权限

当您启用与 AWS Organizations 的共享时，AWS RAM 使用名为 `AWSServiceRoleForResourceAccessManager` 的服务相关角色。此角色向 AWS RAM 服务授予查看组织详细信息的权限，例如，成员账户列表以及每个账户所在的组织单位。

此服务相关角色仅信任以下服务来担任该角色：

- `ram.amazonaws.com`

名为 AWSResourceAccessManagerServiceRolePolicy 的角色权限策略附加到此服务相关角色，并允许 AWS RAM 对指定资源完成以下操作：

- 操作：只读操作，用于检索有关组织结构的详细信息。有关操作的完整列表，您可以在 IAM 控制台中查看策略：AWSResourceAccessManagerServiceRolePolicy。

如果主体要在组织内启用 AWS RAM 共享，则该主体（IAM 实体，如用户、组或角色）必须具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 AWS RAM 创建服务相关角色

无需手动创建服务相关角色。在 AWS Management Console 中开启组织内部 AWS RAM 共享，或者使用 AWS CLI 或 AWS API 在账户中运行 EnableSharingWithAwsOrganization 时，AWS RAM 会为您创建服务相关角色。

如果您删除此服务相关角色，则 AWS RAM 不再有权查看组织结构的详细信息。

为 AWS RAM 编辑服务相关角色

AWS RAM 不允许您编辑 AWSResourceAccessManagerServiceRolePolicy 服务相关角色。创建服务相关角色后，将无法更改角色名称，因为可能有多个实体引用该角色。但是可以使用 IAM 编辑角色说明。有关更多信息，请参见 IAM 用户指南中的编辑服务相关角色。

删除 AWS RAM 的服务相关角色

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。

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 `AWSResourceAccessManagerServiceRolePolicy` 服务相关角色。有关更多信息，请参见 IAM 用户指南中的删除服务相关角色。

AWS RAM 服务相关角色支持的区域

AWS RAM 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 AWS 中的 Amazon Web Services 一般参考 区域和终端节点。

AWS RAM 的 IAM 策略示例

本主题包括用于 AWS RAM 演示共享特定资源和资源类型以及限制共享的 IAM 策略示例。

IAM 策略的示例

- 示例 1：允许共享特定资源
- 示例 2：允许共享特定资源类型
- 示例 3：限制与外部 AWS 账户的共享

示例 1：允许共享特定资源

您可以使用 IAM 权限策略，将主体限制为只将特定资源与资源共享关联。

例如，以下策略将主体限制为只与指定的 Amazon 资源名称 (ARN) 共享解析程序规则。如果请求不包含 `ResourceArn` 参数，或者请求中包含该参数，且其值与指定的 ARN 完全匹配，则运算符 `StringEqualsIfExists` 允许该请求。

有关何时以及为何使用 `...IfExists` 运算符的更多信息，请参阅《IAM 用户指南》中的 ...IfExists 条件运算符。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:ResourceArn": "arn:aws:route53resolver:us-
west-2:123456789012:resolver-rule/rslvr-rr-5328a0899aexample"
            }
        }
    }]
}
```

示例 2：允许共享特定资源类型

您可以使用 IAM 策略，将主体限制为只将特定资源类型与资源共享关联。

例如，以下策略将主体限制为只共享解析程序规则。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
        }
    }]
}
```

示例 3：限制与外部 AWS 账户的共享

您可以使用 IAM 策略，防止主体与其 AWS 组织外部的 AWS 账户共享资源。

例如，以下 IAM 策略防止主体向资源共享添加外部 AWS 账户。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "ram:CreateResourceShare",
        "Resource": "*",
        "Condition": {
            "Bool": {
                "ram:RequestedAllowsExternalPrincipals": "false"
            }
        }
    }]
}
```

AWS Organizations 和的服务控制策略示例 AWS RAM

AWS RAM 支持服务控制策略 (SCPs)。SCPs是您附加到组织中元素的策略，用于管理该组织内的权限。SCP应用于您所连接的元素 AWS 账户 下的所有内容SCP。SCPs集中控制组织中所有账户的最大可用权限。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SCPs，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》中的启用组织中的所有功能。
- 启用SCPs以便在您的组织内使用。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。
- 创建你SCPs需要的。有关创建的更多信息SCPs，请参阅《AWS Organizations 用户指南》SCPs中的创建和更新。

示例服务控制策略

目录

- 示例 4：阻止与整个组织或组织单位共享
- 示例 5：仅允许与特定主体共享

以下示例展示如何能控制组织中资源共享的各个方面。

示例 1：阻止外部共享

以下内容SCP禁止用户创建允许与共享用户组织之外的委托人共享的资源共享。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

示例 2：阻止用户接受来自组织外部账户的资源共享邀请

以下内容SCP阻止受影响账户中的任何委托人接受使用资源共享的邀请。共享给与共享账户所在组织中的其他账户的资源共享不会生成邀请，因此不受此影响SCP。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ram:AcceptResourceShareInvitation",
            "Resource": "*"
        }
    ]
```

```
}
```

示例 3：允许特定账户共享特定资源类型

以下内容仅SCP允许账户111111111111创建共享 Amazon EC2 前缀列表或将前缀列表与现有资源共享关联的新资源共享。222222222222

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEqualsIfExists": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

示例 4：阻止与整个组织或组织单位共享

以下内容SCP禁止用户创建与整个组织或任何组织单位共享资源的资源共享。用户可以与组织 AWS 账户 中的个人共享，也可以与IAM角色或用户共享。

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

```
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

示例 5：仅允许与特定主体共享

以下示例仅SCP允许用户与o-12345abcdef,组织组织单位ou-98765fedcba和共享资源 AWS 账户111111111111。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:AssociateResourceShare",
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ram:Principal": [
            "arn:aws:organizations::123456789012:organization/o-12345abcdef",
            "arn:aws:organizations::123456789012:ou/o-12345abcdef/ou-98765fedcba",
            "111111111111"
          ]
        },
        "Null": {
          "ram:Principal": "false"
        }
```

```
      }
    }
  ]
}
```

禁用与 AWS Organizations 的资源共享

如果您之前启用了与 AWS Organizations 的共享，且不再需要与整个组织或组织单位 (OU) 共享资源，可以禁用共享。禁用与 AWS Organizations 的共享时，所有组织或 OU 都将从您创建的资源共享中删除，并且他们将无法访问共享资源。

要禁用与 AWS Organizations 的共享，请执行以下操作：

1. 使用 AWS Organizations disable-aws-service-accessAWS CLI 命令，禁用对 AWS Organizations 的可信访问。

   ```
   $  aws organizations disable-aws-service-access --service-principal
    ram.amazonaws.com
   ```

   > **Important**
   >
   > 当您禁用对 AWS Organizations 的可信访问后，将从所有资源共享中删除您组织内的主体，他们将无法访问这些共享的资源。

2. 使用 IAM 控制台、AWS CLI 或 IAM API 操作，删除 AWSServiceRoleForResourceAccessManager 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。

登录和监控 AWS RAM

监控是维护 AWS 解决方案的可靠性、可用性和性能的重要组成部分。 AWS RAM 您应该从 AWS 解决方案的各个部分收集监控数据，以便在出现多点故障时可以更轻松地进行调试。 AWS 提供了多种用于监控您的 AWS RAM 资源和应对潜在事件的工具：

Amazon EventBridge

提供描述 AWS 资源变化的系统事件 near-real-time流。 EventBridge 启用事件驱动的自动计算，因为您可以编写规则来监视某些事件，并在这些事件发生时在其他 AWS 服务中触发自动操作。有关更多信息，请参阅 AWS RAM 使用监控 EventBridge。

AWS CloudTrail

捕获由您或代表您发出的API调用和相关事件， AWS 账户 并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 使用 AWS RAM 记录 AWS CloudTrail API 调用。

AWS RAM 使用监控 EventBridge

使用 Amazon EventBridge，您可以在中为特定事件设置自动通知 AWS RAM。来自 AWS RAM 的事件以近乎实时 EventBridge 的方式传送到。您可以配置 EventBridge 为监控事件并调用目标以响应表明您的资源共享发生变化的事件。对资源共享进行更改会针对资源共享的所有者以及获授权访问资源共享的主体触发事件。

当您创建事件模式时，源为 `aws.ram`。

> **Note**
>
> 在编写依赖于这些事件的代码时要小心。这些事件不能得到保证，但会尽最大努力发出。如果 AWS RAM 尝试发出事件时出现错误，则服务会再尝试几次。但是，它可能会超时并导致该特定事件丢失。

有关更多信息，请参阅 Amazon EventBridge 用户指南。

示例：在资源共享失败时发出警报

考虑一下您想要与组织中的其他账户共享 Amazon EC2 容量预留的场景。这样做是降低成本的好方法。

但是，如果您不满足共享容量预留的所有先决条件，则共享资源所涉及的异步任务执行可能会静默失败。如果共享操作失败，而您在其他账户中的用户尝试使用其中一个容量预留启动实例，那么 Amazon的EC2行为就好像容量预留已满，而是将该实例作为按需实例启动。这可能导致成本高于预期。

要监控资源共享故障，请设置 Amazon EventBridge 规则，在 AWS RAM 资源共享失败时提醒您。以下教程过程使用 Amazon 简单通知服务 (SNS) 主题在 EventBridge 发现资源共享失败时通知所有主题订阅者。有关亚马逊的更多信息SNS，请参阅《亚马逊简单通知服务开发者指南》。

要创建在资源共享失败时通知您的规则，请执行以下操作：

1. 打开 Amazon EventBridge 控制台。

2. 在导航窗格中，选择规则，然后在规则列表中，选择创建规则。
3. 输入规则的名称和描述（可选），然后选择下一步。
4. 向下滚动到事件模式框，然后选择自定义模式（JSON编辑器）。
5. 复制并粘贴以下事件模式：

```
{
  "source": ["aws.ram"],
  "detail-type": ["Resource Sharing State Change"],
  "detail": {
    "event": ["Resource Share Association"],
    "status": ["failed"]
  }
}
```

6. 选择下一步。
7. 对于目标 1，在目标类型下选择 AWS 服务。
8. 在 “选择目标” 下，选择SNS主题。
9. 在 “主题” 中，选择要向其发布通知的主SNS题。此主题必须已经存在。
10. 选择下一步，然后再次选择下一步，以查看您的配置。
11. 如果您对选项感到满意，请选择创建规则。
12. 返回到规则页面，确保将您的新规则标记为已启用。如有必要，选择规则名称旁边的单选按钮，然后选择启用。

只要启用该规则，任何失败的 AWS RAM 资源共享都会向您发布到的主题的收件人SNS发出警报。

您还可以尝试在亚马逊EC2控制台中通过共享容量预留的账户查看共享容量预留，从而确认共享容量预留是否可供这些账户访问。

使用 AWS RAM 记录 AWS CloudTrail API 调用

AWS RAM 与 AWS CloudTrail 集成，后者是在 AWS 中记录用户、角色或 AWS RAM 服务所执行操作的服务。CloudTrail 将 AWS RAM 的所有 API 调用作为事件捕获。捕获的调用包含来自 AWS RAM 控制台和代码的 AWS RAM API 操作调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到您指定的 Amazon S3 存储桶（包括 AWS RAM 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。使用 CloudTrail 收集的信息确定向 AWS RAM 发出了什么请求、发出请求的 IP 地址、请求者、发出请求的时间以及其他详细信息。

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

CloudTrail 中的 AWS RAM 信息

在您创建 AWS 账户 时，将在该账户上启用 CloudTrail。当 AWS RAM 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其它 AWS 服务事件一同保存在 Event history（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。

对于AWS 账户中的事件的持续记录（包括 AWS RAM 的事件），请创建跟踪记录。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时，此跟踪应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 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，请参阅下列内容：

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

CloudTrail 记录所有 AWS RAM 操作，AWS RAM API 参考中介绍了这些操作。例如，对 `CreateResourceShare`、`AssociateResourceShare` 和 `EnableSharingWithAwsOrganization` 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。

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

了解 AWS RAM 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。

以下示例显示了用于 `CreateResourceShare` 操作的 CloudTrail 日志条目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "NOPIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/admin",
        "accountId": "111122223333",
        "accessKeyId": "BCDIOSFODNN7EXAMPLE",
        "userName": "admin"
    },
    "eventTime": "2018-11-03T04:23:19Z",
    "eventSource": "ram.amazonaws.com",
    "eventName": "CreateResourceShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.1.0",
    "userAgent": "aws-cli/1.16.2 Python/2.7.10 Darwin/16.7.0 botocore/1.11.2",
    "requestParameters": {
        "name": "foo"
    },
    "responseElements": {
        "resourceShare": {
            "allowExternalPrincipals": true,
            "name": "foo",
            "owningAccountId": "111122223333",
            "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
EXAMPLE0-1234-abcd-1212-987656789098",
            "status": "ACTIVE"
        }
    },
    "requestID": "EXAMPLE0-abcd-1234-mnop-987654567876",
    "eventID": "EXAMPLE0-1234-abcd-hijk-543234565434",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

AWS RAM 中的故障恢复能力

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

有关AWS 区域和可用区的更多信息，请参阅AWS全球基础设施。

中的基础设施安全 AWS RAM

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

您可以使用 AWS 已发布的API呼叫 AWS RAM 通过网络进行访问。客户端必须支持以下内容：

- 传输层安全 (TLS)。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 具有完美前向保密性的密码套件 ()，例如（Ephemeral Diffie-HellmanPFS）或（Elliptic C DHE urve Ephemeral Diffie-Hellman）。ECDHE大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

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

访问 AWS Resource Access Manager 使用接口端点 (AWS PrivateLink)

您可以使用 … AWS PrivateLink 在您的VPC和之间创建私人连接 AWS Resource Access Manager。你可以访问 AWS RAM 就好像它在你的里面一样VPC，无需使用互联网网关、NAT设备、VPN连接或 AWS Direct Connect 连接。你中的实例VPC不需要公有 IP 地址即可访问 AWS RAM.

您可以通过创建接口端点来建立此私有连接，该端点由提供支持 AWS PrivateLink。 我们在您为接口终端节点启用的每个子网中创建一个终端节点网络接口。这些是请求者管理的网络接口，可用作发往的流量的入口点 AWS RAM.

有关更多信息，请参阅访问权限 AWS 服务 通过 AWS PrivateLink中的 AWS PrivateLink 指南。

的注意事项 AWS RAM

在为设置接口终端节点之前 AWS RAM，请查看《注意事项》AWS PrivateLink 指南。

AWS RAM 支持通过接口端点调用其所有API操作。

VPC支持终端节点策略 AWS RAM。 默认情况下，具有完全访问权限 AWS RAM 允许通过接口端点。

为创建接口终端节点 AWS RAM

您可以为创建接口终端节点 AWS RAM 使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI)。 有关更多信息，请参阅中的创建接口终端节点 AWS PrivateLink 指南。

为创建接口终端节点 AWS RAM 使用以下服务名称：

```
com.amazonaws.region.ram
```

如果您DNS为接口终端节点启用私有功能，则可以向发出API请求 AWS RAM 使用其默认的区域DNS名称。例如，`ram.us-east-1.amazonaws.com`。

为 VPC 端点创建端点策略

终端节点策略是您可以附加到接口终端节点的IAM资源。默认终端节点策略允许对以下内容的完全访问权限 AWS RAM 通过接口端点。控制允许的访问权限 AWS RAM 从您的VPC，将自定义终端节点策略附加到接口终端节点。

端点策略指定以下信息：

- 可以执行操作的委托人 (AWS 账户、IAM用户和IAM角色）。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅中的使用终端节点策略控制对服务的访问权限 AWS PrivateLink 指南。

示例：的VPC终端节点策略 AWS RAM actions

以下是自定义端点策略的示例。当您将此策略附加到您的接口终端节点时，它会授予对所列内容的访问权限 AWS RAM 所有委托人对所有资源执行操作。

```
{
```

```
    "Version": "2012-10-17",
    "Statement":
        [
            {
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "ram:CreateResourceShare"
            ],
            "Resource": "*"
            }
        ]
}
```

对问题进行故障排除 AWS RAM

使用本指南本节中的信息来帮助您在使用 AWS Resource Access Manager (AWS RAM) 时诊断和修复常见问题。

主题

错误：“Your account ID does not exist in an AWS organization”

场景

尝试与组织中的账户或 AWS 组织单位 (OUs) 共享资源时，会出现 “您的账户 ID 在组织中不存在” 错误。

原因

如果您在和之间 AWS Resource Access Manager 启用集成时AWSServiceRoleForResourceAccessManager未成功创建服务相关角色，则可能会发生此错误。AWS Organizations

解决方案

要重新创建所需的服务相关角色，请按以下步骤操作，关闭集成，然后再次将其打开。

> **Important**
>
> 禁用对的可信访问权限后 AWS Organizations，组织内的委托人将从所有资源共享中删除，并失去对这些共享资源的访问权限。

1. 使用具有管理权限的IAM角色或用户登录您的组织管理帐户。
2. 在AWS Organizations 控制台中导航到服务页面。
3. 选择RAM。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 导航到AWS RAM 控制台中的设置页面。
6. 选中 “启用与之共享” 复选框 AWS Organizations，然后选择 “保存设置”。

现在，您应该 AWS RAM 能够使用与账户和OUs组织内部共享您的资源。

错误：“AccessDeniedException”

场景

尝试共享资源或查看资源共享时，您会收到 Access Denied 异常。

原因

如果您在没有所需权限的情况下尝试创建资源共享，则可能会收到此错误。这可能是由于附加到您的 AWS Identity and Access Management (IAM) 委托人的策略权限不足造成的。这也可能是因为 AWS Organizations 服务控制策略 (SCP) 中存在的限制会影响您 AWS 账户。

解决方案

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

  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。
- IAM通过身份提供商管理的用户：

  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）中的说明进行操作。

- IAM用户：
  - 创建您的用户可以担任的角色。按照《用户指南》中为IAM用户创建角色中的IAM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《用户指南》中向用户（控制台）添加权限中的IAM说明进行操作。

要解决此错误，您需要确保由发出请求的主体所使用的权限策略中的 `Allow` 语句授予权限。此外，您的组织不得阻止这些权限SCPs。

要创建资源共享，您需要以下两种权限：

- `ram:CreateResourceShare`

- `ram:AssociateResourceShare`

要查看资源共享，您需要以下权限：

- `ram:GetResourceShares`

要向资源共享附加权限，您需要以下权限：

- *`resourceOwningService`*`:`*`PutPolicyAction`*

  这是一个占位符。必须将其替换为拥有您要共享的资源的服务的 PutPolicy “” 权限（或等效权限）。例如，如果您要共享 Route 53 Resolver 规则，则所需的权限将是：`route53resolver:PutResolverRulePolicy`。如果要允许创建包含多种资源类型的资源共享，则必须包括要允许的每种资源类型的相关权限。

以下示例显示了这样的IAM权限策略可能是什么样子。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare",
                "ram:GetResourceShares",
```

```
                "resourceOwningService:PutPolicyAction"
            ],
            "Resource": "*"
        }
    ]
}
```

错误：“UnknownResourceException”

场景

您会收到以下错误之一：

- “CannotCreateResourceShare: UnknownResourceException: OrganizationalUnit ou-*xxxx* 找不到”
- “CannotUpdateResourceShare: UnknownResourceException: OrganizationalUnit ou-*xxxx* 找不到”。

原因

如果您使用 Organizations 控制台或 Organizations E A nableAWSService ccess API 而不是使用控制台来启用 AWS RAM 和 AWS Organizations 之间的集成，则可能会发生这些错误。 AWS RAM 当您使用 Organizations 控制台或启用集成时API，该服务不会在您的账户中创建AWSServiceRoleForResourceAccessManager角色。需要该角色才能访问有关您组织的信息。由于该角色尚未创建，因此 AWS RAM 无法访问有关组织中账户或组织单位 (OUs) 的详细信息。

解决方案

要解决此问题，请关闭 AWS RAM 和之间的集成 AWS Organizations。然后通过调用 AWS RAM EnableSharingWithAwsOrganizationAPI操作或使用执行以下步骤再次将其打开。 AWS Management Console

> **Important**
>
> 禁用对的可信访问权限后 AWS Organizations，组织内的委托人将从所有资源共享中删除，并失去对这些共享资源的访问权限。

1. 使用具有管理权限的IAM角色或用户登录您的组织管理帐户。

2. 在AWS Organizations 控制台中导航到服务页面。
3. 选择RAM。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 导航到AWS RAM 控制台中的设置页面。
6. 选中 “启用与之共享” 复选框 AWS Organizations，然后选择 “保存设置”。

现在，您应该 AWS RAM 能够使用与账户和OUs组织内部共享您的资源。

尝试与组织之外的账户共享时出错

场景

尝试与组织之外的账户共享资源时，您会收到以下错误之一：

- “You cannot share the resource outside your organization.”
- “您尝试共享的资源只能在您的 AWS 组织内共享。“
- “InvalidParameterException: 委托人账户 ID 不在您的 AWS 组织中。You do not have permission to add external AWS 账户 to a resource share.”
- “OperationNotPermittedException: 您尝试共享的资源只能在您的 AWS 组织内共享。“

可能的原因和解决方案

某些资源类型只能与同一组织中的账户共享

某些资源类型不能与任何不是该组织成员的账户共享。具有此限制的示例资源类型是属于亚马逊弹性计算云 (AmazonVPCs) 的虚拟私有连接 (EC2)。

要验证您是否可以与组织外部的账户和主体共享特定资源类型，请参阅可共享的 AWS 资源。

服务相关角色创建不成功

如果您在和之间 AWS RAM 启用集成时`AWSServiceRoleForResourceAccessManager`未成功创建服务相关角色，则可能会出现此问题。 AWS Organizations

如果您在尝试与属于 您组织的账户共享资源时收到其中一个错误，请按以下步骤操作，删除并重新创建服务相关角色。

> **Important**
>
> 禁用对的可信访问权限后 AWS Organizations，组织内的委托人将从所有资源共享中删除，并失去对这些共享资源的访问权限。

1. 使用具有管理权限的IAM角色或用户登录您的组织管理帐户。
2. 在AWS Organizations 控制台中导航到服务页面。
3. 选择RAM。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 导航到AWS RAM 控制台中的设置页面。
6. 选中 “启用与之共享” 复选框 AWS Organizations，然后选择 “保存设置”。

看不到目标账户中的共享资源

场景

用户看不到他们认为通过其他 AWS 账户与自己共享的资源。

可能的原因和解决方案

与共享 AWS Organizations 是通过使用 Organizations 开启的，而不是 AWS RAM

如果 AWS Organizations 是通过使用 Organizations 代替开启的 AWS RAM，则组织内部共享将失败。要检查这是否是导致问题的原因，请导航到AWS RAM 控制台中的 “设置” 页面，并确认选中 “启用共享对象” 复选 AWS Organizations框。

- 如果选中了该复选框，则这不是原因。
- 如果未选中该复选框，则可能是原因所在。暂时不要选中该复选框。按以下步骤操作，纠正这种情况。

> **Important**
>
> 禁用对的可信访问权限后 AWS Organizations，组织内的委托人将从所有资源共享中删除，并失去对这些共享资源的访问权限。

1. 使用具有管理权限的IAM角色或用户登录您的组织管理帐户。
2. 在AWS Organizations 控制台中导航到服务页面。
3. 选择RAM。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 导航到AWS RAM 控制台中的设置页面。
6. 选中 “启用与之共享” 复选框 AWS Organizations，然后选择 “保存设置”。

您可能需要更新共享并指定组织内要与之共享的账户或组织单位。

资源共享未将此账户指定为主体

在 AWS 账户 创建资源共享的中，在AWS RAM 控制台中查看资源共享。检查无法访问资源的账户是否被列为主体。如果不是，请更新共享，将账户添加为主体。

账户中的角色或用户没有所需的最低权限

当您将账户 A 中的资源共享给另一个账户 B 时，账户 B 中的角色和用户不会自动获得对共享中资源的访问权限。账户 B 的管理员必须首先向账户 B 中需要访问资源的IAM角色和用户授予权限。例如，以下策略显示了如何向账户 B 中的角色和用户授予账户 A 中资源的只读访问权限。该策略通过其 Amazon 资源名称 (ARN) 指定资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:Get*",
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:<service>:<Region-code>:<Account-A-ID>:<resource-id>"
        }
    ]
}
```

资源位于与当前控制台设置不同的 AWS 区域 中

AWS RAM 是一项区域服务。资源存在于特定区域 AWS 区域，要查看它们， AWS Management Console 必须将其配置为查看该区域中的资源。

控制台当前 AWS 区域 正在访问的显示在控制台的右上角。要对其进行更改，请选择当前的区域名称，然后从下拉菜单中选择要查看其资源的区域。

错误：超出限制

场景

尝试共享资源时，您会收到 “您已达到可以共享的资源数量限制 ResourceShareLimitExceededException” 或 “”。

原因

当您使用 AWS RAM 服务或创建您尝试共享的资源的服务达到可以共享的最大资源数量时 AWS 服务 ，就会发生这些错误。此配额（以前称为限制）可能会影响共享账户或您与之共享资源的账户。

解决方案

1. 要查看您的配额，请在您看到错误 AWS 账户 的地方导航到以下页面之一，具体取决于您达到的配额类型：
   - 服务限额控制台的AWS RAM 页面
   - 其资源受到配额影响的 AWS 服务的页面
2. 向下滚动并选择相关配额。
3. 如果该配额可用，请选择请求增加配额。
4. 输入新的配额值，然后选择请求。
5. 该请求将显示在配额请求历史记录页面上，您可以在其中查看请求的状态，直到请求最终完成。

我组织中的其他账户从未收到邀请

场景

您与 AWS Organizations管理的同一组织中的其他账户共享资源时，这些账户不会收到邀请。

原因

如果您的账户开启了 AWS 组织内部的共享，则这是预期行为。

如果此选项处于启用状态，并且您与组织中的其他账户共享，则不会发送邀请，用户也无需接受。您在资源共享中作为主体引用的所有组织账户都可以立即开始访问共享中的资源。

如果您的账户尚未在 AWS 组织内开启共享，那么当您与其他账户共享时，即使他们属于同一个 AWS 组织，它们也会被视为独立账户。会发送邀请，用户必须先接受邀请，然后才能访问共享中的资源。

你不能共享子VPC网

场景

当您 AWS RAM 尝试使用与其他账户共享子VPC网时，共享操作会成功。但是， AWS RAM 控制台中会显示`LIMIT EXCEEDED`该资源的使用者账户。

原因

某些资源类型具有与强制执行的限制不同的特定于服务的限制。 AWS RAM即使您尚未达到 AWS RAM中的限制之一，其中一些限制也可以有效地阻止共享。限额就是这些限制的一个示例。Amazon Virtual Private Cloud（亚马逊VPC）限制了您可以与其他个人账户共享的子网数量。如果您尝试与已包含最大子网数量的使用账户共享子网，则该使用账户会在控制台中显示该资源的 `LIMIT EXCEEDED`。有关此限制的更多信息，请参阅《亚马逊虚拟私有云用户指南》中的 “亚马逊VPC配额 —— VPC 共享”。

要解决这个问题，请先检查可能与受影响的账户共享指定资源的其他资源共享，然后移除那些您可能不再需要的共享。您也可以请求提高支持调整的限额。使用服务限额控制台请求增加限额。

> **Note**
>
> AWS RAM 不会自动检测限制增加的变化。您必须将资源或委托人重新关联到资源共享RAM才能检测到更改。

AWS RAM 的服务限额

您的 AWS 账户具有以下与 AWS Resource Access Manager (AWS RAM) 相关的限制。您可以请求增加部分限制的值。要请求提高限制，请联系 Support。

Note

以下定义适用于以下配额中的描述：

- 资源 - 您要共享的单个 AWS 服务创建的元素，例如 Amazon S3 存储桶或 Amazon EC2 实例。资源共享中引用的每个资源都会计入此配额。如果您在三个不同的资源共享中共享同一个资源，则该配额的数量增加三个。
- 资源共享 - AWS RAM 创建的容器，可用于共享资源。每个资源共享（无论其包含多少资源）都计入您的配额。
- 共享的主体 - 您与资源共享关联的标识符。这可以是 AWS Identity and Access Management (IAM) 角色或用户、AWS 账户标识符、组织单位或整个组织。您在资源共享中引用的每个共享主体都会为您的配额使用量增加一个。如果您通过引用其 ID 与整个组织共享，则其在此配额中仅计为一个。
- 客户托管权限 - 您创建的托管权限，用于解决通过最低权限访问来管理共享资源使用方式的特定使用案例。

资源	默认限制
每个 AWS 区域资源共享的最大数量	25000
每个资源共享的最大资源关联数	5000
每个资源共享的最大主体关联数	5000
客户托管权限的最大数量	1500
每种资源类型的最大客户托管权限数	10
每个客户托管权限的最大版本数量	5
一个 AWS 区域中所有资源共享的最大资源关联数	25000

资源	默认限制
Note 资源共享中包含的每个资源都计入此限制。如果某项资源包含在 10 个不同的资源共享中，则将 10 计入该限制中。	
一个 AWS 区域中所有资源共享的最大主体关联数 **Note** 资源共享中包含的每个主体都计入此限制。如果某个主体包含在 10 个不同的资源共享中，则将 10 计入该限制中。	25000
每个共享账户的最大待接受邀请数 • 此配额仅适用于与不属于同一 AWS Organizations 的账户共享的发送 账户。 • 对于接收账户可以有多少个待接受邀请，没有配额。 • 在属于同一 AWS Organizations 的账户之间共享并且 AWS Organizations 内的资源共享处于启用状态时，不 使用邀请。	250

将 AWS RAM 与 AWS 开发工具包配合使用

AWS 软件开发工具包（SDK）适用于许多常用编程语言。每个软件开发工具包都提供 API、代码示例和文档，使开发人员能够以其首选语言构建应用程序。

软件开发工具包文档	代码示例
AWS SDK for C++	AWS SDK for C++ 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 .NET	AWS SDK for .NET 代码示例
AWS SDK for PHP	AWS SDK for PHP 代码示例
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

可用性示例

找不到所需的内容？ 请求提供包含反馈链接的代码示例。

《AWS RAM 用户指南》的文档历史记录

下表描述了 AWS Resource Access Manager 文档的重要补充。我们还更新文档来处理发送给我们的反馈意见。

要获得有关这些更新的通知，您可以订阅 AWS RAM RSS Feed。

变更	说明	日期
增加了对共享 AWS Billing 资源的支持。	现在，您可以与组织 AWS 账户 中的其他人共享 AWS Billing 视图。	2024年12月20日
增加了对共享 Amazon API Gateway 资源的支持。	现在，您可以与其他人共享API网关域名 AWS 账户 或在您的组织内共享 Gateway 域名。	2024 年 11 月 21 日
增加了对共享 Amazon VPC 资源的支持。	现在，您可以与其他人 AWS 账户 或在您的组织内共享 Amazon VPC 安全组。	2024 年 10 月 30 日
增加了对共享 AWS End User Messaging SMS 资源的支持。	您可以与其他人 AWS 账户 或您的组织共享 AWS End User Messaging SMS 资源 AWS RAM。	2024 年 9 月 24 日
AWS PrivateLink	使用 f AWS PrivateLink or AWS RAM，您可以使用虚拟私有云中的接口终端节点直接连接 (VPC)。RAM	2024 年 9 月 9 日
增加了对共享的支持 AWS Backup。	您可以在组织内部 AWS 账户 或组织内部共享逻辑上存在气隙的保管库。	2024 年 8 月 7 日
增加了对共享 Amazon Bedrock 定制模型的支持	现在，您可以使用与其他 AWS RAM 人 AWS 账户 以及您的组	2024 年 8 月 1 日

	织共享 Amazon Bedrock 自定义模型。	
增加了对共享 AWS CloudHSM 备份的支持。	您可以与其他人 AWS 账户 或您的组织共享 AWS CloudHSM 备份 AWS RAM。	2024 年 6 月 28 日
增加了对共享 Amazon A SageMaker I 的支持 Model Registry 资源。	现在，您可以在组织内部 AWS 账户 或组织内部安全高效地共享高级参数。	2024 年 6 月 27 日
增加了对共享 Amazon A SageMaker I 的支持 JumpStart。	现在，您可以与您的组织共享 AWS 账户 或在组织内部共享 SageMaker Amazon AI JumpStart Hubs。	2024 年 6 月 27 日
增加了对共享的支持 Amazon Route 53 ResolverProfiles.	你现在可以 AWS RAM 用来分享 Amazon Route 53 Resolver Profiles 与组织 AWS 账户 内的其他人共享。	2024 年 4 月 22 日
增加了对共享 AWS Systems Manager 参数存储资源的支持。	现在，您可以在组织内部 AWS 账户 或组织内部安全高效地共享高级参数。	2024 年 2 月 21 日
增加了对共享 Amazon 以FSx获取打开ZFS快照的支持。	现在，您可以与组织 AWS 账户 内的其他人共享 Amazon f FSx o ZFS r Open Snapshots 。	2023 年 12 月 19 日
增加了对共享 Amazon Simple Storage Service 资源的支持。	现在，您可以与其他人 AWS 账户 或您的组织共享 Amazon Simple Storage Service 访问权限授予实例 AWS RAM。	2023 年 11 月 27 日
增加了对共享 AWS 资源探索器 视图的支持。	现在，您可以与组织 AWS 账户 内的其他人共享 AWS 资源探索器 视图。	2023 年 11 月 14 日

增加了对共享 Amazon 应用程序恢复控制器 (ARC) 资源的支持。	现在，您可以与其他人 AWS 账户 或您的组织共享 Amazon 应用程序恢复控制器 (ARC) 集群 AWS RAM。	2023 年 10 月 18 日
增加了对共享 Amazon DataZone 资源的支持。	现在，您可以与其他人 AWS 账户 或您的组织共享 Amazon DataZone 资源。	2023 年 10 月 4 日
增加了对服务主体共享的支持。	现在，您可以将服务主体与资源共享相关联。这允许指定服务代表您管理客户资源的必要操作。	2023 年 8 月 29 日
增加了对共享 SageMaker 模型卡片资源的支持。	现在，您可以与其他人 AWS 账户 或您的组织共享 SageMaker 模型卡资源。	2023 年 8 月 18 日
增加了对 Amazon SageMaker AI 功能商店功能组和 SageMaker AI 目录作为可共享资源的支持。	现在，您可以与其他人 AWS 账户 或您的组织共享 SageMaker Amazon SageMaker AI 功能商店功能组和 AI 目录资源。	2023 年 7 月 20 日
提高待处理邀请的服务配额限制。	每个共享账户的待处理邀请的最大数量已从 20 增加到 250。	2023 年 6 月 8 日
增加了对 AWS AppSync GraphQL APIs 作为可共享资源的支持。	现在，您可以APIs与其他 AWS 账户 人共享 AWS AppSync GraphQL。 AWS RAM	2023 年 5 月 24 日
增加了对 AWS Verified Access 群组作为可共享资源的支持。	现在，您可以集中创建和管理 AWS Verified Access 群组，然后与其他人 AWS 账户 或您的组织共享群组。	2023 年 4 月 27 日

在 AWS RAM 控制台中增加了对客户托管权限的支持。	现在，您可以安全地为支持的资源类型创建和维护精细的资源访问控制。	2023 年 4 月 19 日
增加了对 Amazon VPC Lattice 服务和服务网络可共享资源的支持。	现在，您可以与其他 AWS 账户人共享 Amazon VPC Lattice 服务和服务网络资源。	2023 年 3 月 31 日
增加了对 AWS Marketplace 目录实体作为可共享资源的支持。	现在，您可以在 Marketplace AWS 账户 中与其他人共享您的实体。	2023 年 3 月 27 日
增加了对在 AWS RAM 控制台中管理权限版本的支持。	现在，您可以使用 AWS RAM 控制台查看版本详细信息并将权限更新到指定为默认版本的任何版本。	2023 年 1 月 16 日
IAM最佳实践更新。	更新了指南以符合IAM最佳实践。有关更多信息，请参阅中的安全最佳实践IAM。	2023 年 1 月 3 日
增加了对 Amazon EC2 置放群组作为可共享资源的支持。	现在，您可以与其他人共享 Amazon EC2 置放群组 AWS 账户 ，以便在其中启动他们的实例。	2022 年 11 月 8 日
添加了两个关于的介绍性视频的链接 AWS RAM。	添加了概述视频，这些视频描述 AWS RAM 并提供了与他人共享资源的演练。 AWS 账户	2022 年 8 月 29 日
增加了对 Amazon A SageMaker I 管道的支持。	现在，您可以与其他人共享 SageMaker AI 管道 AWS 账户。	2022 年 8 月 2 日
增加了对 AWS Service Catalog AppRegistry 应用程序和属性组作为可共享资源类型的支持。	现在，您可以与其他人共享 AppRegistry 应用程序和属性组 AWS 账户。	2022 年 6 月 17 日

AWS Resource Access Manager 接收SOC和ISO认证。	AWS RAM 已被证实符合服务组织控制 (SOC) 和国际标准化组织 () 9001、27 ISO 001、ISO 270 ISO 17、ISO 27018 和 27701 标准。ISO ISO	2022 年 5 月 31 日
AWS Resource Access Manager 获得美联储RAMP认证。	AWS RAM 已被证实符合联邦风险和授权管理计划 (FedRAMP) 。	2022 年 4 月 8 日
AWS Resource Access Manager 获得PCIDSS认证。	AWS RAM 已被验证符合支付卡行业 (PCI) 数据安全标准 (DSS)。	2022 年 2 月 27 日
增加了对 Amazon VPC IPAM 资源发现作为可共享资源的支持。此外，您现在可以与组织外部的帐户共享资源IPAM池。	现在，您可以与其他人共享IPAM资源发现 AWS 账户。	2022 年 1 月 25 日
增加了对共享全球资源的支持	现在，您可以与其他人共享全球资源 AWS 账户。	2021 年 12 月 2 日
增加了对 AWS 云WAN核心网络作为可共享的全球资源的支持。	现在，您可以与其他人共享 Cloud WAN 核心网络 AWS 账户。	2021 年 12 月 2 日
支持共享 Amazon VPC IP 地址管理器 (IPAM) 池	您可以使用 AWS RAM 共享 Amazon 资源VPCIPAM池。有关更多信息，请参阅《AWS RAM 用户指南》中的可共享 AWS 资源。	2021 年 12 月 1 日
支持共享 Amazon SageMaker AI 资源	您可以使用共享 AWS RAM A SageMaker I 血统组。有关更多信息，请参阅《AWS RAM 用户指南》中的可共享 AWS 资源。	2021 年 11 月 30 日

Support 支持共享 “ AWS Migration Hub 重构空间” 资源	您可以使用共享 Mig AWS RAM ration Hub 环境。有关更多信息，请参阅《AWS RAM 用户指南》中的可共享 AWS 资源。	2021 年 11 月 29 日
添加了有关 AWS RAMAWS托管IAM权限策略的信息。	已发布有关可用的 AWS托管权限策略的详细信息，您可以在IAM控制台中访问这些策略并附加到您的IAM委托人。 AWS 账户	2021 年 9 月 16 日
增加了对在 Outposts 资源上共享 S3 的支持	现在，你可以使用与其他 AWS RAM 人共享 Outposts 上的 S3。 AWS 账户	2021 年 8 月 5 日
增加了对其他托管权限和与IAM委托人共享资源的支持	对于支持的资源类型，您可以从其他 AWS RAM 托管权限中进行选择，并与各个IAM角色和用户共享资源。	2021 年 6 月 10 日
增加了对共享 S AWS ystems Manager 事件管理器资源的支持	现在，您可以使用 AWS RAM 与其他人共享 AWS Systems Manager 事件管理器的联系人和响应计划 AWS 账户。	2021 年 5 月 10 日
增加了对共享 Amazon Route 53 资源的支持	现在，您可以使用与其他 AWS 账户人共享 Amazon Route 53 解析器DNS防火墙规则组。 AWS RAM	2021 年 3 月 31 日
增加了对共享 AWS Transit Gateway 资源的支持	现在，您可以使用与其他 AWS RAM AWS 账户人共享传输网关组播域。	2020 年 12 月 10 日

增加了对共享 AWS Network Firewall 资源的支持	现在，您可以使用与其他 AWS RAM 人共享 AWS Network Firewall 防火墙策略和规则组 AWS 账户。	2020 年 11 月 17 日
增加了对共享 Outposts 和本地网关路由表的支持	现在，您可以使用与其他 AWS RAM 人共享 Outposts 和本地网关路由表。 AWS 账户	2020 年 10 月 15 日
增加了对共享 Route 53 查询日志的支持	现在，您可以使用与其他 AWS RAM 人共享 Route 53 查询日志 AWS 账户。	2020 年 9 月 7 日
增加了对共享 AWS Private Certificate Authority 资源的支持。	现在，您可以使用与其他 AWS RAM 人共享 AWS 私有 CA 私有证书颁发机构 (CAs) AWS 账户。	2020 年 8 月 17 日
增加了对共享 G AWS lue 数据目录、数据库和表格的支持。	现在，您可以使用与其他 AWS RAM 人共 AWS 享 Glue 数据目录、数据库和表。 AWS 账户	2020 年 7 月 7 日
增加了对共享 Amazon VPC 前缀列表的支持。	现在，您可以使用 AWS RAM 共享前缀列表。	2020 年 6 月 29 日
增加了对共享 AWS Outposts 客户拥有IPv4的地址的支持。	现在，您可以使用与其他 AWS RAM AWS 账户人共享 AWS Outposts 客户拥有IPv4的地址。	2020 年 4 月 22 日
增加了对共享 AWS App Mesh 网格的支持	现在，您可以使用与其他 AWS RAM AWS 账户人共享网格。	2020 年 1 月 17 日
增加了对共享 AWS CodeBuild 项目和报告组的支持	现在 AWS RAM ，您可以使用与其他人共享 AWS CodeBuild 项目和报告组 AWS 账户。	2019 年 12 月 13 日

增加了对共享额外资源的支持	现在，您可以使用 AWS RAM 与其他人共享亚马逊EC2专用主机、 AWS Resource Groups 资源组和 Amazon EC2 Image Builder 组件、图像和图像配方 AWS 账户。	2019 年 12 月 2 日
增加了对共享按需容量预留的支持	现在，您可以使用与其他 AWS RAM 人共享按需容量预留 AWS 账户。	2019 年 7 月 29 日
增加了对共享 Aurora DB 集群的支持	现在，您可以使用与其他 AWS RAM 人共享 Aurora 数据库集群 AWS 账户。	2019 年 7 月 2 日
增加了对共享流量镜像目标的支持	现在，您可以使用与其他 AWS RAM AWS 账户人共享流量镜像目标。	2019 年 6 月 25 日
增加了对共享许可证配置的支持	现在，您可以使用与其他 AWS RAM 人共享 License Manager AWS 许可证配置 AWS 账户。	2018 年 12 月 5 日
增加了对共享子网的支持	现在，您可以使用与其他 AWS RAM AWS 账户人共享 Amazon VPC 子网。	2018 年 11 月 27 日
增加了对共享中转网关的支持	现在，您可以使用与其他 AWS RAM 人共享 Amazon VPC 公交网关 AWS 账户。	2018 年 11 月 26 日
增加了对共享 Resolver 规则的支持	现在，您可以使用与其他 AWS 账户人共享 Route 53 Resolver 规则。 AWS RAM	2018 年 11 月 20 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。