AWS Resource Access Manager

用户指南

AWS Resource Access Manager: 用户指南

Table of Contents

什么是 AWS RAM？

AWS Resource Access Manager (AWS RAM) 可让您与任何 AWS 账户或通过 AWS Organizations 共享您的资源。如果您有多个 AWS 账户，您可以集中创建资源，并使用 AWS RAM 与其他账户共享这些资源。

内容

Benefits

AWS RAM 具备下列优点：

- 减少运营开销 — 集中创建资源，并使用 AWS RAM 与其他账户共享这些资源。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。
- 提供安全性和一致性 — 使用现有策略和权限控制共享资源的消耗，以实现安全性和控制。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 — 通过与 Amazon CloudWatch 和 AWS CloudTrail 集成，查看共享资源的使用详情。AWS RAM 提供了对共享资源和账户的全面深入的了解。

资源共享工作原理

当您与另一个账户共享资源时，将向该账户授予对资源的访问权限。应用于您已共享资源的账户的任何策略和权限将应用于共享资源。

共享您的资源

您可以通过创建资源共享来共享您拥有的资源。当您创建资源共享时，您可以指定名称、要共享的资源以及要与之共享的委托人。委托人可以是 AWS Organizations 中的 AWS 账户、组织部门或整个组织。您的账户对您共享的资源保留完整所有权。

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。您可以使用各自服务的控制台、AWS CLI 和 API 访问此资源。允许用户执行的操作因资源类型而异。所有 IAM 策略以及在您的账户中配置的服务控制策略都将适用，这使您能够利用在安全性和管理控制方面的现有投资。

服务限制

您的 AWS 账户具有以下与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 AWS Support。

Resource	默认限制
每个账户的最大资源共享数量	5000
每个账户的最大共享委托人数	5000
每个账户的最大共享资源数	5000
每个账户的最大待接受邀请数	20

访问AWS RAM

您可以通过任何以下方法使用 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 管理控制台并从控制台主页选择 AWS RAM 来访问 AWS RAM 控制台。

AWS Command Line Interface (AWS CLI)

AWS CLI 提供对 AWS RAM 公共 API 操作的直接访问。它在 Windows、macOS 和 Linux 上受支持。有关入门的更多信息，请参阅 AWS Command Line Interface 用户指南。有关 AWS RAM 的命令的更多信息，请参阅 AWS CLI Command Reference。

适用于 Windows PowerShell 的 AWS 工具

AWS 为在 PowerShell 环境中编写脚本的用户提供大量 AWS 产品的相关命令。有关入门的更多信息，请参阅 适用于 Windows PowerShell 的 AWS 工具 用户指南。有关 AWS RAM 的 cmdlet 的更多信息，请参阅 适用于 Windows PowerShell 的 AWS 工具Cmdlet 参考。

查询 API

AWS RAM HTTPS 查询 API 使您能够以编程方式访问 AWS RAM 和 AWS。AWS RAM API 可让您直接向服务发出 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。有关更多信息，请参阅 AWS RAM API 参考。

Pricing

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。有关如何为可共享资源计费的更多信息,请参阅相应服务的文档。

可共享资源

AWS RAM 允许您共享在其他 AWS 服务中预置和管理的资源。AWS RAM 不允许您管理资源,但它提供的功能可让您使资源跨 AWS 账户可用。

以下部分列出了与 AWS RAM 集成的服务以及支持共享的资源。

服务

- AWS App Mesh (p. 3)
- Amazon Aurora (p. 3)

AWS App Mesh

您可以使用 AWS App Mesh 共享以下 AWS RAM 资源。

Resource	使用案例
Mesh	集中创建和管理网格,并与其他 AWS 账户共享。共享网格允许不同 AWS 账户创建的资源在同一网格中相互通信。有关更多信息,请参阅 https://docs.amazonaws.cn/app-mesh/latest/userguide/sharing.html 用户指南 中的AWS App Mesh使用共享网格。

Amazon Aurora

您可以使用 Amazon Aurora 共享以下 AWS RAM 资源。

Resource	使用案例
数据库 集群	集中创建和管理数据库集群,并与其他 AWS 账户共享。这允许多个 AWS 账户克隆共享的集中管理数据库集群。有关更多信息,请参阅 Amazon Aurora 用户指南 中的 跨账户 Aurora 数据库集群克隆。

AWS Certificate Manager 私有证书颁发机构

您可以使用 ACM Private CA 共享以下 AWS RAM 资源。

Resource	使用案例
私有证书颁发机构 (CA)	为组织的内部 PKI 创建和管理私有证书颁发机构 (CA),并与其他 AWS 账户共享它们。这允许其他账户中的 AWS Certificate Manager 用户颁发由共享 CA 签名的 X.509 证书。有关更多信息,请参阅 AWS Certificate Manager 私有证书颁发机构用户指南 中的启用对私有 CA 的访问。

AWS CodeBuild

您可以使用 AWS CodeBuild 共享以下 AWS RAM 资源。

Resource	使用案例
项目	创建项目并使用它运行构建任务。与其他 AWS 账户或用户共享项目。这使多个 AWS 账户和用户能够查看有关项目的信息并分析其构建。有关更多信息,请参阅 用户指南 中的AWS CodeBuild使用共享项目。
报告 组	创建报告组,并在构建项目时使用它来创建报告。与其他 AWS 账户或用户共享报告组。这允许多个 AWS 账户和用户查看报告组及其报告,以及每个报告的测试用例结果。报告可在创建后 30 天内查看,然后过期且不再可供查看。有关更多信息,请参阅 https://docs.amazonaws.cn/codebuild/latest/userguide/project-sharing.html 用户指南 中的AWS CodeBuild使用共享报告组。

Amazon EC2

您可以使用 Amazon EC2 共享以下 AWS RAM 资源。

Resource	使用案例
容量 预留	集中创建和管理容量预留,并与其他 AWS 账户共享预留容量。这使多个 AWS 账户可以在集中管理的预留容量中启动其 Amazon EC2 实例。有关更多信息,请参阅 https://docs.amazonaws.cn/AWSEC2/latest/UserGuide/capacity-reservation-sharing.html 中的使用共享容量预留Amazon EC2 用户指南（适用于 Linux 实例）。
专用 主机	集中分配和管理 Amazon EC2 专用主机,并与其他 AWS 账户共享主机的实例容量。这使多个 AWS 账户可以在集中管理的专用主机上启动其 Amazon EC2 实例。有关更多信息,请参阅 https://docs.amazonaws.cn/AWSEC2/latest/UserGuide/dh-sharing.html 中的使用共享专用主机Amazon EC2 用户指南（适用于 Linux 实例）。

Amazon EC2 映像生成器

您可以使用 Amazon EC2 共享以下 AWS RAM 映像生成器资源。

Resource	使用案例
组件	集中创建和管理组件,并与其他 AWS 账户或您的组织共享。管理谁可以在其镜像配方中使用预定义的生成和测试组件。有关更多信息,请参阅 EC2 Image

Resource	使用案例
	Builder 用户指南 中的 EC2 Image Builder 中的资源共享。
镜像	集中创建和管理您的黄金镜像,并与其他 AWS 账户和您的组织共享镜像。在组织中管理可使用 EC2 Image Builder 创建映像的人员。有关更多信息,请参阅 EC2 映像生成器用户指南 中的 EC2 映像生成器中的资源共享。
映像 配方	集中创建和管理镜像配方,并与其他 AWS 账户和您的组织共享它们。这使您可以管理哪些用户可以使用预定义的文档为所需的配置自动完成可重复镜像管道。有关更多信息,请参阅 EC2 Image Builder 用户指南 中的 EC2 Image Builder 中的资源共享。

AWS 粘合

您可以使用 AWS 共享以下 AWS RAM Glue 资源。

Resource	使用案例
数据目录	管理中央数据目录,并与企业内的 AWS 账户和组织共享有关数据库和表的元数据。这使用户能够对多个账户中的数据运行查询。有关更多信息,请参阅 AWS Lake Formation 指南 中的跨 AWS 账户共享数据目录表和数据库。
数据库	集中创建和管理数据目录数据库,并与企业内的 AWS 账户和组织共享。数据库是数据目录表的集合。这使用户能够运行查询以及提取、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 指南 中的跨 AWS 账户共享数据目录表和数据库。
表	集中创建和管理数据目录表,并与企业内的 AWS 账户和组织共享。数据目录表包含有关 Amazon S3、JDBC 数据源、Amazon Redshift、流式传输源和其他数据存储中数据表的元数据。这使用户能够运行查询和 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 指南 中的跨 AWS 账户共享数据目录表和数据库。

AWS License Manager

您可以使用 AWS 共享以下 AWS RAM License Manager 资源。

Resource	使用案例
许可证 配置	集中创建和管理许可证配置,并与其他 AWS 账户共享。这使您可以在多个 AWS 账户中实施基于您的企业协议条款的集中管理许可规则。有关更多信息,请

Resource	使用案例
	参阅 AWS License Manager 用户指南 中的使用许可证配置。

AWS Outposts

您可以使用 AWS Outposts 共享以下 AWS RAM 资源。

Resource	使用案例
输出	集中创建和管理 Outposts,并在您的 AWS 组织内共享它们。这使多个账户能够在共享的集中托管 Outposts 上创建子网和 EBS 卷。有关更多信息,请参阅 用户指南 中的使用共享的 AWS Outposts 资源AWS Outposts。
本地 网关路由表	在 Outpost 上集中创建和管理本地网关路由表,并在您的 AWS 组织内共享这些路由表。这将使 ultuple 账户能够创建与本地网关的 VPC 关联,并在 Outpost 上查看本地网关路由表和虚拟接口的配置。有关更多信息,请参阅 用户指南 中的使用共享的 AWS Outposts 资源AWS Outposts。
Subnets (子网)	在 Outpost 上集中创建和管理子网,并在您的 AWS 组织内共享它们。这使多个账户可以在 Outpost 上的共享子网中启动并运行 EC2 实例。有关更多信息,请参阅 用户指南 中的使用共享的 AWS Outposts 资源AWS Outposts。

AWS 资源组

您可以使用 AWS 资源组 共享以下 AWS RAM 资源。

Resource	使用案例
资源 组	集中创建和管理主机资源组,并将其与其他 AWS 账户共享。这允许多个 AWS 账户共享使用 Amazon EC2 创建的一组 AWS License Manager 专用主机。有关更多信息,请参阅 用户指南AWS License Manager 中的 中的主机资源组。AWS License Manager

Amazon Route 53

您可以使用 Amazon Route 53 共享以下 AWS RAM 资源。

Resource	使用案例
转发 规则	集中创建和管理转发规则,并与其他 AWS 账户共享。这允许多个 AWS 账户将 DNS 查询从其 VPCs 转发到在共享的集中管理的解

Resource	使用案例
	析程序规则中定义的目标 IP 地址。有关更多信息,请参阅 https://docs.amazonaws.cn/Route53/latest/DeveloperGuide/resolver-rules-managing.html#resolver-rules-managing-sharing 中的与其他 AWS 账户共享转发规则并使用共享规则Amazon Route 53 开发人员指南。
查询日志	集中创建和管理查询日志,并与其他 AWS 账户共享。这使多人 AWS 账户能够将源自其 VPCs 的 DNS 查询记录到集中管理的查询日志。有关更多信息,请参阅 https://docs.amazonaws.cn/Route53/latest/DeveloperGuide/query-logging-configurations-managing-sharing.html 中的与其他 AWS 账户共享解析程序查询日志记录配置Amazon Route 53 开发人员指南。

Amazon VPC

您可以使用 Amazon VPC 共享以下 AWS RAM 资源。

Resource	使用案例
客户拥有的 IPv4 地址	在 AWS Outposts 安装过程中,AWS 会根据您提供的有关本地网络的信息创建一个地址池(称为客户拥有的 IP 地址池)。 客户拥有的 IP 地址通过本地网络提供到 Outpost 子网中资源的本地或外部连接。您可以使用弹性 IP 地址将这些地址分配给 Outpost 上的资源,例如 EC2 实例。
前缀列表	集中创建和管理前缀列表,并与其他 AWS 账户共享。这允许多个 AWS 账户在其资源(如 VPC 安全组和子网路由表)中引用前缀列表。有关更多信息,请参阅 https://docs.amazonaws.cn/vpc/latest/userguide/sharing-managed-prefix-lists.html 中的使用共享前缀列表Amazon VPC 用户指南。
Subnets (子网)	集中创建和管理子网,并与 AWS Organizations 中位于同一组织的其他账户或组织单位共享。这使多个 AWS 账户可以在集中管理的 VPCs 中启动其应用程序资源。 这些资源包括 Amazon EC2 实例、Amazon Relational Database Service (RDS) 数据库、Amazon Redshift 集群和 AWS Lambda 函数。有关更多信息,请参阅 https://docs.amazonaws.cn/vpc/latest/userguide/vpc-sharing.html 中的使用 VPC 共享Amazon VPC 用户指南。
流量 镜像 目标	集中创建和管理流量镜像目标,并与其他 AWS 账户共享。这使多个 AWS 账户能够将来自其账户中的流量镜像源的镜像网络流量发送到集中管理的共享流量镜像目标。有关更多信息,请参阅 指南 中的跨账户流量镜像目标Traffic Mirroring。

Resource	使用案例
中转网关	集中创建和管理中转网关,并与其他 AWS 账户共享。这使多个 AWS 账户能够通过共享的集中管理中转网关在其 VPCs 与本地网络之间路由流量。有关更多信息,请参阅 中转网关指南 中的共享中转网关。

开始使用 AWS RAM

借助 AWS RAM，您可以与各 AWS 账户或通过 AWS Organizations 共享您拥有的资源，并且您可以使用由其他 AWS 账户或通过 AWS Organizations 与您共享的资源。

主题

共享您的资源

要开始使用 AWS RAM 共享您拥有的资源，请执行以下操作：

> Note
>
> 一些资源对共享有特殊的注意事项和先决条件。有关更多信息，请参阅可共享资源 (p. 2)。

启用与 AWS Organizations 共享

如果您要与您的组织或组织单位共享资源,则必须使用 AWS RAM 控制台或 CLI 命令启用与 AWS Organizations 的共享。当您在组织内共享资源时，AWS RAM 不会向委托人发送邀请。组织中的委托人获取对共享资源的访问权限，而无需交换邀请。

如果您不再需要与整个组织或组织单位共享资源,则可以禁用共享。有关更多信息，请参阅禁用与 AWS Organizations 的共享 (p. 23)。

Requirements

- 只有 管理账户 账户才能启用与 AWS Organizations 共享。
- 必须为所有功能启用组织。有关更多信息,请参阅 https://docs.amazonaws.cn/organizations/latest/userguide/orgs_manage_org_support-all-features.html 用户指南 中的AWS Organizations启用组织中的所有功能。

> Important
>
> - 如果您未启用与 AWS Organizations 共享，则无法与组织或组织内的组织部门共享资源。但是，您仍可以与组织中的各 AWS 账户共享资源。在这种情况下,账户将被视为外部委托人。他们会收到加入资源共享的邀请,并且必须接受邀请才能获取对共享资源的访问权限。
> - 您必须使用 AWS Organizations 控制台或 AWS RAMenable-sharing-with-aws-organization 命令启用与 共享。AWS CLI这可确保创建 `AWSServiceRoleForResourceAccessManager` 服务相关角色。如果您使用 AWS Organizations 控制台或 AWS Organizationsenable-aws-service-access 命令启用对 的可信访问,则不会创建 AWS CLI 服务相关角色,并且您将无法在组织内共享资源。`AWSServiceRoleForResourceAccessManager`

启用与 AWS Organizations 的共享(控制台)

1. 通过以下网址打开 AWS RAM 控制台的设置页面：https://console.amazonaws.cn/ram/home#Settings。
2. 选择 Enable sharing with AWS Organizations (启用与 AWS Organizations 共享)。

启用与 AWS Organizations 共享 (AWS CLI)

使用 enable-sharing-with-aws-organization 命令。

此命令可用于任何区域中，并且它在支持 AWS RAM 的所有区域中都启用与 AWS Organizations 共享。

创建资源共享

要共享您拥有的资源，请创建资源共享，添加要共享的资源，并指定要与其共享资源的principals。

Considerations

- 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。
- 如果您是 AWS Organizations 中某组织的一部分并且已在您的组织中启用共享，组织中的principals将自动获得对共享资源的访问权限。否则，principals会收到加入资源共享的邀请，并在接受邀请后获得对共享资源的访问权限。
- 在将组织添加到资源共享之后，对 OU 或组织进行更改会影响资源共享。例如，如果您向组织添加新账户，则此账户有权访问共享资源。
- 您不能将以下内容作为 资源共享 添加到 principals:IAM 用户、IAM 角色、OUs 或 AWS Organizations 中您组织外部的组织。

创建 资源共享(控制台)

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 如果您是首次使用 AWS RAM，请从主页选择 Create a resource share (创建资源共享)。否则,从 资源共享 页面中选择 Create （创建 AWS Lambda)资源共享。
3. 在 Description (描述) 下，对于 Name (名称)，键入资源共享的描述性名称。
4. （可选）在 Resources (资源) 下，选择要添加到资源共享的资源，如下所示：

   a. 对于选择资源类型，选择资源的类型。这会将可共享资源的列表筛选为所选类型的资源。

   b. 选中资源旁边的复选框。所选资源将移至 Selected resources (选定资源) 下。

      如果您要共享区域性资源，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，请参阅适用于您的资源的 AZIDs (p. 17)。

5. （可选）在委托人下，执行以下操作：

   a. 默认情况下，您可以与任何 AWS 账户共享资源。要将资源共享限制为 AWS Organizations 中您的组织，请清除 Allow external accounts (允许外部账户)。

   b. 对于每个principal，指定其 ID，然后选择添加：

      - 要添加 AWS 账户，请键入 12 位的账户 ID。例如：`123456789012`。
      - 要添加一个 OU，请键入 OU 的 ID。例如：`ou-abcd1234-mnop5678qrst9098uv76`。
      - 要添加您的整个组织，请键入组织的 ID。例如：`o-abcd1234efgh5678`。

6. （可选）在标签下，键入标签密钥和标签值。要添加其他标签，请选择添加标签，然后键入标签键和标签值对。这些标签不应用于资源共享中包含的资源。
7. 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。先让此过程完成，然后再尝试使用资源共享。

8. 您可以随时添加和删除资源和principals，或将自定义标签应用于资源共享。您不再希望共享资源时，可以删除您的资源共享。有关更多信息，请参阅共享您拥有的资源 (p. 12)。

创建 资源共享 (AWS CLI)

使用 create-resource-share 命令。

使用共享资源

要开始使用共享资源，请执行以下操作：

- 回复资源共享邀请 (p. 11)
- 使用与您共享的资源 (p. 11)

回复资源共享邀请

如果您收到加入资源共享的邀请，您必须接受它才能获得对共享资源的访问权限。如果您是 AWS Organizations中某组织的一部分并且已在您的组织中启用共享，组织中的principals将自动获得对共享资源的访问权限而不会收到这些邀请。

响应邀请

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 在导航窗格中，依次选择与我共享和 Resource shares (资源共享)。
3. 审核已添加您的 资源共享 列表。

   Status 列显示您当前参与 资源共享 的状态。`Pending` 状态显示您已被添加至 资源共享，但您尚未接受或拒绝该邀请。
4. 若要响应 资源共享 邀请，请选择 资源共享 ID 并选择接受资源共享，以接受邀请；或者拒绝资源共享来拒绝邀请。如果您拒绝邀请，则您无法访问该资源。如果您接受邀请，则可访问该资源。

使用与您共享的资源

在您接受加入资源共享的邀请后，您就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，请参阅可共享资源 (p. 2)。

使用共享资源

您可以共享您拥有的 AWS 资源和访问与您共享的 AWS 资源。

目录

共享您拥有的资源

通过 AWS RAM，您可以与您指定的principals共享您指定的资源。任何时候，您都可以修改已创建的资源共享，并在不再需要时将其删除。

内容

创建资源共享

要共享您拥有的资源，请创建资源共享，添加要共享的资源，并指定要与其共享资源的principals。

要创建资源共享，请按照共享您的资源 (p. 9)中的指导操作。

更新资源共享

您可以随时更新资源共享。您可以向您创建的资源共享添加principals、资源或标签。您可以通过从资源共享中删除principals或资源来撤消对共享资源的访问权限。如果您撤消访问权限，principals不再对共享资源具有访问权限。

使用控制台更新资源共享

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 在导航窗格中，依次选择由我共享和资源共享。
3. 选择资源共享，然后选择修改。
4. （可选）要更改资源共享的名称，请编辑 Name (名称)。
5. （可选）要将资源添加到资源共享，在资源下，选择资源的类型并选中资源旁边的复选框。
6. （可选）要删除资源，请在 Selected resources (选定资源) 面板中找到此资源，然后选择 X。
7. （可选）要添加principal，请键入 AWS 账户 OU 或组织的 ID，然后选择添加。
8. （可选）要删除principal，请在 Selected principals (选定委托人) 面板中找到它，然后选择 X。
9. （可选）要将标签添加到资源共享，在标签下，选择添加标签，然后键入标签键和标签值对。
10. 要从资源共享删除标签，请找到此标签并选择删除标签。
11. 选择保存更改。

使用 AWS CLI 更新资源共享

使用以下命令：

- associate-resource-share
- disassociate-resource-share
- tag-resource
- update-resource-share

查看资源共享

您可以查看您已创建的所有资源共享的列表。您可以看到您共享了哪些资源以及与哪些principals共享了这些资源。

使用控制台查看资源共享

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 在导航窗格中，依次选择由我共享和资源共享。
3. 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。
4. 选择资源共享以进行检查。界面中会提供以下信息：
   - Summary (摘要) — 列出有关资源共享的信息，如其名称、ID、所有者、Amazon 资源名称 (ARN)、创建日期和当前状态。
   - Shared resources (共享资源) — 列出资源共享中包含的资源。选择资源的 ID 以在其服务控制台查看此资源。
   - Shared principals (共享委托人) — 列出与其共享资源的principals。
   - Tags (标签) — 列出资源共享的标签键值对。

使用 AWS CLI 查看资源共享

使用 get-resource-shares 命令。

查看您的共享资源

您可以跨所有资源共享查看由您的账户共享的资源。这样，您能够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，以及有权访问它们的principals数量。

使用控制台查看您共享的资源

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 在导航窗格中，依次选择由我共享和 Shared resources (共享资源)。
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 以在其服务控制台查看此资源。
   - 资源类型 — 资源的类型。
   - Last share date (上次共享日期) — 上次共享资源的日期。
   - Resource shares (资源共享) — 包含资源的资源共享的数量。选择值以列出资源共享。
   - Principals (委托人) — 与其共享资源的principals的数量。选择此值以查看principals。

使用 AWS CLI 查看您共享的资源

使用 list-resources 命令。

查看您与其共享资源的委托人

您可以跨所有资源共享查看您与其共享资源的principals。通过查看您与其共享资源的委托人，您可以确定谁有权访问您共享的资源。

使用控制台查看您与其共享资源的principals

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 在导航窗格中，依次选择由我共享和委托人。
3. 对于每个principal，提供以下信息：
   - Principal ID (委托人 ID) — principal的 ID。
   - Resource shares (资源共享) — 您与principal共享的资源共享的数量。选择此值以查看资源共享。
   - 资源 — 您与principal共享的资源数量。选择此值以查看共享资源。

使用 AWS CLI 查看您与其共享资源的principals

使用 list-principals 命令。

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principals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资源。

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

使用控制台删除资源共享

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 在导航窗格中，依次选择由我共享和资源共享。
3. 选择资源共享。确保选择正确的资源共享。您无法在删除资源共享后恢复它。
4. 选择删除，键入确认消息，然后选择删除。

使用 AWS CLI 删除资源共享

使用 delete-resource-share 命令。

共享资源支持的操作

您可以使用 AWS CLI 查看principals可以对共享资源执行的操作。有关更多信息,请参阅 get-resource-policies 命令。

访问与您共享的资源

借助 AWS RAM，您可以查看已将您添加到的资源共享、您可以访问的共享资源，以及与您共享资源的账户。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

接受和拒绝邀请

要访问共享资源，principal必须将您添加到资源共享。

如果 AWS Organizations 中您组织内的账户已将您添加到资源共享，并且已在您的组织中启用共享，您将自动获得对共享资源的访问权限。

如果以下账户之一已将您添加到资源共享，您将收到加入资源共享的邀请：

- AWS Organizations 中您组织外部的账户
- 您组织内的账户（如果尚未启用与 AWS Organizations 共享）

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，则您无法访问共享的资源。

您有七天时间可接受加入资源共享的邀请。如果您在七天内未接受邀请，则邀请将被自动拒绝。

响应邀请

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 在导航窗格中，依次选择与我共享和 Resource shares (资源共享)。
3. 审核已添加您的 资源共享 列表。

   Status 列显示您当前参与 资源共享 的状态。`Pending` 状态显示您已被添加至 资源共享，但您尚未接受或拒绝该邀请。
4. 若要响应 资源共享 邀请，请选择 资源共享 ID 并选择接受资源共享，以接受邀请；或者拒绝资源共享来拒绝邀请。如果您拒绝邀请，则您无法访问该资源。如果您接受邀请，则可访问该资源。

响应邀请 (AWS CLI)

使用以下命令：

- accept-resource-share-invitation
- reject-resource-share-invitation

查看资源共享

您可以查看已将您添加的资源共享。您可以看到哪些principals与您共享资源和共享了哪些资源。

使用控制台查看资源共享

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 在导航窗格中，依次选择与我共享和 Resource shares (资源共享)。
3. 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。
4. 界面中会提供以下信息：

   - Name (名称) — 资源共享的名称。
   - ID — 资源共享的 ID。选择 ID 以查看资源共享。
   - Owner (所有者) — 创建资源共享的 AWS 账户的 ID。
   - Status (状态) — 资源共享的当前状态。可能的值包括：
     - Active (活跃) — 资源共享处于活跃状态，可供使用。
     - Deleted (已删除) — 资源共享已被删除且不再可供使用。
     - Pending (待处理) — 加入资源共享的邀请正等待处理。

使用 AWS CLI 查看资源共享

使用 get-resource-shares 命令。

查看共享资源

您可以查看您可以访问的共享资源。您可以看到哪些principals正在共享资源以及这些资源包含在哪些资源共享中。

使用控制台查看共享资源

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 在导航窗格中，依次选择与我共享和 Shared resources (共享资源)。
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。
   - Last share date (上次共享日期) — 与您共享资源的日期。
   - Resource shares (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principal的 ID。

使用 AWS CLI 查看共享资源

使用 list-resources 命令。

查看与您共享资源的委托人

您可以查看正在与您共享资源的所有principals的列表。您可以查看他们已与您共享哪些资源和资源共享。

使用控制台查看正在与您共享资源的principals

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。

2. 在导航窗格中，选择与我共享和委托人。
3. 应用筛选条件以查找特定principals。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：
   - Principal ID (委托人 ID) — 与您共享资源的principal的 ID。
   - Resource shares (资源共享) — principal 已将您添加到的资源共享的数量。选择此值以查看资源共享。
   - 资源 — principal与您共享的资源数量。选择此值以查看资源。

使用 AWS CLI 查看正在与您共享资源的principals

使用 list-principals 命令。

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。

如果您由组织内的账户添加到资源共享并且启用了与 AWS Organizations 共享，则您不能退出。

使用控制台退出资源共享

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 在导航窗格中，依次选择与我共享和 Resource shares (资源共享)。
3. 选择资源共享。
4. 选择 Leave resource share (退出资源共享)，键入确认文本，然后选择 Leave resource share (退出资源共享)。

使用 AWS CLI 退出资源共享

使用 disassociate-resource-share 命令。

适用于您的资源的 AZIDs

为确保资源分配到区域的各可用区，我们将可用区独立映射到每个账户的名称。例如，您的 AWS 账户的可用区 `us-east-1a` 可能与另一 AWS 账户的 `us-east-1a` 不在同一位置。有关更多信息，请参阅 用户指南 中的 Amazon EC2 区域和可用区。

要确定与您的账户相关的资源的位置，您必须使用 AZ ID（可用区的唯一且一致的标识符）。例如，`use1-az1` 是 `us-east-1` 区域的 AZ ID，它在每个 AWS 账户中的位置均相同。

查看账户中的可用区的 AZIDs

1. 从 https://console.amazonaws.cn/ram 打开 AWS RAM 控制台。
2. 在导航窗格中，选择 Resource Access Manager (资源访问管理器)。
3. 当前区域的 AZ IDs 位于 Your AZ ID (您的 AZ ID) 下。

通过查看 AZ IDs,您可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,如果您在可用区中与另一个账户共享可用区 ID 为 `use-az2` 的子网,则此子网可用于可用区中其可用区 ID 也为 `use-az2` 的账户。 将在 Amazon VPC 控制台中显示每个子网的可用区 ID。

使用 IDs 查看 AZAWS CLI

- describe-availability-zones
- DescribeAvailabilityZones

AWS RAM 中的安全性

AWS 的云安全性的优先级最高。作为 AWS 客户，您将从专为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益。

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

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

该文档帮助您了解如何在使用 AWS RAM 时应用责任共担模型。以下主题说明如何配置 AWS RAM 以实现您的安全性和合规性目标。您还将了解如何使用其他 AWS 服务来帮助您监控和保护 AWS RAM 资源。

主题

AWS Resource Access Manager 中的数据保护

AWS Resource Access Manager 符合 AWS 责任共担模式，该模式包含适用于数据保护的法规和准则。AWS 负责保护运行所有 AWS 服务的全球基础设施。AWS 保持对该基础设施上托管的数据的控制，包括用于处理客户内容和个人数据的安全配置控制。作为数据控制者或数据处理者，AWS 客户和 APN 合作伙伴对他们放在 AWS 云中的任何个人数据承担责任。

出于数据保护的目的，我们建议您保护 AWS 账户凭证并使用 AWS Identity and Access Management (IAM) 设置单个用户账户，以便仅向每个用户提供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您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与 AWS 资源进行通信。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 使用高级托管安全服务,如 Amazon Macie。

我们强烈建议您切勿将敏感的可识别信息（例如您客户的账号）放入自由格式字段（例如 Name (名称) 字段）。这包括使用控制台、API、AWS RAM 或 AWS AWS CLI 处理 AWS 或其他 SDKs 服务时。 您输入到 AWS RAM 或其他服务中的任何数据都可能被选取以包含在诊断日志中。当您向外部服务器提供 URL 时，请勿在 URL 中包含凭证信息来验证您对该服务器的请求。

有关数据保护的更多信息,请参阅 AWS 安全博客上的 责任共担模型和 GDPRAWS 博客文章。

适用于 AWS RAM 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一项 AWS 服务,可帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制谁可以通过身份验证(登录)和授权(具有权限)使用 AWS 资源。利用 IAM,您可以在 AWS 账户下创建用户和组。您可以控制用户使用 AWS 资源执行任务所必需的权限。您可以使用 IAM,无需额外付费。有关管理和创建自定义 IAM 策略的更多信息，请参阅管理 IAM 策略。

主题

AWS RAM 如何与 IAM 协同工作

默认情况下,IAM 用户没有创建或修改 AWS RAM 资源的权限。要允许 IAM 用户创建或修改资源并执行任务,您必须创建 IAM 策略来授予使用特定资源和 API 操作的权限。然后,将这些策略附加到需要这些权限的 IAM 用户或组。

主题

策略结构

策略是一个 JSON 文档,其中包含以下语句:IAM 效果、操作、资源和条件。策略通常采用以下形式:IAM

```
{
     "Statement":[{
         "Effect":"effect",
         "Action":"action",
         "Resource":"arn",
         "Condition":{
             "condition":{
                 "key":"value"
             }
         }
     }]
 }
```

Effect

Effect 语句指示策略是允许还是拒绝用户执行操作的权限。可能值包括：`Allow` 和 `Deny`。

Action

Action 语句指定策略为其允许或拒绝权限的 API 操作。AWS RAM有关允许的操作的完整列表,请参阅 AWS Resource Access Manager 中的 定义的操作。IAM 用户指南

Resource

资源语句指定受策略影响的 资源。AWS RAM要在语句中指定资源,您需要使用其唯一 Amazon 资源名称 (ARN)。有关所允许资源的完整列表,请参阅 AWS Resource Access Manager 中的 定义的资源。IAM 用户指南

Condition

条件语句是可选的。它们可用于进一步优化应用策略的条件。AWS RAM 支持以下条件键:

- `aws:RequestTag/${TagKey}` — 指定在创建或标记资源共享时必须使用的标签键值对。
- `aws:ResourceTag/${TagKey}` — 表示只能对具有指定标签键值对的资源执行操作。
- `aws:TagKeys` — 指定可在创建或标记资源共享时使用的标签键。
- `ram:AllowsExternalPrincipals` — 表示只能对允许或拒绝与外部委托人共享的资源共享执行该操作。外部委托人是 AWS 组织外部的 AWS 账户
- `ram:Principal` — 表示只能对指定的委托人执行该操作。
- `ram:RequestedResourceType` — 表示只能对指定的资源类型执行该操作。必须按以下格式指定资源类型:
  - `aws:RequestTag/${TagKey}` — 指定在创建或标记资源共享时必须使用的标签键值对。
  - `aws:ResourceTag/${TagKey}` — 表示只能对具有指定标签键值对的资源执行操作。
  - `aws:TagKeys` — 指定可在创建或标记资源共享时使用的标签键。
  - `ram:AllowsExternalPrincipals` — 表示只能对允许或拒绝与外部委托人共享的资源共享执行该操作。外部委托人是 AWS 组织外部的 AWS 账户
  - `ram:Principal` — 表示只能对指定的委托人执行该操作。
  - `ram:RequestedResourceType` — 表示只能对指定的资源类型执行该操作。必须按以下格式指定资源类型:
    - AWS App Mesh
      - `appmesh:Mesh`
    - Amazon Aurora
      - `rds:Cluster`
    - AWS Certificate Manager 私有证书颁发机构
      - `acm-pca:CertificateAuthority`
    - AWS CodeBuild
      - `codebuild:Project`
      - `codebuild:ReportGroup`
    - Amazon EC2
      - `ec2:CapacityReservation`
      - `ec2:DedicatedHost`
    - Amazon EC2 映像生成器
      - `imagebuilder:Component`
      - `imagebuilder:Image`
      - `imagebuilder:ImageRecipe`
    - AWS 粘合
      - `glue:Catalog`
      - `glue:Database`
      - `glue:Table`
    - AWS License Manager
      - `license-manager:LicenseConfiguration`
    - AWS Outposts
      - `outposts:Outpost`
    - AWS 资源组
      - `resource-groups:Group`
    - Amazon Route 53

        - route53resolver:ResolverRule
        - route53resolver:ResolverQueryLogConfig
      - Amazon VPC
        - ec2:PrefixList
        - ec2:Subnet
        - ec2:TrafficMirrorTarget
        - ec2:TransitGateway
        - ec2:LocalGatewayRouteTable
    - ram:ResourceArn — 表示只能对具有指定 ARN 的资源执行该操作。
    - ram:ResourceShareName — 表示只能对具有指定名称的资源共享执行该操作。
    - ram:ShareOwnerAccountId — 表示只能对特定账户拥有的资源共享执行该操作。
- ram:ResourceArn — 表示只能对具有指定 ARN 的资源执行操作。
- ram:ResourceShareName — 表示只能对具有指定名称的资源共享执行该操作。
- ram:ShareOwnerAccountId — 表示只能对特定账户拥有的资源共享执行该操作。

示例 IAM 策略

示例

示例 1：允许共享特定资源

您可以使用 IAM 策略来限制principals只将特定资源与资源共享关联。

例如，以下策略限制principals只与指定的 Amazon 资源名称 (ARN) 共享解析程序规则。

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

示例 2：允许共享特定的资源类型

您可以使用 IAM 策略来限制principals只将特定的资源类型与资源共享关联。

例如，以下策略限制principals只共享解析程序规则。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
        }
    }]
}
```

示例 3: 限制与外部 AWS 账户共享

您可以使用 IAM 策略防止principals与其 AWS 组织外部的 AWS 账户共享资源。

例如，以下 IAM 策略禁止principals将外部 AWS 账户添加到资源共享。

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

禁用与 AWS Organizations 的共享

如果您之前启用了与 AWS Organizations 的共享,并且您不再需要与整个组织或组织单位共享资源,则可以禁用共享。当您禁用与 AWS Organizations 共享时,将从已创建的 资源共享 中删除所有组织或组织单位,这些组织或组织单位将失去对共享资源的访问权限。

禁用与 AWS Organizations 的共享

1. 使用 AWS Organizations AWS Organizationsdisable-aws-service-access 命令禁用对 AWS CLI 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委托人，他们将失去对这些共享资源的访问权限。

2. 使用 IAM 控制台、IAM AWS CLI 或 IAM API 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。

AWS RAM 权限

AWS RAM 权限是 AWS RAM 使用的策略片段。它们控制允许委托人对与其共享的资源执行哪些操作。AWS RAM 权限用于生成附加到共享资源的基于资源的策略。

AWS RAM 包括每个受支持的可共享资源类型的默认 AWS 托管权限。这些托管权限由 AWS 创建和管理,它们为每个可共享资源类型定义允许的操作。有关默认 AWS 托管权限的更多信息,请参阅AWS 托管权限 (p. 24)。

主题

权限的工作方式AWS RAM

当您创建资源共享时,AWS RAM 会自动将每个关联资源类型的默认权限附加到资源共享。例如,如果您创建资源共享并将子网和容量预留关联,AWS RAM 会自动将子网和容量预留权限附加到资源共享。

在创建资源共享后,将向相应的资源拥有服务提供权限。资源拥有服务使用提供的权限为资源共享中包含的每个资源创建基于资源的策略。资源拥有服务创建的生成的基于资源的策略包括以下元素:

- `Resource` 资源共享中包含的资源。—
- `Effect`— 权限的效果。AWS RAM始终为 `allow`。
- `Principal`— 与资源共享关联的委托人的 ARNs。
- `Action`— 权限中定义的标准操作。AWS RAM

基于资源的策略将附加到共享资源。它们允许指定的委托人对资源执行允许的操作。

AWS 托管权限

AWS RAM 提供以下默认的 AWS 托管权限:

主题

AWS App Mesh

AWS RAM 为可共享的 AWS 资源提供以下默认 AWS App Mesh 托管权限。

资源类型	权限名称和 ARN	效果	操作
appmesh:Mesh	名称:AWSRAMDefaultPermissionAppMesh	Allow	• `appmesh:CreateVirtualNode` • `appmesh:CreateVirtualRouter` • `appmesh:CreateRoute`

资源类型	权限名称和 ARN	效果	操作
	ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAppMesh		• appmesh:CreateVirtualService • appmesh:UpdateVirtualNode • appmesh:UpdateVirtualRouter • appmesh:UpdateRoute • appmesh:UpdateVirtualService • appmesh:ListVirtualNodes • appmesh:ListVirtualRouters • appmesh:ListRoutes • appmesh:ListVirtualServices • appmesh:DescribeVirtualNode • appmesh:DescribeVirtualRouter • appmesh:DescribeRoute • appmesh:DescribeVirtualService • appmesh:DeleteVirtualNode • appmesh:DeleteVirtualRouter • appmesh:DeleteRoute • appmesh:DeleteVirtualService

Amazon Aurora

AWS RAM 为可共享的 AWS 资源提供以下默认 Amazon Aurora 托管权限。

资源类型	权限名称和 ARN	效果	操作
rds:Cluster	名称:AWSRAMDefaultPermissionRDSCluster ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionRDSCluster	Allow	• rds:RestoreDbClusterToPointInTime • rds:DescribeDbClusters

AWS Certificate Manager 私有证书颁发机构

AWS RAM 为可共享的 AWS 资源提供以下默认 ACM Private CA 托管权限。

资源类型	权限名称和 ARN	效果	操作
acm-pca:CertificateAuthority	名称:AWSRAMDefaultPermissionCertificateAuthority ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionCertificateAuthority	Allow	• acm-pca:IssueCertificate • acm-pca:DescribeCertificateAuthority • acm-pca:GetCertificate • acm-pca:GetCertificateAuthorityCertifi • acm-pca:ListPermissions • acm-pca:ListTags

AWS CodeBuild

AWS RAM 为可共享的 AWS 资源提供以下默认 AWS CodeBuild 托管权限。

资源类型	权限名称和 ARN	效果	操作
Codebuild:项目	名称:AWSRAMDefaultPermissionCodeBuildProject ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionCodeBuildProject	Allow	• codebuild:BatchGetBuilds • codebuild:BatchGetProjects • codebuild:ListBuildsForProject
codebuild:报告组	名称:AWSRAMDefaultPermissionCodeBuildReportGroup ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionCodeBuildReportGroup	Allow	• codebuild:BatchGetReports • codebuild:BatchGetReportGroups • codebuild:ListReportsForReportGrou • codebuild:DescribeTestCases

Amazon EC2

AWS RAM 为可共享的 AWS 资源提供以下默认 Amazon EC2 托管权限。

资源类型	权限名称和 ARN	效果	操作
ec2:容量预留	名称:AWSRAMDefaultPermissionCapacityReservation ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionCapacityReservation	Allow	• ec2:RunInstance • ec2:DescribeCapacityReservations
ec2:DedicatedHost	名称:AWSRAMDefaultPermissionDedicatedHost ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionDedicatedHost	Allow	• ec2:RunInstances • ec2:StartInstances • ec2:DescribeHosts • ec2:ModifyInstancePlacement

Amazon EC2 映像生成器

AWS RAM 为可共享的 AWS 映像生成器资源提供以下默认 Amazon EC2 托管权限。

资源类型	权限名称和 ARN	效果	操作
映像生成器:组件	名称:AWSRAMDefaultPermissionImageBuilderComponent ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionImageBuilderComponent	Allow	• imagebuilder:GetComponent • imagebuilder:ListComponents

资源类型	权限名称和 ARN	效果	操作
映像生成器:映像	名称:AWSRAMDefaultPermissionImageBuilderImage ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionImageBuilderImage	Allow	• imagebuilder:GetImage • imagebuilder:ListImages
映像生成器:ImageRecipe	名称:AWSRAMDefaultPermissionImageBuilderImageRecipe ARN: arn:aws:ram::aws:permission/imagebuilder:AWSRAMDefaultPermissionImageBuilderImageRecipe	Allow	• imagebuilder:GetImageRecipe • imagebuilder:ListImageRecipes

AWS 粘合

AWS RAM 为可共享的 AWS Glue 资源提供以下默认 AWS 托管权限。

资源类型	权限名称和 ARN	效果	操作
glue:Catalog	名称:AWSRAMDefaultPermissionGlueCatalog ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionGlueCatalog	Allow	• glue:GetTable • glue:GetTableVersion • glue:GetTableVersions • glue:GetPartition • glue:GetPartitions • glue:BatchGetPartition • glue:GetDatabase • glue:GetTables • glue:GetDatabases • glue:SearchTables
glue:Database	名称:AWSRAMDefaultPermissionGlueDatabase ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionGlueDatabase	Allow	• glue:GetTable • glue:GetTableVersion • glue:GetTableVersions • glue:GetPartition • glue:GetPartitions • glue:BatchGetPartition • glue:GetDatabase • glue:GetDatabases • glue:GetTables • glue:SearchTables
glue:Table	名称:AWSRAMDefaultPermissionGlueTable ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionGlueTable	Allow	• glue:GetTable • glue:GetTableVersion • glue:GetTableVersions • glue:GetPartition • glue:GetPartitions • glue:BatchGetPartition

资源类型	权限名称和 ARN	效果	操作
			• glue:SearchTables

AWS License Manager

AWS RAM 为可共享的 AWS 资源提供以下默认 AWS License Manager 托管权限。

资源类型	权限名称和 ARN	效果	操作
license-manager:LicenseConfiguration	名称:AWSRAMDefaultPermissionLicenseConfiguration ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionLicenseConfiguration	Allow	• license-manager:GetLicenseConfiguration • license-manager:ListLicenseConfigurations • license-manager:ListAssociationsForLicense • license-manager:ListUsageForLicenseConfigu

AWS Outposts

AWS RAM 为可共享的 AWS 资源提供以下默认 AWS Outposts 托管权限。

> **Note**
>
> 有关 Outposts 上共享子网和本地网关路由表的默认 AWS 托管权限,请参阅子网 (p.)和本地网关路由表 (p.)。

资源类型	权限名称和 ARN	效果	操作
Outposts:Outpost	名称:AWSRAMDefaultPermissionOutpostsOutpost ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionOutpostsOutposts	Allow	• outposts:GetOutpost • outposts:GetOutpostInstanceTypes • outposts:ListOutposts

AWS 资源组

AWS RAM 为可共享的 AWS 资源提供以下默认 AWS 资源组 托管权限。

资源类型	权限名称和 ARN	效果	操作
resource-groups:组	名称:AWSRAMDefaultPermissionResourceGroup ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionResourceGroup	Allow	• resource-groups:GetGroup • resource-groups:GetGroupConfiguration • resource-groups:ListGroupResources

Amazon Route 53

AWS RAM 为可共享的 AWS 资源提供以下默认 Amazon Route 53 托管权限。

资源类型	权限名称和 ARN	效果	操作
route53resolver:ResolverRule	名称:AWSRAMDefaultPermissionResolverRule ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionResolverRule	Allow	• route53resolver:GetResolverRule • route53resolver:AssociateResolverR • route53resolver:DisassociateResolv • route53resolver:ListResolverRules • route53resolver:ListResolverRuleAs
route53resolver:ResolverQueryLogConfig	名称:AWSRAMDefaultPermissionResolverQueryLogConfig ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionResolverQueryLogConfig	Allow	• route53resolver:AssociateResolverQ • route53resolver:DisassociateResolv • route53resolver:ListResolverQueryL

Amazon VPC

AWS RAM 为可共享的 AWS 资源提供以下默认 Amazon VPC 托管权限。

资源类型	权限名称和 ARN	效果	操作
ec2:前缀列表	名称:AWSRAMDefaultPermissionPrefixList ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionPrefixList	Allow	• ec2:DescribeManagedPrefixLists • ec2:GetManagedPrefixListEntries
ec2:Subnet	名称:AWSRAMDefaultPermissionSubnet ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet	Allow	• ec2:RunInstances • ec2:CreateNetworkInterface • ec2:DescribeSubnets
ec2:TrafficMirrorTarget	名称:AWSRAMDefaultPermissionTrafficMirror ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionTrafficMirror	Allow	• ec2:DescribeTrafficMirrorTargets • ec2:CreateTrafficMirrorSession • ec2:DeleteTrafficMirrorSession • ec2:DescribeTrafficMirrorSessions
ec2:中转网关	名称:AWSRAMDefaultPermissionTransitGateway ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionTransitGateway	Allow	• ec2:DescribeTransitGateways • ec2:CreateTransitGatewayVpcAttachm • ec2:ModifyTransitGatewayVpcAttachm • ec2:DeleteTransitGatewayVpcAttachm
ec2:本地网关路由表	名称:AWSRAMDefaultPermissionLocalGateway	Allow	• ec2:CreateLocalGatewayRouteTableVp

资源类型	权限名称和 ARN	效果	操作
	ARN: arn:aws:ram::aws:permission/AWSRAMDefaultPermissionLocalGateway		• ec2:DeleteLocalGatewayRouteTableVp • ec2:DescribeLocalGatewayRouteTable • ec2:DescribeLocalGatewayRouteTable • ec2:DescribeLocalGatewayRouteTable • ec2:DescribeLocalGatewayVirtualInt • ec2:DescribeLocalGatewayVirtualInt • ec2:DescribeLocalGateways • ec2:SearchTransitGatewayRoutes

AWS RAM 中的日志记录和监控

监控是保持 AWS RAM 和 AWS 解决方案的可靠性、可用性和性能的重要环节。您应该从 AWS 解决方案的各个部分收集监控数据，以便您可以更轻松地调试多点故障（如果发生）。AWS 提供了多种工具来监控您的 AWS RAM 资源并对潜在事件做出响应：

Amazon CloudWatch Events

提供近乎实时的系统事件流以描述 AWS 资源的变化。CloudWatch Events 支持自动事件驱动型计算,因为您可以编写规则,以监控某些事件和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，请参阅使用 CloudWatch 事件监控 (p. 30)。

AWS CloudTrail

捕获由您的 AWS 账户或代表该账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以标识哪些用户和账户调用了 AWS、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅使用 AWS RAM 记录 AWS CloudTrail API 调用 (p. 30)。

使用 CloudWatch 事件监控

使用 Amazon CloudWatch Events，您可以为 AWS RAM 中的特定事件设置自动通知。AWS RAM 中的事件将近乎实时地传输到 CloudWatch Events。您可以将 CloudWatch Events 配置为监控事件并调用目标以响应指出对资源共享进行更改的事件。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可访问资源共享的principals触发事件。

当您创建事件模式时，源为 `aws.ram`。

有关更多信息，请参阅 Amazon CloudWatch Events 用户指南。

使用 AWS RAM 记录 AWS CloudTrail API 调用

AWS RAM 与 AWS CloudTrail 集成，后者是一项服务，该服务提供由用户、角色或 AWS RAM 中的 AWS 服务执行的操作的记录。CloudTrail 会捕获 AWS RAM 的所有 API 调用作为事件。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 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 User Guide。

CloudTrail中的 AWS RAM 信息

创建账户时，将在 AWS 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，并与其他 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。

要持续记录 AWS 账户中的事件（包括 AWS RAM 的事件），请创建跟踪。通过跟踪，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪在 AWS 分区中记录来自所有区域的事件，并将日志文件传送至您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 为 配置 Amazon SNS 通知 CloudTrail
- 接收多个区域中的 CloudTrail 日志文件和从多个账户中接收 CloudTrail 日志文件

所有 AWS RAM 操作均由 CloudTrail 记录下来并记载到 AWS RAM API 参考 中。例如，对 `CreateResourceShare` `AssociateResourceShare` 和 `EnableSharingWithAwsOrganization` 操作的调用在 CloudTrail 日志文件中生成一些条目。

每个事件或日志条目都包含有关生成请求的人员的信息。身份信息帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management (IAM) 用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

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 存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会以任何特定顺序显示。

以下示例说明了 `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 Resource Access Manager 中的恢复功能

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

有关 AWS 区域和可用区的更多信息，请参阅 AWS 全球基础设施。

AWS RAM 中的基础设施安全性

作为一项托管服务,AWS RAM 由 AWS 中所述的 Amazon Web Services 全球网络安全程序提供保护: 安全流程概述白皮书。

您可以使用 AWS 发布的 API 调用通过网络访问 AWS RAM。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve 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 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service (AWS STS) 生成临时安全凭证来对请求进行签名。

AWS RAM用户指南文档历史记录

下表介绍 AWS RAM 的文档更新。

更改	Description	Date
支持共享 Outposts 和本地网关路由表	使用 AWS RAM 共享 Outposts 和本地网关路由表。有关更多信息，请参阅 AWS Outposts (p. 6)和Amazon VPC (p. 7)。	2020 年 10 月 15 日
支持共享查询日志	使用 AWS RAM 共享 Route 53 查询日志。有关更多信息，请参阅Amazon Route 53 (p. 6)。	2020 年 9 月 7 日
支持共享 ACM Private CA 私有证书颁发机构 (CA)	使用 AWS RAM 共享 ACM Private CA 私有 CAs。 有关更多信息,请参阅AWS Certificate Manager 私有证书颁发机构 (p. 3)。	2020 年 8 月 17 日
支持共享 AWS Glue 数据目录、数据库和表	使用 AWS RAM 共享 AWS Glue 数据目录、数据库和表。有关更多信息，请参阅AWS 粘合 (p. 5)。	2020 年 7 月 07 日
支持共享托管前缀列表	使用 AWS RAM 共享托管前缀列表。有关更多信息，请参阅Amazon EC2 (p. 4)。	2020 年 6 月 29 日
支持共享 AWS Outposts 客户拥有的 IPv4 地址	使用 AWS RAM 共享 AWS Outposts 客户拥有的 IPv4 地址。有关更多信息，请参阅Amazon EC2 (p. 4)。	2020 年 4 月 22 日
支持共享 AWS App Mesh 网格	使用 AWS RAM 共享网格。有关更多信息，请参阅AWS App Mesh (p. 3)。	2020 年 1 月 17 日
支持共享 AWS CodeBuild 项目和报告组	使用 AWS RAM 共享 AWS CodeBuild 项目和报告组。有关更多信息，请参阅AWS CodeBuild (p. 4)。	2019 年 12 月 13 日
支持共享其他资源	使用 AWS RAM 共享 Amazon EC2 专用主机、AWS 资源组 资源组和 Amazon EC2 映像生成器组件、镜像和镜像配方。有关更多信息，请参阅可共享资源 (p. 2)。	2019 年 12 月 2 日
支持共享按需容量预留	使用 AWS RAM 共享按需容量预留。有关更多信息，请参阅Amazon EC2 (p. 4)。	2019 年 7 月 29 日

更改	Description	Date
支持共享 Aurora 数据库集群	使用 AWS RAM 共享 Aurora 数据库集群。有关更多信息，请参阅Amazon Aurora (p. 3)。	2019 年 7 月 02 日
支持共享 Traffic Mirroring 目标	使用 AWS RAM 共享 Traffic Mirroring 目标。有关更多信息，请参阅Amazon EC2 (p. 4)。	2019 年 6 月 25 日
支持共享许可证配置	使用 AWS RAM 共享 AWS License Manager 许可证配置。有关更多信息，请参阅AWS License Manager (p. 5)。	2018 年 12 月 5 日
支持共享子网	使用 AWS RAM 共享 Amazon VPC 子网。有关更多信息，请参阅Amazon EC2 (p. 4)。	2018 年 11 月 27 日
支持共享中转网关	使用 AWS RAM 共享 Amazon VPC 中转网关。有关更多信息，请参阅AWS License Manager (p. 5)。	2018 年 11 月 26 日
支持共享转发规则	使用 AWS RAM 共享 Route 53 转发规则。有关更多信息，请参阅Amazon Route 53 (p. 6)。	2018 年 11 月 20 日
首次发布	此版本引入了 AWS Resource Access Manager。	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。