aws

用户指南

AWS Organizations

AWS Organizations: 用户指南

Table of Contents

什么是 AWS Organizations？

AWS Organizations 是一项账户管理服务，使您能够将多个AWS 账户整合到您创建并集中管理的组织中。AWS Organizations 包含账户管理和整合账单功能，可利用这些功能更好地满足企业的预算、安全性和合规性需求。作为组织的管理员，您可以在组织中创建账户并邀请现有账户加入组织。

本用户指南定义 AWS Organizations 的关键概念、提供 教程并说明了如何创建和管理组织。

主题

AWS Organizations 功能

AWS Organizations 提供以下功能：

集中管理您的所有 AWS 账户

> 您可以将您的现有账户并入组织中，以便集中管理这些账户。您可以创建自动成为组织的一部分的账户，并且您可以邀请其他账户加入您的组织。您也可以附加将影响您的部分或所有账户的策略。

所有成员账户的整合账单

> 整合账单是 AWS Organizations 的一项功能。您可以使用自己所属组织的管理账户，来整合所有成员账户，并为成员账户进行支付。在整合账单中，管理账户还可以访问其组织中成员账户的账单信息、账户信息和账户活动。此信息可用于诸如 Cost Explorer 之类的服务，这些服务可以帮助管理账户提高其组织的成本性能。

对账户进行分层分组以满足预算、安全性或合规性需求

> 您可以将您的账户分组到组织单元 (OU) 中并将不同的访问策略附加到每个 OU。例如，如果您的账户必须仅访问满足特定法规要求的 AWS 服务，您可以将这些账户放入一个 OU 中。然后，您可以将策略附加到该 OU，这将阻止访问未满足这些法规要求的服务。您可以将 OU 嵌套在其他 OU 内 (深度为 5 个分层)，以便灵活地构建账户组的结构。

集中控制每个账户可访问的 AWS 服务和 API 操作的策略

作为组织管理账户的管理员，您可以使用服务控制策略（SCP）指定组织中成员账户的最大权限数。在 SCP 中，您可以限制每个成员账户中的用户和角色可以访问的 AWS 服务、资源和各个 API 操作。您还可以定义有关何时限制对 AWS 服务、资源和 API 操作的访问的条件。这些限制甚至会覆盖组织内的成员账户的管理员。当 AWS Organizations 阻止对某个成员账户对服务、资源或 API 操作的访问时，该账户中的用户或角色将无法访问它。即使成员账户的管理员在 IAM 策略中明确授予此类权限，此阻止仍然有效。

有关更多信息，请参阅服务控制策略 (SCP)。

在组织账户中跨资源标准化标签的策略

您可以使用标签策略来维护一致的标签，包括标签键和标签值的首选大小写处理。

有关更多信息，请参阅标签策略

控制 AWS 人工智能 (AI) 和机器学习服务如何收集和存储数据的策略。

您可以使用 AI 服务选择退出策略来选择退出任何您不希望使用的 AWS AI 服务的数据收集和存储服务。

有关更多信息，请参阅AI 服务选择退出策略

为组织账户中的资源配置自动备份的策略

您可以使用备份策略为所有组织账户中的资源配置和自动应用 AWS Backup 计划。

有关更多信息，请参阅备份策略

针对 AWS Identity and Access Management (IAM) 的集成和支持

IAM 提供对单个账户中的用户和角色的精细控制。AWS Organizations 通过使您能够控制一个账户或一组账户中的哪些用户和角色可执行哪些操作来扩展对账户级别的控制。生成的权限是账户级别的 AWS Organizations 允许的内容的逻辑交集，以及 IAM 在该账户内的用户或角色级别明确授予的权限。换言之，用户只能访问 AWS Organizations 策略和 IAM 策略都允许的内容。如果任一策略阻止某个操作，用户将无法访问该操作。

与其他 AWS 服务集成

您可以将 AWS Organizations 中提供的多账户管理服务与选定 AWS 服务结合使用，以在作为组织成员的所有账户上执行任务。有关服务以及在组织范围级别使用每项服务的好处的列表，请参阅AWS 可以与之配合使用的服务 AWS Organizations。

当您启用某个AWS服务代表您执行组织成员账户中的任务时，AWS Organizations 会在每个成员账户中为该服务创建一个 IAM 服务相关角色。此服务相关角色具有预定义的 IAM 权限，此类权限允许另一AWS服务在您的组织及其账户中执行特定任务。为正常工作，组织中的所有账户都会自动具有服务相关角色。此角色允许 AWS Organizations 服务创建您启用了信任访问权限的AWS服务所需的服务相关角色。这些额外的服务相关角色已附加到 IAM 权限策略，这些策略指定服务能够仅执行您的配置选择所需的那些任务。有关更多信息，请参阅将 AWS Organizations 与其它 AWS 产品结合使用。

全局访问

AWS Organizations 是一项全局服务，具有单个终端节点，可从任何和所有AWS 区域中工作。您无需明确地选择要在其中操作的区域。

具备最终一致性的数据复制

与许多其他 AWS 服务一样，AWS Organizations 具有最终一致性。AWS Organizations 通过复制其区域内 AWS 数据中心的多个服务器上的数据来实现高可用性。如果成功请求更改某些数据，则更改会提交并安全存储。但是，之后必须在多个服务器中复制此更改。有关更多信息，请参阅我所做的更改不总是立即可见。

免费使用

AWS Organizations 是为您的AWS 账户账户提供的一项功能，无需额外收费。只有在您访问组织账户中其他AWS服务时，才会向您收费。有关其他AWS产品定价信息，请参阅亚马逊云科技定价页。

AWS Organizations 定价

不另外收取 AWS Organizations 费用。您只需为成员账户中的用户和角色所使用的 AWS 资源付费。例如，您需要支付成员账户中的用户或角色所使用的 Amazon EC2 实例的标准费用。有关其他AWS服务定价的信息，请参阅AWS定价。

访问 AWS Organizations

您可以通过以下任何方式使用 AWS Organizations:

AWS Management Console

AWS Organizations 控制台是一个基于浏览器的界面，您可以用它来管理您的组织和您的 AWS 资源。您可以使用控制台在组织中执行任何任务。

AWS 命令行工具

使用 AWS 命令行工具，您可在系统的命令行中发出命令以执行 AWS Organizations 和 AWS 任务。与使用控制台相比，使用命令行处理更快、更方便。如果要构建执行 AWS 任务的脚本，命令行工具也会十分有用。

AWS 提供两组命令行工具：

- AWS Command Line Interface（AWS CLI）。有关安装与使用 AWS CLI 的信息，请参阅 AWS Command Line Interface 用户指南。
- AWS Tools for Windows PowerShell。有关安装和使用 Tools for Windows PowerShell 的信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

AWS 开发工具包

AWS 开发工具包包含各种编程语言和平台（例如，Java、Python、Ruby、.NET、iOS 和 Android）的库和示例代码。开发工具包执行以下类似任务：加密签署请求、管理错误以及自动重试请求。有关 AWS 开发工具包的更多信息（包括如何下载和安装这些工具包），请参阅适用于 Amazon Web Services 的工具。

AWS Organizations HTTPS 查询 API

AWS Organizations HTTPS 查询 API 使您能够以编程方式访问 AWS Organizations 和 AWS。HTTPS 查询 API 可让您直接向服务发布 HTTPS 请求。使用 HTTPS 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，请参阅通过提出 HTTP 查询请求来调用 API 和 AWS Organizations API 参考。

对 AWS Organizations 的支持和反馈

我们欢迎您提供反馈。您可以将评论发送到 feedback-awsorganizations@amazon.com。您也可以在 AWS Organizations 支持论坛上发布反馈和问题。有关 AWS 支持论坛的更多信息，请参阅论坛帮助。

其他 AWS 资源

- AWS培训和课程 – 指向基于角色的专业课程和自主进度动手实验室的链接，这些课程和实验室旨在帮助您增强AWS技能并获得实践经验。
- AWS开发工具 – 指向开发工具和资源的链接，其中提供了文档、代码示例、发布说明和有助于您利用AWS构建创新应用程序的其他信息。
- AWS Support Center – 用于创建和管理 AWS Support 案例的中心。还包括指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况和 AWS Trusted Advisor。

- AWS Support – 提供有关 AWS Support 的信息的主要网页，是一种一对一的快速响应支持渠道，可帮助您在云中构建和运行应用程序。
- 联系我们 – 用于查询有关AWS账单、账户、事件、滥用和其他问题的中央联系点。
- AWS 网站条款 – 有关我们的版权和商标、您的账户、许可、网站访问和其他主题的详细信息。

AWS Organizations 入门

以下主题提供了帮助您开始学习和使用 AWS Organizations 的信息。

了解...

[AWS Organizations 术语和概念]

学习了解 AWS Organizations 所要掌握的术语和核心概念。本部分介绍组织的每个组件及其如何协同工作来提升对账户中用户操作的控制能力。

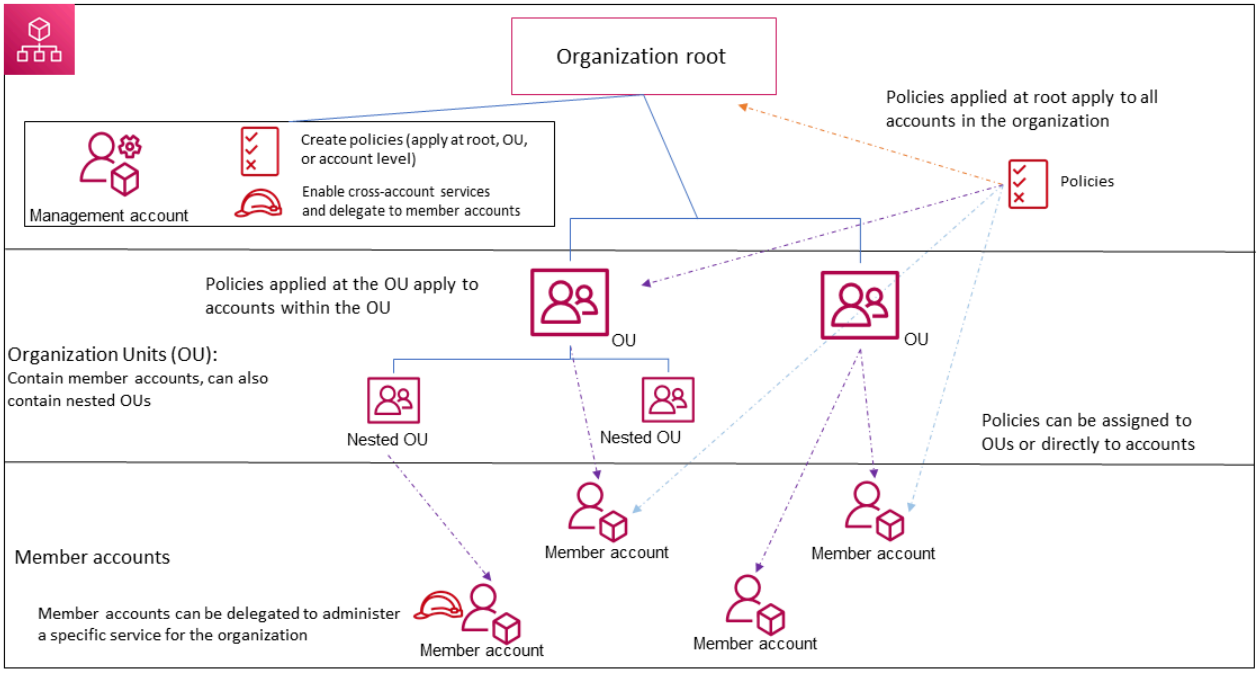
[组织的整合账单]

AWS Organizations 的主要功能之一是整合组织中所有账户的账单。详细了解组织中账单的处理方式以及在多个账户间共享的各种折扣的工作原理。此内容位于《AWS Billing 用户指南》中。

AWS Organizations 术语和概念

为了帮助您开始使用 AWS Organizations，本主题介绍了一些主要概念。

下图显示了一个包含五个账户的基本组织，这些账户在根下分为四个组织部门（OU）。此外，该组织还有一些策略附加到其中部分 OU 或者直接附加到账户。有关这些项目中每一项的描述，请参阅本主题中的定义。



Organization（组织）

您为合并 AWS 账户（以便可以将这些账户作为单个单位进行管理）而创建的实体。您可以使用 AWS Organizations 控制台集中查看和管理组织内您的所有账户。一个组织有一个管理账户以及零个或多个成员账户。您可以以分层树状结构组织账户，将根放在树顶部，组织部门嵌套在根下。每个账户都可以直接放在根中，也可以放在层次结构的其中一个 OU 中。一个组织的功能由您启用的功能集决定。

Root

您的组织的所有账户的父容器。如果您将一个策略附加到根，则它应用于组织中的所有组织部门 (OU) 和账户。

> **Note**
>
> 当前，您只能有一个根。AWS Organizations 将在您创建组织时自动为您创建此根。

组织部门 (OU)

根中账户的容器。OU 还可以包含其他 OU，这使您能够创建类似于倒置树的层次结构，根位于顶部，OU 分支向下延伸，结束于作为树叶的账户。当您将策略附加到层次结构中的其中一个节点时，策略会向下流动，影响该节点下的所有分支 (OU) 和树叶 (账户)。一个 OU 有且仅有一个父级，而目前每个账户都正好是一个 OU 的成员。

账户

Organizations 中的账户是标准AWS 账户，其中包含您的AWS资源以及可以访问这些资源的身份。

> **Tip**
>
> AWS 账户与用户账户并非同一账户。AWS用户是您使用 AWS Identity and Access Management（IAM）创建的身份，其形式为具有长期凭证的 IAM 用户，或具有短期凭证的 IAM 角色。单个AWS账户可以而且通常包含许多用户和角色。

组织中有两种类型的账户：一个指定为管理账户的单个账户，以及一个或多个成员账户。

- 管理账户是您用于创建组织的账户。从组织的管理账户中，您可以执行以下操作：
  - 在组织中创建账户
  - 邀请其他现有账户到组织中
  - 从组织中删除账户
  - 指定委托管理员账户
  - 管理邀请
  - 将策略应用到组织内的实体（根、OU 或者账户）
  - 启用与支持的AWS服务的集成，以便为组织中的所有账户提供服务功能。

  管理账户具有付款人账户的责任，并负责支付成员账户产生的所有费用。您无法更改一个组织的管理账户。
- 成员账户组成组织中的所有账户的其余部分。一个账户一次只能是一个组织的成员。您可以将策略附加到账户，以仅对这个账户进行控制。

> **Note**
>
> 您可以将一些成员账户指定为委托管理员账户。请参阅下面的 委托管理员。

委托管理员

我们建议您将 Organizations 管理账户及其用户和角色仅用于必须由该账户执行的任务。我们建议您将所有的 AWS 资源存储在组织的其他成员账户中，而非保存在管理账户中。这是因为，Organizations 服务控制策略（SCP）等安全功能不会限制管理账户中的任何用户或角色。将资源与管理账户分离还可帮助您了解发票上的费用。在组织的管理账户中，您可以将一个或多个成员账户指定为委托管理员账户，以帮助您实施此建议。您可以使用两种类型的委托管理员：

- Organizations 委托管理员：通过这些账户，您可以管理组织策略并将策略附加到组织内的实体（根、OU 或账户）。管理账户可以对委托权限进行精细控制。参阅 的委派管理员 AWS Organizations 了解更多信息。
- AWS 服务的委托管理员：通过这些账户，您可以管理与 Organizations 集成的 AWS 服务。管理账户可以根据需要，将不同的成员账户注册为不同服务的委托管理员。这些账户拥有特定服务的管理权限，以及 Organizations 只读操作权限。参阅 与 Organizations 配合使用的 AWS 服务的委托管理员 了解更多信息。

邀请

邀请其他账户加入您的组织的过程。邀请只能由组织的管理账户发出。邀请扩展到与受邀账户相关联的账户 ID 或电子邮件地址。受邀账户接受邀请后，它将成为组织中的成员账户。如果组织需要所有当前成员账户批准将仅支持整合账单功能更改为支持组织中的所有功能，也可以将邀请发送到所有成员。通过交换握手信息，对各个账户发出邀请。在 AWS Organizations 控制台中处理时，您可能看不到握手。但是，如果您使用 AWS CLI 或 AWS Organizations API，则必须直接处理握手。

握手

在双方之间交换信息的多步骤过程。它在 AWS Organizations 中的一项主要用途就是作为邀请的底层实施。握手消息在握手发起方和接收方之间传递并由双方进行响应。消息的传递方式有助于确保双方知道当前状态是什么。将组织从仅支持整合账单功能更改为支持 提供的所有功能AWS Organizations时，也可以使用握手。仅当您使用 AWS Organizations API 或命令行工具（如 AWS CLI）时，您通常需要直接与握手交互。

可用的功能集

- 所有功能 – AWS Organizations 可用的默认功能集。它包括整合账单的所有功能，此外还包括高级功能，可让您更好地控制组织中的账户。例如，当启用了所有功能时，组织的管理账户将能够完全控制成员账户可以执行的操作。管理账户可以应用 SCP 来限制账户中的用户（包括根用户）和角色可以访问的服务和操作。管理账户可以防止成员账户退出组织。此外，您还可以启用与支持的 AWS 服务的集成，以便让这些服务为组织中的所有账户提供功能。

您可以创建一个已启用所有功能的组织，或者您可以启用最初仅支持整合账单功能的组织中的所有功能。要启用所有功能，所有受邀成员账户都必须批准更改，方法为接受当管理账户启动此过程时发送的邀请。

- 整合账单 – 此功能集提供共享账单功能，但不包括 AWS Organizations 的更多高级功能。例如，您无法让与组织集成的其他 AWS 服务在组织内的所有账户中运作，也不能使用策略来限制不同账户中的用户和角色可以执行的操作。要使用高级 AWS Organizations 功能，您必须启用组织中的所有功能。

服务控制策略 (SCP)

一个策略，用于指定 SCP 所影响账户中的用户和角色可以使用的服务和操作。SCP 类似于 IAM 权限策略，不同的是前者不授予任何权限。相反，SCP 指定组织、组织单位 (OU) 或账户的最大权限数。在将 SCP 附加到组织根或 OU 时，SCP 限制成员账户中实体的权限。

允许列表与拒绝列表

允许列表和拒绝列表是您应用 SCP 以筛选可供账户使用的权限时的补充策略。

- 允许列表策略 – 您明确指定允许的访问权限。隐式阻止所有其他访问权。默认情况下，AWS Organizations 将名为 `FullAWSAccess` 的 AWS 托管策略附加到所有根、OU 和账户。这样有助于确保在您构建您的组织时，除非您希望，否则不会阻止任何内容。换句话说，默认情况下将允许所有权限。当您准备限制权限时，您需要将 `FullAWSAccess` 策略替换为仅允许限制性更强的所需权限集的策略。然后，受影响账户中的用户和角色只能使用该级别的访问权限，即使它们的 IAM policy 允许所有操作也是如此。如果您在根上替换默认策略，则组织中的所有账户都受限制规则的影响。您不能在层次结构中的较低级别重新添加权限，因为 SCP 永远不会授予权限；它只筛选权限。

- 拒绝列表策略 – 您明确指定不允许的访问权限。允许所有其他访问权。在这种情况下，除非明确阻止，否则允许所有权限。这是 AWS Organizations 的默认行为。默认情况下，AWS Organizations 将名为 `FullAWSAccess` 的 AWS 托管策略附加到所有根、OU 和账户。这样允许任何账户访问任何服务或操作，没有 AWS Organizations 施加的限制。与上述允许列表技术不同，使用拒绝列表时，您会保留默认 `FullAWSAccess` 策略（允许“全部”）。但是，您可以附加额外的策略，明确拒绝 访问不需要的服务和操作。与使用 IAM 权限策略一样，显式拒绝服务操作将覆盖该操作的任何允许规则。

人工智能（AI）服务选择退出政策

一种策略，可帮助您标准化您组织中的所有账户的 AWS AI 服务的选择退出设置。某些 AWS AI 服务可以存储和使用通过这些服务处理的客户内容，以开发和持续改进 Amazon AI 服务和技术。作为

AWS客户，您可以使用 AI 服务选择退出策略选择退出存储或使用您的内容以这一服务，以改进服务。

备份策略

此策略可帮助您将资源标准化，并为组织中的所有账户的资源实施备份策略。在备份策略中，您可以为资源配置和部署备份计划。

标签策略

策略的一种类型，可帮助您在组织中所有账户内的资源中标准化标签。在标签策略中，您可以为特定资源指定标记规则。

AWS Organizations 教程

使用本部分的教程，了解如何使用 AWS Organizations 执行任务。

教程：创建和配置组织

通过分步说明来创建组织并启动和运行，邀请您的第一个成员账户，创建包含账户的 OU 层次结构，以及应用几个服务控制策略 (SCP)。

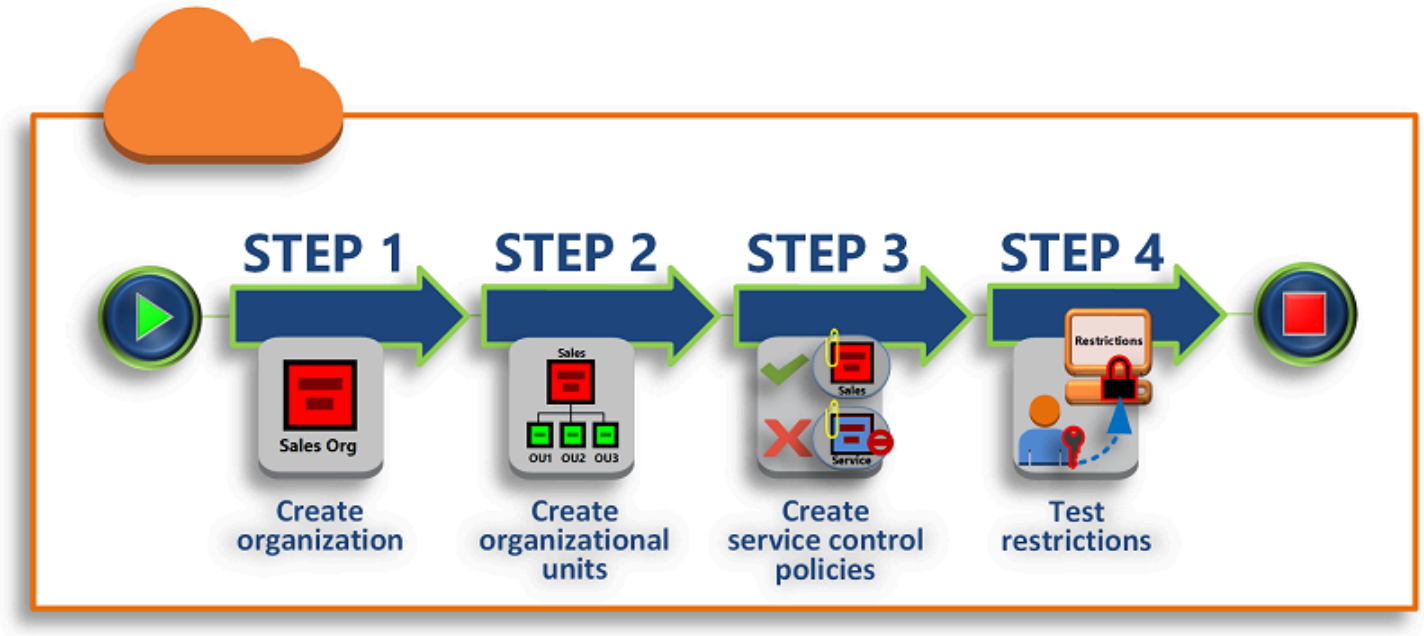
教程：使用 Amazon EventBridge 监控对您的组织进行的重要更改

配置 Amazon EventBridge 来监控组织中的重要更改，从而在组织中发生您指定的操作时，通过电子邮件、短信或日志条目等形式触发警报。例如，许多组织希望了解何时创建了新账户，或账户何时尝试离开组织。

教程：创建和配置组织

在本教程中，您将创建组织并为其配置两个 AWS 成员账户。您可以在组织中创建其中一个成员账户，然后邀请另一个账户加入您的组织。接下来，您可以使用允许列表方法指定账户管理员只能委派明确列出的服务和操作。这使得管理员可以先验证 AWS 引入的任何新服务，然后才允许由公司中的任何其他人使用。这样，如果 AWS 引入新服务，它将保持被禁止的状态，直至管理员将该服务添加到相应策略的允许列表中。本教程还为您演示如何使用拒绝列表来确保成员账户中的任何用户都无法更改 AWS CloudTrail 创建的审核日志的配置。

下图演示了本教程的主要步骤。



步骤 1：创建组织

在此步骤中，您将使用现有的AWS 账户作为管理账户来创建组织。您还将邀请一个AWS 账户加入您的组织，并创建另一个账户作为成员账户。

步骤 2：创建组织单元

接下来，您将在新组织中创建两个组织部门 (OU)，并将成员账户放在这些 OU 中。

步骤 3：创建服务控制策略

您可以应用限制，使用服务控制策略 (SCP) 来限制可以将哪些操作委派给成员账户中的用户和角色。在此步骤中，您将创建两个 SCP 并将其附加到您组织中的 OU。

步骤 4：测试组织的策略

您可以使用各测试账户中用户的身份登录，查看 SCP 在相应账户上产生的效果。

本教程中的任何步骤都不会在 AWS 账单中产生费用。AWS Organizations 是一项免费服务。

前提条件

本教程假设您有权访问两个现有的AWS 账户（在本教程中将创建第三个），并且可以使用管理员身份登录各个账户。

教程使用的账户如下：

- 111111111111 – 您用于创建组织的账户。此账户将成为管理账户。此账户的所有者的电子邮件地址为 OrgAccount111@example.com。
- 222222222222 – 您邀请作为成员账户加入组织的账户。此账户的所有者的电子邮件地址为 member222@example.com。
- 333333333333 – 您作为组织成员创建的账户。此账户的所有者的电子邮件地址为 member333@example.com。

使用与您的测试账户关联的值替换以上值。我们建议您不要为本教程使用生产账户。

步骤 1：创建组织

在此步骤中，您将以管理员身份登录账户 111111111111，使用该账户作为管理账户创建组织，然后邀请现有账户 222222222222 作为成员账户加入。

AWS Management Console

1. 以账户 111111111111 的管理员身份登录AWS，并打开 AWS Organizations 控制台。
2. 在介绍页面上，选择 Create an organization (创建组织)。
3. 在确认对话框中，选择 Create an organization (创建组织)。

   > **Note**
   >
   > 默认情况下，组织在创建时已启用所有功能。您也可以创建自己的组织并仅启用整合账单功能。

   AWS创建组织，并向您显示AWS 账户页面。如果您在其他页面上，请在左侧的导航窗格中选择AWS 账户。

   如果您使用的账户使用未经过AWS验证的电子邮件地址，则验证电子邮件自动发送至您的管理账户关联的地址。在您接收到验证电子邮件之前可能会有一段延迟。
4. 在 24 小时内验证您的电子邮件地址。有关更多信息，请参阅电子邮件地址验证。

您现在拥有一个组织，并且您的账户是其唯一成员。这是组织的管理账户。

邀请现有账户加入组织

现在您已拥有一个组织，您可以开始向其中填充账户。在本部分的步骤中，您将邀请现有账户作为组织成员加入。

AWS Management Console

邀请现有账户加入

1. 导航到AWS 账户页面，然后选择 Add an AWS 账户 (添加亚马逊云科技账户)。
2. 在添加 AWS 账户页面上，选择邀请现有 AWS 账户。
3. 在 Email address or account ID of an AWS 账户 to invite (待邀请亚马逊云科技账户的电子邮件地址和账户 ID) 框中，输入待邀请账户的拥有者的电子邮件地址，类似于以下内容：**member222@example.com**。或者，如果您知道 AWS 账户 ID 号，可以将其输入。
4. 在 Message to include in the invitation email message (要包含在邀请电子邮件中的信息) 框中键入所需的任何文本。此文本会包含在发送到账户所有者的电子邮件中。
5. 选择 Send invitation (发送邀请)。AWS Organizations 向账户拥有者发送邀请。

   > **Important**
   >
   > 如果有错误消息指示，请将其展开。如果错误指示您超出了组织的账户限制或因组织仍在初始化而无法添加账户，请在创建组织后等待一个小时，然后重试。如果错误仍然存在，请联系 AWS Support。

6. 对于本教程，您现在需要接受自己的邀请。执行以下操作之一可在控制台中打开 Invitations 页面：

   - 打开AWS从管理账户发出的电子邮件，并选择链接以接受邀请。在系统提示登录时，以受邀成员账户的管理员身份执行操作。
   - 打开 AWS Organizations 控制台 并导航到 Invitations (邀请) 页面。

7. 在AWS 账户页面上，选择 Accept (接受)，然后选择 Confirm (确认)。

   > **Tip**
   >
   > 邀请回执可能会延迟，在您能接受邀请前，可能需要等待一段时间。

8. 注销成员账户，然后以管理账户管理员的身份登录。

创建成员账户

在本部分的步骤中，您将创建一个自动成为组织成员的AWS 账户。在本教程中，我们将此账户称为333333333333。

AWS Management Console

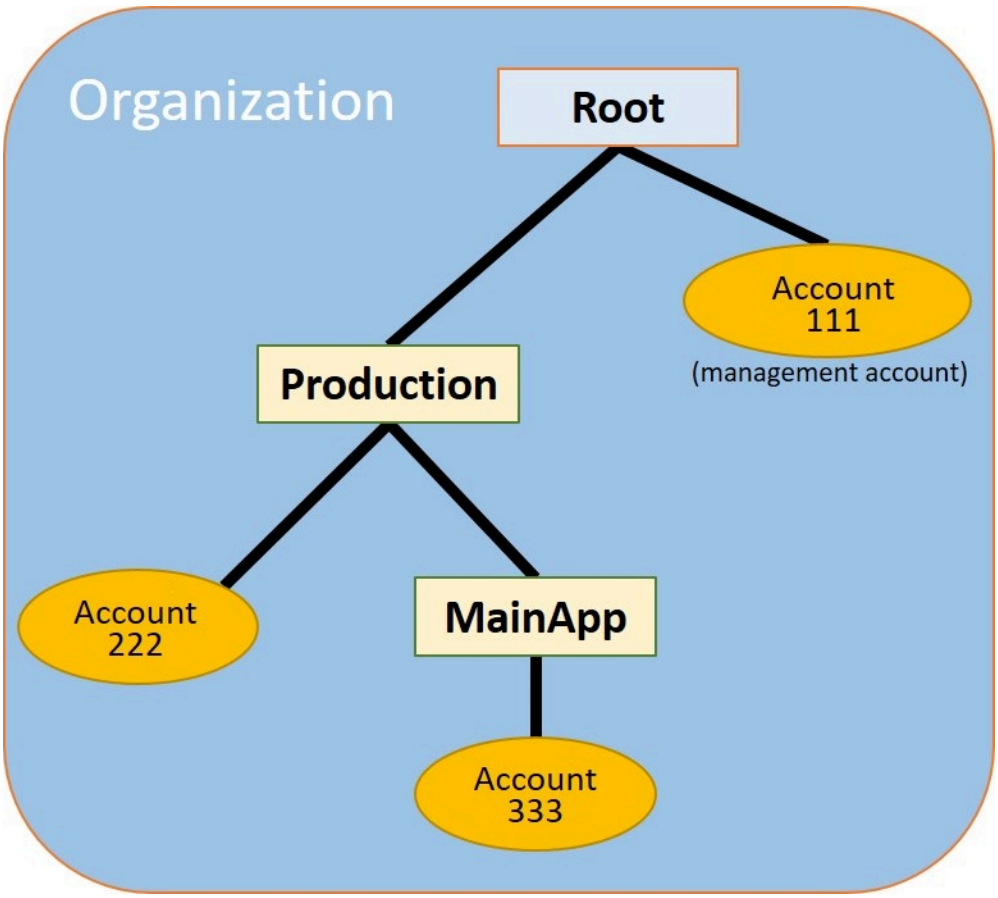
创建成员账户

1. 在 AWS Organizations 控制台的AWS 账户页面上，选择 Add AWS 账户 (添加亚马逊云科技账户)。
2. 在 Add an AWS 账户 (添加亚马逊云科技账户) 页面上，选择 Create an AWS 账户 (创建亚马逊云科技账户)。
3. 对于 AWS 账户 name (亚马逊云科技账户名称)，输入账户的名称，例如 **MainApp Account**。
4. 对于 Email address of the account's root user (账户根用户的电子邮件)，输入代表账户接收通信的人员的电子邮件地址。此值必须全局唯一。任何两个账户不能具有相同的电子邮件地址。例如，您可能会使用类似于 **mainapp@example.com** 的内容。
5. 对于 IAM role name，您可以将此处留空以自动使用 `OrganizationAccountAccessRole` 的默认角色名称，也可以提供自己的名称。此角色使您在以管理账户中 IAM 用户的身份登录时能够访问新成员账户。对于本教程，将此字段留空可指示 AWS Organizations 创建具有默认名称的角色。
6. 选择 Create AWS 账户 (创建亚马逊云科技账户)。您可能需要等待片刻再刷新页面，才能看到新账户显示在AWS 账户页面上。

> **Important**
>
> 如果您收到一个错误，它指明您超出了组织的账户限制或因组织仍在初始化而无法添加账户，请在创建组织后等待一个小时，然后重试。如果错误仍然存在，请联系 AWS Support。

步骤 2：创建组织单元

在本部分的步骤中，您将创建组织部门 (OU) 并放入成员账户。在完成后，您的层次结构类似于下图所示。管理账户将保留在根中。一个成员账户移动到 Production OU，另一个成员账户移动到 MainApp OU，这是 Production 的子级。



AWS Management Console

创建和填充 OU

> **Note**
>
> 在随后的步骤中，您可以与对象交互，您可以选择对象本身的名称或对象旁边的单选按钮。
>
> - 如果选择对象的名称，则会打开一个显示对象详细信息的新页面。
> - 如果选择对象旁边的单选按钮，则会识别要对该对象执行操作的其他操作（例如选择菜单选项）。
>
> 后续步骤会让您选择单选按钮，以便您随后可以通过选择菜单来对关联的对象执行操作。

1. 在 AWS Organizations 控制台中，导航到AWS 账户页面。

2. 选中 Root (根) 容器旁的复选框

   。
3. 在 Children (子级) 选项卡上，选择 Actions (操作)，然后在 Organizational unit (组织部门) 中选择 Create new (新建)。
4. 在 Create organizational unit in Root (在根中创建组织部门) 页面上，为 Organizational unit name (组织部门名称) 输入 **`Production`**，然后选择 Create organizational unit (创建组织部门)。
5. 选中您的新 Production OU 旁边的复选框

   。
6. 选择 Actions (操作)，然后在 Organizational unit (组织部门) 中，选择 Create new (新建)。
7. 在 Create organizational unit in Production (在生产中创建组织部门) 页面上，为次要 OU 名称输入 **`MainApp`**，然后选择 Create organizational unit (创建组织部门)。

   现在，您可以将成员账户移动到这些 OU 中。
8. 返回到AWS 账户页面，然后选择 Production OU 旁边的三角形

   ，以展开该 OU 的树形图。这将 MainAppOU 显示为 Production (生产) 的子级。
9. 在 333333333333 旁边，选中复选框

   （而不是其名称），选择操作，然后在 AWS 账户 下选择移动。
10. 在移动 AWS 账户 '333333333333' 页面上，选择生产旁边的三角形将其展开。在 MainApp 旁边，选择单选按钮

    （而不是其名称），然后选择移动 AWS 账户。
11. 在 222222222222 旁边，选中复选框

    （而不是其名称），选择操作，然后在 AWS 账户 下选择移动。
12. 在移动 AWS 账户 '222222222222' 页面上，在生产旁边选择单选按钮（而不是其名称），然后选择移动 AWS 账户。

步骤 3：创建服务控制策略

在本部分的步骤中，您将创建三个服务控制策略 (SCP) 并将其附加到根和 OU，用于限制组织账户中的用户所能执行的操作。第一个 SCP 防止任何成员账户中的任何人创建或修改您配置的任何 AWS

CloudTrail 日志。管理账户不受任何 SCP 的影响，因此在应用 CloudTrail SCP 之后，您必须从管理账户创建任何日志。

在根中为组织启用服务控制策略类型

您必须先为组织启用策略类型，然后才能附加任何类型的策略到该根或根中的任何 OU。默认情况下未启用策略类型。本部分的步骤将向您演示如何为组织启用服务控制策略 (SCP) 类型。

AWS Management Console

为您的组织启用 SCP

1. 导航到策略页面，然后选择服务控制策略。
2. 在存储库的 Service control policies (服务控制策略) 页面上，选择 Enable service control policies (启用服务控制策略)。

   此时将显示一个绿色横幅，通知您现在可以在组织中创建 SCP。

创建 SCP

现在，您的组织中已启用服务控制策略，您可以创建本教程所需的三个策略。

AWS Management Console

创建阻止 CloudTrail 配置操作的第一个 SCP

1. 导航到策略页面，然后选择服务控制策略。
2. 在 Service control policies (服务控制策略) 页面上，选择 Create policy (创建策略)。
3. 对于 Policy name，输入 **`Block CloudTrail Configuration Actions`**。
4. 在策略部分右侧的服务列表中，选择服务的 CloudTrail。然后选择以下操作：：AddTags、CreateTrail、DeleteTrail、RemoveTags、StartLogging、StopLogging 和 UpdateTrail。
5. 仍在右侧窗格中，选择添加资源并指定 CloudTrail 和所有资源。选择添加资源。

   左侧的策略语句应与以下内容类似。

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

```
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. 选择创建策略。

第二条策略定义一个允许列表，其中包含您要为生产 OU 中的用户和角色启用的所有服务和操作。完成后，生产 OU 中的用户只能 访问列出的服务和操作。

AWS Management Console

创建第二个策略，该策略将允许生产 OU 的已批准服务

1. 在 Service control policies (服务控制策略) 页面上，选择 Create policy (创建策略)。
2. 对于 Policy name，输入 **`Allow List for All Approved Services`**。
3. 将光标置于 Policy (策略) 部分的右窗格中，并粘贴一个与以下内容类似的策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
```

```
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
}
```

4. 选择创建策略。

最后一条策略提供了阻止在 MainApp OU 中使用的服务的拒绝列表。对于本教程，您需要阻止 MainApp OU 中的任何账户访问 Amazon DynamoDB。

AWS Management Console

创建第三条策略，将拒绝访问不能在 MainApp OU 中使用的服务

1. 在 Service control policies (服务控制策略) 页面上，选择 Create policy (创建策略)。
2. 对于 Policy name，输入 **`Deny List for MainApp Prohibited Services`**。
3. 在左侧的 Policy (策略) 部分中，选择服务的 Amazon DynamoDB。对于操作，选择 All actions (所有操作)。
4. 仍在左侧窗格中，选择 Add resource (添加资源) 并指定 DynamoDB 和 All Resources (所有资源)。选择添加资源。

   右侧的策略语句将更新为与以下内容类似的内容。

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

5. 选择 Create policy (创建策略) 保存 SCP。

将 SCP 附加到您的 OU

现在已经存在 SCP 并且为您的根启用了这些策略，您可以将它们附加到根和 OU。

AWS Management Console

将策略附加到根和 OU

1. 导航到AWS 账户页面。
2. 在AWS 账户页面上，选择 Root (根)（其名称，而不是单选按钮）导航到其详细信息页面。
3. 在 Root (根) 详细信息页面上，选择 Policies (策略) 选项卡，然后在 Service Control Policies (服务控制策略) 下，选择 Attach (附加)。
4. 在 Attach a service control policy (附加服务控制策略) 页面上，选择名为 `Block CloudTrail Configuration Actions` 的 SCP 旁边的单选按钮，然后选择 Attach (附加)。在本教程中，您会将其附加到根，这样它会影响所有成员账户，阻止任何人变更 CloudTrail 的配置方式。

   Root (根) 详细信息页面、Policies (策略) 选项卡显示有两个 SCP 已经附加到了根：您刚刚附加的一个以及默认的 `FullAWSAccess` SCP。
5. 导航回AWS 账户页面，然后选择 Production OU（它的名称，而不是单选按钮）导航到其详细信息页面。
6. 在 Production OU 的详细信息页面上，选择 Policies (策略) 选项卡。
7. 在 Service Control Policies (服务控制策略) 下，选择 Attach (附加)。
8. 在 Attach a service control policy (附加服务控制策略) 页面上，选择 `Allow List for All Approved Services` 旁边的单选按钮，然后选择 Attach (附加)。这允许 Production OU 的成员账户中的用户或角色访问批准的服务。
9. 选择 Policies (策略) 选项卡，可以看到有两个 SCP 已附加到 OU：您刚刚附加的一个以及默认的 `FullAWSAccess` SCP。但是，由于 `FullAWSAccess` SCP 同时也是允许所有服务和操作的允许列表，您现在必须分离此 SCP 以确保只允许您批准的服务。
10. 要从 Production OU 删除默认策略，请选择单选按钮 FullAWSAccess，选择 Detach (分离)，然后在确认对话框中选择 Detach policy (分离策略)。

    删除此默认策略之后，Production OU 下的所有成员账户都将立即失去对不在允许列表 SCP（您已在前一步中附加）中的所有操作和服务的访问权。任何使用未包含在所有批准服务的允许列表 SCP 中的操作的请求都将被拒绝。即使账户中的管理员通过将 IAM 权限策略附加到其中一个成员账户中的用户来授予对其他服务的访问权限，情况依然如此。

11. 现在，您可以附加名为 `Deny List for MainApp Prohibited services` 的 SCP，以防止 MainApp OU 的账户中的任何人使用任何受限制服务。

    要执行此操作，请导航到AWS 账户页面上，选择三角形图标以展开 Production 的分支，然后选择 MainAppOU（它的名称，而不是单选按钮）以导航到其内容。

12. 在 MainApp 详细信息页面上，选择 Policies (策略) 选项卡。
13. 在 Service Control Policies (服务控制策略) 下，选择 Attach (附加)，然后在可用策略列表中，选择 Deny List for MainApp Prohibited Services (MainApp 禁止的服务的拒绝列表) 旁边的单选按钮，然后选择 Attach policy (附加策略)。

步骤 4：测试组织的策略

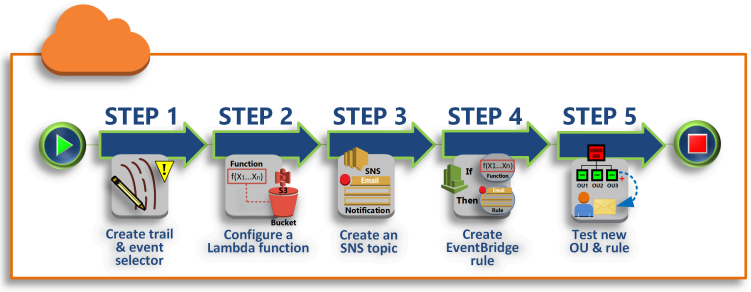
现在，您可以使用任何成员账户中的用户身份登录，并尝试执行各种 AWS 操作：

- 如果您以管理账户中用户的身份登录，则可以执行您的 IAM 权限策略允许的任何操作。SCP 不会影响管理账户中的任何用户或角色，不论账户位于哪个根或 OU 中。
- 如果您以 222222222222 账户中的用户身份登录，则可以执行允许列表允许的任何操作。AWS Organizations 拒绝尝试执行允许列表中未列出的任何服务的操作。此外，AWS Organizations 拒绝尝试执行 CloudTrail 配置操作之一。
- 如果您以 333333333333 账户中的用户身份登录，则可以执行允许列表允许且拒绝列表未阻止的任何操作。AWS Organizations 将拒绝尝试执行允许列表策略中未列出的任何操作，并拒绝尝试执行拒绝列表策略中列出的任何操作。此外，AWS Organizations 拒绝尝试执行 CloudTrail 配置操作之一。

教程：使用 Amazon EventBridge 监控对您的组织进行的重要更改

本教程将演示如何配置 Amazon EventBridge（之前称为 Amazon CloudWatch Events）来监控组织中的更改。首先，学会配置一条规则，当用户调用特定 AWS Organizations 操作时即触发该规则。然后，您可将 Amazon EventBridge 配置为在触发规则后运行 AWS Lambda 函数，并将 Amazon SNS 配置为发送一封电子邮件，其中包含有关该事件的详细信息。

下图演示了本教程的主要步骤。



步骤 1：配置跟踪和事件选择器

在 中创建称为跟踪AWS CloudTrail的日志。对其进行配置，捕获所有 API 调用。

步骤 2：配置 Lambda 函数

创建 AWS Lambda 函数，将事件的详细信息记录到 S3 存储桶中。

步骤 3：创建 Amazon SNS 主题，向订阅者发送电子邮件

创建一个 Amazon SNS 主题，向其订阅者发送电子邮件，然后自己订阅该主题。

步骤 4：创建 Amazon EventBridge 规则

创建一条规则，要求 Amazon EventBridge 将指定 API 调用的详细信息传递给 Lambda 函数，并发送给 SNS 主题的订阅用户。

步骤 5：测试您的 Amazon EventBridge 规则

运行某项监控操作，测试您的新规则。在本教程中，所监控的操作是创建组织部门 (OU)。您可以查看 Lambda 函数创建的日志条目，并查看 Amazon SNS 发送给订阅者的电子邮件。

> **提示**
>
> 您还可以将本教程用作配置类似操作的指南，如在账户创建完成时发送电子邮件通知。因为创建账户是异步操作，所以在默认情况下，在完成时不会通知您。有关在 AWS Organizations 中将 AWS CloudTrail 和 Amazon EventBridge 结合使用的更多信息，请参阅 AWS Organizations 中的日志记录和监控。

前提条件

本教程假定：

- 您可以从组织的管理账户中以 IAM 用户的身份登录 AWS Management Console。IAM 用户必须拥有权限，以在 CloudTrail 中创建和配置日志，在 Lambda 中创建和配置函数，在 Amazon SNS 中创建和配置主题，在 Amazon EventBridge 中创建和配置规则。有关授予权限的更多信息，请参阅《IAM 用户指南》中的访问管理，或参阅要配置访问权限的服务的指南。
- 您可以访问现有的 Amazon Simple Storage Service（Amazon S3）存储桶（或有权限创建存储桶），用于接收在第一步配置的 CloudTrail 日志。

> **Important**
>
> 目前，AWS Organizations 只在美国东部（弗吉尼亚北部）区域托管（尽管它面向全球提供）。要执行本教程中的步骤，您必须配置 AWS Management Console，才能使用该区域。

步骤 1：配置跟踪和事件选择器

在此步骤中，您登录管理账户并在 AWS CloudTrail 中配置日志（称为跟踪）。您还需配置跟踪的事件选择器，以捕获所有读/写 API 调用，这样 Amazon EventBridge 就有了可以触发的调用。

创建跟踪

1. 以组织管理账户的管理员身份登录AWS，然后通过 https://console.aws.amazon.com/cloudtrail/ 打开 CloudTrail 控制台。
2. 在控制台右上角的导航栏中，选择美国东部（弗吉尼亚北部）区域。如果您选择其他区域，AWS Organizations 不会在 Amazon EventBridge 配置设置中作为一个选项出现，CloudTrail 也不会捕获 AWS Organizations 的相关信息。
3. 在导航窗格中，选择 Trails（跟踪记录）。
4. 选择 Create trail (创建跟踪)。
5. 对于 Trail name (跟踪名称)，输入 **`My-Test-Trail`**。
6. 执行下列选项之一来指定 CloudTrail 将日志提交到的位置：

   - 如果您需要创建存储桶，请选择 Create new S3 bucket（创建新 S3 存储桶），然后在 Trail log bucket and folder（跟踪日志存储桶和文件夹）中输入新存储桶的名称。

     > **Note**
     >
     > S3 存储桶的名称必须是全球唯一的。

- 如果您已有一个存储桶，选择 Use existing S3 bucket（使用现有 S3 存储桶），然后从 S3 bucket（S3 存储桶）列表中选择存储桶名称。

7. 选择下一步。
8. 在 Choose log events（选择日志事件）页面的 Management events（管理事件）部分中，选择 Read（读取）和 Write（写入）。
9. 选择下一步。
10. 检查您的选择，然后选择 Create trail（创建跟踪）。

如果警报规则匹配传入的 API 调用，Amazon EventBridge 允许您选择多种不同的方式发送警报。本教程演示了两种方法：调用 Lambda 函数，该函数可记录 API 调用；向 Amazon SNS 主题发送信息，向该主题的订阅者发送电子邮件或短信。在接下来的两个步骤中，您将创建所需的组件：Lambda 函数和 Amazon SNS 主题。

步骤 2：配置 Lambda 函数

在本步骤中，您将创建记录 API 活动的 Lambda 函数，这些活动由您稍后配置的 Amazon EventBridge 规则发送给函数。

创建记录 Amazon EventBridge 事件的 Lambda 函数

1. 从 AWS Lambda 打开 https://console.aws.amazon.com/lambda/ 控制台。
2. 如果您是首次使用 Lambda，请在欢迎页面上选择 Get Started Now（立即开始使用）；否则，选择 Create function（创建函数）。
3. 在 Create function（创建函数）页面中，选择 Use a blueprint（使用蓝图）。
4. 从 Blueprints (蓝图) 搜索框中，为筛选条件输入 **`hello`**，然后选择 hello-world 蓝图。
5. 选择 Configure（配置）。
6. 在 Basic information (基本信息) 页面上，执行以下操作：

   a. 对于 Lambda 函数名称，在 Name (名称) 文本框中输入 **`LogOrganizationEvents`**。

   b. 对于 Role (角色)，选择 Create a new role with basic Lambda permissions (创建具有基本 Lambda 权限的新角色)。此角色授予您的 Lambda 函数访问所需数据的权限和写入输出日志的权限。

7. 编辑 Lambda 函数的代码，如以下示例所示。

```
console.log('Loading function');
```

```
exports.handler = async (event, context) => {
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1;  // Echo back the first key value
    // throw new Error('Something went wrong');
};
```

该示例代码使用 **LogOrganizationEvents** 标记字符串记录事件，后跟组成事件的 JSON 字符串。

8. 选择 Create function（创建函数）。

步骤 3：创建 Amazon SNS 主题，向订阅者发送电子邮件

在此步骤中，您将创建 Amazon SNS 主题，向订阅者发送电子邮件信息。请将该主题作为您稍后创建的 Amazon EventBridge 规则的“目标”。

创建 Amazon SNS 主题，向订阅者发送电子邮件

1. 从 https://console.aws.amazon.com/sns/v3/ 打开 Amazon SNS 控制台。
2. 在导航窗格中，选择 Topics (主题)。
3. 选择 Create new topic (创建新主题)。
   a. 对于 Topic name (主题名称)，输入 **OrganizationsCloudWatchTopic**。
   b. 对于 Display name (显示名称)，输入 **OrgsCWEvnt**。
   c. 选择 创建主题。
4. 现在，您可以创建该主题的订阅。选择您刚刚创建的主题的 ARN。
5. 选择创建订阅。
   a. 在 Create subscription (创建订阅) 页面上，为 Protocol (协议) 选择 Email (电子邮件)。
   b. 对于 Endpoint (终端节点)，输入您的电子邮件地址。
   c. 选择 Create subscription (创建订阅)。AWS 将向前一步中指定的电子邮件地址发送电子邮件。收到这封电子邮件后，选择电子邮件中的 Confirm subscription (确认订阅) 链接，验证您已成功接收到这封电子邮件。
   d. 返回控制台并刷新页面。Pending confirmation 消息消失，现已替换为有效的订阅 ID。

步骤 4：创建 Amazon EventBridge 规则

现在，您的账户中存在所需的 Lambda 函数，您可以创建 Amazon EventBridge 规则，在满足该规则的条件时调用该函数。

创建 EventBridge 规则

1. 在 https://console.aws.amazon.com/events/ 打开 Amazon EventBridge 控制台。
2. 您必须将控制台设置为美国东部（弗吉尼亚州北部）区域，否则有关 Organizations 的信息不可用。在控制台右上角的导航栏中，选择美国东部（弗吉尼亚北部）区域。
3. 有关创建规则的说明，请参阅 Amazon EventBridge 用户指南中的 Getting started with Amazon EventBridge（Amazon EventBridge 入门）。

步骤 5：测试您的 Amazon EventBridge 规则

在此步骤中，您将创建一个组织单元（OU），然后观察 Amazon EventBridge 规则，生成日志条目，并向您发送有关事件详细信息的电子邮件。

AWS Management Console

创建 OU

1. 打开 AWS Organizations 控制台的AWS 账户页。
2. 选择复选框

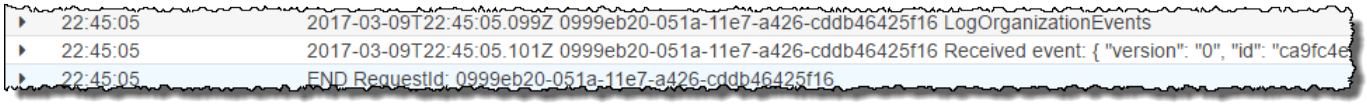
   ☑

   Root OU，选择 Actions (操作)，然后在 Organizational unit (组织部门) 下选择 Create new (新建)。
3. 对于 OU 的名称，输入 **`TestCWEOU`**，然后选择 Create organizational unit (创建组织部门)。

查看 EventBridge 日志条目

1. 从 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Logs (日志)。
3. 在 Log Groups (日志组) 下，选择与您的 Lambda 函数关联的组：/aws/lambda/LogOrganizationEvents。
4. 每个组包含一个或多个流，应该有一个今天的组。选择这个组。

5. 查看日志。您应该可以看到与以下内容类似的行：



6. 选择条目中间的行，查看收到事件的完整 JSON 文本。您可以在输出的 `requestParameters` 和 `responseElements` 部分查看 API 请求的所有详细信息。

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
    "version": "0",
    "id": "123456-EXAMPLE-GUID-123456",
    "detail-type": "AWS API Call via CloudTrail",
    "source": "aws.organizations",
    "account": "123456789012",
    "time": "2017-03-09T22:44:26Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.04",
        "userIdentity": {
            ...
        },
        "eventTime": "2017-03-09T22:44:26Z",
        "eventSource": "organizations.amazonaws.com",
        "eventName": "CreateOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.168.0.1",
        "userAgent": "AWS Organizations Console, aws-internal/3",
        "requestParameters": {
            "parentId": "r-exampleRootId",
            "name": "TestCWEOU"
        },
        "responseElements": {
            "organizationalUnit": {
                "name": "TestCWEOU",
                "id": "ou-exampleRootId-exampleOUId",
                "arn": "arn:aws:organizations::1234567789012:ou/o-exampleOrgId/ou-
exampleRootId-exampeOUId"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
        "eventID": "123456-EXAMPLE-GUID-123456",
```

```
        "eventType": "AwsApiCall"
    }
}
```

7. 检查您的电子邮件账户是否收到来自 OrgsCWEvnt 的邮件（您的 Amazon SNS 主题的显示名称）。电子邮件正文中包含与上一步所示的日志条目相同的 JSON 文本输出。

清理：删除您不再需要的资源

为避免产生费用，您应删除本教程要求您创建，而您也不希望保留的全部 AWS 资源。

清理您的 AWS 环境

1. 使用 CloudTrail 控制台 删除您通过步骤 1 创建的、名为 **My-Test-Trail** 的跟踪。
2. 如果您在步骤 1 中创建了 Amazon S3 存储桶，请使用 Amazon S3 控制台将其删除。
3. 使用 Lambda 控制台删除您通过步骤 2 创建的、名为 **LogOrganizationEvents** 的函数。
4. 使用 Amazon SNS 控制台删除您通过步骤 3 创建的、名为**OrganizationsCloudWatchTopic** 的 Amazon SNS 主题。
5. 使用 CloudWatch 控制台，删除您通过步骤 4 创建的名为 **OrgsMonitorRule** 的 EventBridge 规则。
6. 使用 Organizations 控制台删除您通过步骤 5 创建的、名为 **TestCWEOU** 的 OU。

就是这样。在本教程中，您配置了 EventBridge 来监控组织中的更改。您配置了一条规则，当用户调用特定 AWS Organizations 操作时即触发该规则。该规则运行 Lambda 函数来记录事件，并发送包含该事件详细信息的电子邮件。

多账户管理最佳实践

遵循以下建议，以帮助指导您在 AWS Organizations 中设置和管理多账户环境。

主题

在单个组织中管理账户

我们建议您创建单个组织，并在该组织中管理您的所有账户。组织是一种安全边界，可帮助确保您环境中的账户保持一致。您可以在一个组织中跨账户集中应用策略或服务级别配置。如果要在多账户环境中实现一致的策略、集中可见性和编程控制，则建议通过单个组织来实现。

为根用户使用强密码

我们建议您使用独有的强密码。多种密码管理器和强密码生成算法及工具都可帮助您实现这些目标。有关更多信息，请参阅更改 AWS 账户根用户 的密码。使用企业的信息安全政策来管理根用户密码的长期存储和访问。我们建议将密码存储在符合组织安全要求的密码管理器系统或同等系统中。为了避免创建循环依赖，请不要使用依赖于您使用受保护账户登录的AWS服务的工具来存储根用户密码。无论选择哪种方法，我们都建议您优先考虑弹性，此外还可考虑要求获得多个参与者的授权后才能访问密码保

管库，从而增强保护能力。对密码或其存储位置的任何访问都应有日志记录和监控。有关其他根用户密码建议，请参阅您的 AWS 账户 的根用户最佳实践。

记录使用根用户凭证的过程

记录重要流程的执行情况，以确保每个步骤中涉及的人员和使用的值均有记录。在密码管理方面，我们建议使用安全的加密密码管理器。记录可能出现的任何异常和意外事件也很重要。有关更多信息，请参阅《AWS Management Console 登录用户指南》中的 AWS 登录故障排除和《IAM 用户指南》中的需要根用户凭证的任务。

至少每季度测试并验证您是否有权继续访问根用户，以及联系电话号码是否正常。这有利于帮助企业确认相关流程运行正常，并确保您拥有根用户的访问权限。这还可以证明，负责根访问权限的人员了解他们必须执行哪些步骤，以确保整个过程的成功。为加快响应速度并提高成功率，必须确保参与流程的所有人员都准确了解必须进行哪些操作，以备访问之需。

为您的根用户凭证启用 MFA

我们建议您为 AWS 账户中的 AWS 账户 根用户和 IAM 用户启用多个多重身份验证（MFA）设备。这可以提高您的 AWS 账户的安全水准，简化对高权限用户（例如 AWS 账户根用户）的访问管理。为满足不同的客户需求，AWS 支持三种可用于 IAM 的 MFA 设备，包括 FIDO 安全密钥、虚拟身份验证器应用程序和基于时间的一次性密码（TOTP）硬件令牌。

每种类型的身份验证器具有略有不同的物理和安全特性，适合不同的应用场景。FIDO2 安全密钥可提供最佳的安全保障，可抵御网络钓鱼。任何形式的 MFA 都比纯密码身份验证具有更好的安全性，我们强烈建议您在账户中添加某种形式的 MFA。选择与您的安全和操作要求最相符的设备类型。

如果主身份验证器选择使用电池供电的设备，例如 TOTP 硬件令牌，请考虑注册一个不依赖电池的身份验证器，以作为备用机制。定期检查设备功能并在有效期届满之前进行更换，对于确保不间断的访问也至关重要。无论选择哪种类型的设备，我们都建议至少注册两台设备（IAM 支持每位用户最多八台 MFA 设备），以提高您抵御设备丢失或故障的能力。

根据贵组织的信息安全政策来保管 MFA 设备。我们建议您将 MFA 设备与关联的密码分开保管。这样可以确保需要具备不同的资源（人员、数据和工具）才能访问密码和 MFA 设备。这种隔离增加了额外的保护层，可防止未经授权的访问。我们还建议您记录和监控对 MFA 设备或其保管位置的任何访问。这有利于发现和处置任何未经授权的访问。

有关更多信息，请参阅《IAM 用户指南》中的使用多重身份验证 (MFA) 保护根用户。有关启用 MFA 的说明，请参阅 在 AWS 中使用多重身份验证（MFA） 以及 在 AWS 中为用户启用 MFA 设备。

应用控件来监视对根用户凭证的访问

对根用户凭证的访问应该是罕见事件。使用诸如 Amazon EventBridge 之类的工具创建提醒，以在发生管理账户根用户凭证的登录和使用事件时发送通知。此提醒应包括但不限于用于根用户本身的电子邮件地址。此提醒应当醒目，难以漏掉。有关示例，请参阅AWS 账户根用户活动的监控和通知。确保收到此类提醒的人员了解如何验证是否需要根用户访问权限，以及在其认为发生安全事件时如何上报。有关更多信息，请参阅 报告可疑电子邮件 或 漏洞报告。您还可以 联系 AWS 以获取帮助和其他指导。

确保更新联系电话号码

要找回 AWS 账户的访问权限，您必须拥有一个有效的联系电话号码并保持畅通，以便接收短信或电话。我们建议您使用专用的电话号码，以确保 AWS 可以就账户支持和恢复目的与您联系。您可以通过 AWS Management Console 或账户管理 API，来轻松查看和管理您的账户电话号码。

您可以通过多种方法来获得专用电话号码，以确保 AWS 可以与您联系。我们强烈建议您购买专用 SIM 卡和实体电话。妥善长期保管手机和 SIM 卡，确保电话号码始终可用于恢复账户。此外还应确保负责手机账单的团队了解该号码的重要性，即使该号码长期未使用。必须对您组织内的此电话号码保密，以加强保护。

在 AWS 联系信息控制台页面中记录该电话号码，并将其详情告知组织中必须了解该号码的具体团队。这种方法可帮助尽可能减少将电话号码转移到其他 SIM 卡相关的风险。根据您现有的信息安全策略存储电话。但是，请勿将电话存储在与其他相关凭证信息相同的位置。对电话或其保管位置的任何访问都应记录和监控。如果与账户关联的电话号码发生变化，请根据相关流程更新现有文档中记录的电话号码。

为根用户使用组电子邮件地址

使用由您的企业管理的电子邮件地址。使用会收到的邮件直接转发到一组用户的电子邮件地址。如果 AWS 必须联系账户的所有（例如，确认访问权限），则电子邮件将分发给多个当事方。这种方法有助于降低响应延迟的风险，即使个人在度假、生病或离开公司时也是如此。

根据业务目的而不是报告架构对工作负载进行分组

我们建议您利用面向工作负载的顶层 OU 来隔离生产工作负载环境和数据。您的 OU 应基于一组通用的控制措施，而不是基于贵公司的报告架构。除生产 OU 外，我们建议您定义一个或多个非生产 OU，其中包含用于开发和测试工作负载的账户和工作负载环境。有关其他指导意见，请参阅 整理面向工作负载的 OU。

使用多个账户来整理工作负载

AWS 账户为您的 AWS 资源提供了自然的安全、访问和计费边界。使用多个账户有很多好处，因为这样可以分配账户级别的限额和 API 请求速率限制，其他好处 详见此处。我们建议您使用多个 组织范围的基础账户，例如安全账户、日志记录账户和基础设施账户。对于工作负载账户，您应 利用不同的账户来隔离生产工作负载和测试/开发工作负载。

使用服务控制台或 API/CLI 操作在组织层面启用 AWS 服务

作为最佳实践，如需启用或禁用您想跨 AWS Organizations 集成的任何服务，我们建议使用该服务的控制台或等效的 API 操作/CLI 命令。使用这种方法，AWS 服务可以为您的组织执行所有需要的初始化步骤，例如在禁用服务时创建任何需要的资源以及清理资源。AWS Account Management 是唯一需要使用 AWS Organizations 控制台或 API 才能启用的服务。要查看与 AWS Organizations 集成的服务列表，请参阅 AWS 可以与之配合使用的服务 AWS Organizations。

使用计费工具跟踪成本并优化资源使用情况

管理组织时，您会收到一份包含组织中账户的所有费用的整合账单。如果需要访问成本可见性功能的业务用户，您可以在管理账户中提供一个角色，并为其提供查看账单和成本工具的受限只读权限。例如，您可以 创建权限集 来提供账单报告的访问权限，也可以使用 AWS Cost Explorer Service（一种用于查看一段时间内成本趋势的工具）以及 Amazon S3 Storage Lens 存储统计管理工具 和 AWS Compute Optimizer 等成本效率管理服务。

制定标记策略并在组织资源中强制使用标签

随着账户和工作负载的扩展，利用标签可以有效地帮助跟踪成本、控制访问权限和整理资源。对于标记命名策略，请遵循 为 AWS 资源添加标签 中的指导意见。除资源外，您还可以为组织的根目录、账户、OU 和策略创建标签。有关更多信息，请参阅 制定标记策略。

管理账户的最佳实践

请遵循以下建议，来帮助保护 AWS Organizations 中管理账户的安全。这些建议假定您还遵守仅将根用户用于真正需要它的任务的最佳实践。

主题

- 限制谁有权访问管理账户

- 检查并跟踪谁有访问权限
- 仅将管理账户用于需要管理账户的任务
- 避免将工作负载部署到组织的管理账户中
- 将责任委托给非管理账户以实现去中心化

限制谁有权访问管理账户

管理账户是所有上述管理任务的关键，例如账户管理、策略、与其他 AWS 服务的集成、整合账单等。因此，您应限定和限制管理账户的访问权限，仅允许那些需要相关权限以对组织进行更改的管理员用户使用。

检查并跟踪谁有访问权限

为确保您保持对管理账户的访问权限，请定期检查您企业中有权访问与管理账户关联的电子邮件地址、密码、MFA 和电话号码的人员。使您的审查与现有业务流程保持一致。每月或每季度对这些信息进行一次审查，以确认只有正确的人才能访问。确保恢复或重置对根用户凭证的访问权限的过程不依赖于任何特定个人来完成。所有流程都应能解决人员不可用的可能情况。

仅将管理账户用于需要管理账户的任务

我们建议您将管理账户及其用户和角色仅用于必须由该账户执行的任务。将您的所有 AWS 资源存储在组织中的其他 AWS 账户中，而非保存在管理账户中。将资源保留在其他账户中的一个重要原因是，Organizations 服务控制策略（SCP）无法限制管理账户中的任何用户或角色。将资源与管理账户分离还有助于您了解发票上的费用。

避免将工作负载部署到组织的管理账户中

组织的管理账户中可以执行特权操作，SCP 不适用于管理账户。因此，管理账户中包含的云资源和数据应仅限必须在管理账户中管理的云资源和数据。

将责任委托给非管理账户以实现去中心化

我们建议尽可能将责任和服务委托给非管理账户。为团队自己的账户提供无需访问管理账户，即可满足组织需求所需的权限。此外，您可以为支持此功能的服务注册多个委托管理员，例如用于在组织内共享软件的 AWS Service Catalog，或用于创作和部署堆栈的 AWS CloudFormation StackSets。

有关更多信息，请参阅 安全参考架构、使用多个账户整理 AWS环境 ，以及 AWS 可以与之配合使用的服务 AWS Organizations，以了解有关将成员账户注册为各种 AWS 服务的委托管理员的建议。有关设

置委托管理员的更多信息，请参阅 为 AWS Account Management 启用委托管理员账户 和 的委派管理员 AWS Organizations。

成员账户的最佳实践

请遵循以下建议，以帮助保护组织中成员账户的安全。这些建议假定您还遵守仅将根用户用于真正需要它的任务的最佳实践。

主题

- 定义账户名称和属性
- 高效扩展环境和使用账户
- 使用 SCP 限制成员账户中的根用户可以执行的操作

定义账户名称和属性

对于成员账户，请使用反映账户使用情况的命名结构和电子邮件地址。例如，Workloads+fooA+dev@domain.com 可用于 WorkloadsFooADev，Workloads+fooB+dev@domain.com 可用于 WorkloadsFooBDev。如果您为组织定义了自定义标签，我们建议您根据账户使用情况、成本中心、环境和项目，来为账户分配这些标签。这样可以更轻松地识别、整理和搜索账户。

高效扩展环境和使用账户

随着组织的不断扩展，在创建新账户之前，请确认满足类似需求的账户是否尚不存在，以避免不必要的重复。AWS 账户应基于常用的访问需求。如果您计划回收利用某些账户（例如沙盒账户或等效账户），我们建议您清理账户中不需要的资源或工作负载，但保存这些账户以备将来使用。

在注销账户之前，请注意账户注销限额限制。有关更多信息，请参阅的配额 AWS Organizations。考虑实施清理流程以回收利用账户，而不是尽可能注销账户和创建新账户。这样可以避免因运行的资源产生成本，以及避免达到 CloseAccount API 限制。

使用 SCP 限制成员账户中的根用户可以执行的操作

我们建议您在组织中创建服务控制策略（SCP）并将其附加到组织的根，以便将其应用于所有成员账户。有关更多信息，请参阅保护 Organizations 账户根用户凭证。

除必须在成员账户中执行的特定仅限根操作外，您可以拒绝所有根操作。例如，以下 SCP 会阻止任何成员账户中的根用户进行任何 AWS 服务 API 调用，但“更新配置错误的 S3 桶策略并拒绝所有主体的

访问权限”（需要根凭证的操作之一）除外。有关更多信息，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

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

    "Statement": [

        {

            "Effect": "Deny",

            "NotAction":[

            "s3:GetBucketPolicy",

            "s3:PutBucketPolicy",

            "s3:DeleteBucketPolicy"

                 ],

            "Resource": "*",

            "Condition": {
 "StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }

            }

        }

    ]
 }
```

在大多数情况下，任何管理任务都可以由成员账户中具有相关管理员权限的 AWS Identity and Access Management（IAM）角色执行。对于任何此类角色，都应使用适当的控件来限制、记录和监控其活动。

创建和管理组织

您可以使用 AWS Organizations 控制台或通过运行 AWS Command Line Interface（AWS CLI）命令或等效 AWS SDK API 操作来执行以下任务：

- 创建组织。使用您当前的账户作为管理账户创建组织。在您的组织内创建成员账户，并邀请其他账户加入组织。
- 启用组织中的所有功能。启用所有功能是使用 AWS Organizations 的首选方式。在创建组织时，您可以选择启用用于整合账单的所有或部分功能。启用所有功能是默认选择，它包括整合账单功能。

  在启用所有功能的情况下，您可以使用 AWS Organizations 中提供的高级账户管理功能，例如服务控制策略 (SCP)。SCP 提供对组织中所有账户的最大可用权限的集中控制，可帮助您确保您的账户遵循组织的访问控制指南。
- 查看有关组织的详细信息。查看有关您的组织、根、组织单元 (OU) 和账户的详细信息。
- 删除组织。当您不再需要某个组织时删除它。

> **Note**
>
> 此部分中的过程指定执行任务所需的最低权限。这些通常应用到 API 或对命令行工具的访问权。
> 在控制台中执行任务可能需要其他权限。例如，您可以将只读权限授予组织中的所有用户，然后授予允许所选用户执行特定任务的其他权限。

创建企业

您可以从使用AWS 账户作为管理账户开始来创建组织。创建组织时，您可以选择组织是支持所有功能（建议使用）还是只支持整合账单功能。

创建组织之后，您可以通过以下方式从管理账户中向您的组织添加账户：

- 创建可作为成员账户自动加入您的组织的其他AWS 账户。
- 验证您的电子邮件地址后，邀请现有AWS 账户作为会员账户加入您的组织。

创建组织

可通过以下两种方式创建组织：使用AWS Management Console或者通过使用 AWS CLI 或其中一个 SDK API。

> **最小权限**
>
> 要使用您当前的AWS 账户创建组织，您必须具有以下权限：
>
> - `organizations:CreateOrganization`
> - `iam:CreateServiceLinkedRole`
>
> 您可以将此权限限制为仅服务委托人 `organizations.amazonaws.com`。

AWS Management Console

创建 组织

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 默认情况下，组织在创建时已启用所有功能。但是，您可以选择以下步骤之一：

   - 要创建已启用所有功能的组织，请在介绍页面上选择 Create an organization (创建组织)。
   - 要创建仅具有整合账单功能的组织，请在介绍页面 Create an organization (创建组织) 中，选择 consolidated billing features (整合账单功能)，然后在确认对话框中，选择 Create an organization (创建组织)。

   如果您意外选择了错误的选项，您可以立即转到 Settings (设置) 页面，然后选择 Delete organization (删除组织) 并重新开始。
3. 组织已创建，并且会显示AWS 账户页面。唯一存在的账户是您的管理账户，它当前存储在根组织部门（OU）中。

   如果需要，Organizations 会自动向与管理账户关联的地址发送验证电子邮件。在您接收到验证电子邮件之前可能会有一段延迟。在 24 小时内验证您的电子邮件地址。有关更多信息，请参阅电子邮件地址验证。您可以在不验证管理账户电子邮件地址的情况下创建账户以添加到组织中。但是，要邀请现有账户，您必须先完成电子邮件验证。

> **Note**
>
> 如果此账户之前验证了其电子邮件地址，则当您使用该账户创建组织时，验证不会再次发生。

AWS CLI & AWS SDKs

创建 组织

您可以使用以下命令之一创建组织：

- AWS CLI：create-organization

  以下示例创建组织，并使当前已登录的AWS 账户成为组织的管理账户。

```
$ aws organizations create-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [  ...DEPRECATED - DO NOT USE ... ]
    }
}
```

> **Important**
>
> `AvailablePolicyTypes` 字段已弃用，并且不包含有关在组织中启用的策略的准确信息。要查看组织实际启用的策略类型的准确且完整的列表，请使用 `ListRoots` 命令，如以下部分的 AWS CLI 中所述。

- AWS SDK：CreateOrganization

现在，您可以按以下步骤向组织添加其他账户：

- 要创建自动属于AWS组织的AWS 账户，请参阅在组织中创建成员账户。
- 若要邀请现有账户加入您的组织，请参阅邀请一个 AWS 账户 人加入你的组织。

电子邮件地址验证

在创建组织后、邀请账户加入前，您必须验证与组织内的管理账户关联的电子邮件地址。

创建组织时，如果以前未验证管理账户，AWS会自动向指定的电子邮件地址发送验证电子邮件。在您接收到验证电子邮件之前可能会有一段延迟。

在 24 小时内，按照电子邮件中的说明验证您的电子邮件地址。

如果未在 24 小时内验证您的电子邮件地址，您可以重新发送验证请求，以便邀请其他AWS 账户加入您的组织。如果您没有收到验证电子邮件，请检查您的电子邮件地址是否正确，如有必要，请对其进行修改。

- 要查看与您的管理账户关联的电子邮件地址是什么，请参阅从管理账户查看组织的详细信息。
- 若要更改与管理账户关联的电子邮件地址，请参阅《AWS Billing 用户指南》中的管理AWS 账户。

AWS Management Console

若要重新发送验证请求

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 导航到 Settings (设置) 页面，然后选择 Send verification request (发送验证请求)。只有在未验证管理账户时才存在该选项。
3. 在 24 小时内验证您的电子邮件地址。

   验证您的电子邮件地址后，您可以邀请其他AWS 账户加入您的组织。有关更多信息，请参阅邀请一个 AWS 账户 人加入你的组织。

如果您更改管理账户的电子邮件地址，该账户的状态会恢复为“未验证电子邮件”，并且您必须为新的电子邮件地址完成验证过程。

> **Note**
>
> 如果您在更改管理账户的电子邮件地址之前邀请了账户加入组织，并且这些邀请尚未被接受，则在您验证管理账户的新电子邮件地址之前，无法接受这些邀请。使用上一步骤重新发送验证请求。通过回复电子邮件完成此过程后，受邀的账户可以接受邀请。

启用企业中的所有功能

AWS Organizations 有两个可用的功能集：

- 所有功能 – 此功能集是使用 AWS Organizations 的首选方式，并且它包括整合账单功能。在创建组织时，默认情况下将启用所有功能。在启用所有功能的情况下，您可以使用 AWS Organizations 中提供的高级账户管理功能，例如与支持的AWS服务的集成和组织管理策略。
- 整合账单功能 – 所有组织都支持此功能子集，这提供了可用于集中管理组织中的账户的基本管理工具。

如果仅创建具有整合账单功能的组织，则可以稍后启用所有功能。此页面描述启用所有功能的过程。

在启用所有功能之前

在从仅支持整合账单功能的组织更改为支持所有功能的组织之前，请注意以下几点：

- 当您开始启用所有功能的流程时，AWS Organizations 会向您邀请 加入组织的每个成员账户发送请求。每个受邀账户必须通过接受请求来批准启用所有功能。只有这样，您才可以完成在组织中启用所有功能的流程。如果某个账户拒绝请求，则必须从组织中删除该账户或重新发送请求。您必须接受请求，然后才能完成启用所有功能的过程。您使用 创建AWS Organizations 的账户无需获取请求，因为这些账户无需批准额外控制。
- 您可以在启用所有功能的同时继续邀请账户加入您的组织。邀请将通知受邀请账户的所有者是在仅启用整合账单功能的情况下加入组织，还是在启用所有功能的情况下加入组织。
  - 如果您在启用所有功能的流程中邀请一个账户，则邀请声明他们加入的组织已启用所有功能。如果在账户接受邀请之前取消启用所有功能的流程，则该邀请将被取消。您必须再次邀请账户成为仅使用整合账单功能的组织的成员。
  - 如果您邀请一个账户，但在开始启用所有功能的流程之前，该邀请未被接受，则该邀请将被取消，因为邀请声明该组织仅使用整合账单功能。您必须再次邀请账户成为已启用所有功能的组织的成员。
- 您还可以继续在组织中创建账户。该过程不受此更改的影响。

- AWS Organizations 还将验证每个成员账户是否都有一个名为 `AWSServiceRoleForOrganizations` 的服务相关角色。此角色在要启用所有功能的所有账户中都是必需的。如果您在受邀账户中删除了此角色，则接受“启用所有功能”邀请会重新创建此角色。如果您已删除使用 AWS Organizations 创建的账户中的此角色，则该账户会收到专门重新创建此角色的邀请。组织必须接受所有这些邀请才能完成启用所有功能的过程。
- 由于启用所有功能可让您使用 SCP，因此，请确保账户管理员了解将 SCP 附加到组织、组织单位或账户的效果。SCP 可以限制用户甚至是管理员能够在受影响的账户中执行的操作。例如，管理账户可以应用 SCP，防止成员账户退出组织。
- 管理账户不受任何 SCP 的影响。您无法通过应用 SCP 来限制管理账户中的用户和角色能够执行的操作。SCP 仅影响成员账户。
- 从整合账单功能迁移到所有功能的过程是单向的。您无法将已启用了所有功能的组织切换回仅启用整合账单功能。
- （不推荐）如果您的组织仅启用了整合账单功能，则成员账户管理员可以选择删除名为 `AWSServiceRoleForOrganizations` 的服务相关角色。如果稍后选择在组织中启用所有功能，则此角色是必需的，并且将在所有账户中作为接受“启用所有功能”邀请的一部分重新创建。有关 AWS Organizations 如何使用此角色的更多信息，请参阅AWS Organizations 和服务相关角色。

开始启用所有功能的流程

当登录到组织的管理账户时，您可以开始启用所有功能的流程。为此，请完成以下步骤。

> **最小权限**
>
> 要启用组织中的所有功能，您必须具有以下权限：
>
> - `organizations:EnableAllFeatures`
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要

AWS Management Console

邀请受邀成员账户同意启用组织中的所有功能

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在设置页面上，选择开始流程以启用所有功能。

3. 在启用所有功能页面上，确认您了解在选择开始流程以启用所有功能进行切换之后便无法再恢复到仅整合账单功能。

   AWS Organizations 将请求发送到组织中的每个受邀 (而非已创建) 账户，要求批准请求以在组织中启用所有功能。如果您有使用 AWS Organizations 创建的任何账户且成员账户管理员删除了名为 `AWSServiceRoleForOrganizations` 的服务相关角色，则 AWS Organizations 会向该账户发送重新创建该角色的请求。

   控制台会显示被邀请账户的 Request approval status (请求审批状态) 列表。

   > **Tip**
   >
   > 若要稍后返回此页面，请打开 Settings (设置) 页面，并在 Request sent date (请求发送日期) 部分中选择 View status (查看状态)。

4. Enable all features (启用所有功能) 页面显示了组织中各账户的当前请求状态。同意该请求的账户将显示状态 ACCEPTED (已接受)。尚未同意的账户显示状态 OPEN (待接受)。

AWS CLI & AWS SDKs

邀请受邀成员账户同意启用组织中的所有功能

可以使用以下命令之一在组织中启用所有功能：

- AWS CLI：enable-all-features

  以下命令将开始启用组织中所有功能的流程。

```
$ aws organizations enable-all-features
{
    "Handshake": {
        "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "REQUESTED",
```

```
        "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

输出显示受邀成员账户必须同意的握手详细信息。

- AWS SDK：EnableAllFeatures

> **注意**
>
> - 向成员账户发送请求之后，将开始 90 天倒计时。所有账户必须在该时段内批准请求，否则请求将过期。如果请求过期，所有与此尝试相关的请求将被取消，您必须从步骤 2 从头开始。
> - 请求启用所有功能后，将取消所有未接受的现有账户邀请。
> - 在所有功能迁移期间，您仍然可以发起新账户邀请并创建新账户。

组织中的所有受邀账户批准请求之后，您可以完成流程并启用所有功能。如果您的组织中没有任何受邀成员账户，也可以立即完成流程。要最终完成该过程，请继续根据完成流程以启用所有功能中的内容操作。

批准启用所有功能或重新创建服务相关角色的请求

在登录到组织的受邀成员账户之一后，您可以从管理账户批准请求。如果您的账户最初受邀加入组织，则该邀请将启用所有功能并隐式包含对重新创建 `AWSServiceRoleForOrganizations` 角色的批准（如果需要）。如果您的账户是使用 AWS Organizations 创建的且您删除了 `AWSServiceRoleForOrganizations` 服务相关角色，则您将仅收到重新创建该角色的邀请。为此，请完成以下步骤。

Important

如果启用所有功能，组织中的管理账户可以对您的成员账户应用基于策略的控制。这些控制可以限制用户、甚至限制您作为管理员可以在账户中执行的操作。此类限制可能会阻止您的账户退出组织。

最小权限

要批准为成员账户启用所有功能的请求，您必须拥有以下权限：

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
- `organizations:ListHandshakesForAccount` – 仅当使用 Organizations 控制台时才需要
- `iam:CreateServiceLinkedRole` – 仅当在成员账户中必须重新创建 `AWSServiceRoleForOrganizations` 角色时需要

AWS Management Console

同意在组织中启用所有功能的请求

1. 在 AWS Organizations 控制台处登录到 AWS Organizations 控制台。您必须以 IAM 用户身份登录，担任 IAM 角色；或以组织成员账户中的根用户身份登录（不推荐）。
2. 阅读以了解接受在组织中启用所有功能的请求对您的账户意味着什么，然后选择 Accept。在组织中的所有账户接受请求并且管理账户管理员完成流程之前，此页面一直将该流程显示为未完成。

AWS CLI & AWS SDKs

同意在组织中启用所有功能的请求

要同意请求，您必须接受与 `"Action": "APPROVE_ALL_FEATURES"` 握手。

- AWS CLI:
  - accept-handshake

- list-handshakes-for-account

以下示例演示如何列出可用于您账户的握手。输出的第四行中的 "Id" 的值是下一个命令所需的值。

```
$ aws organizations list-handshakes-for-account
{
    "Handshakes": [
        {
            "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "111122223333",
                    "Type": "ACCOUNT"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
            "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
            "Action": "APPROVE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "c440da758cab44068cdafc812EXAMPLE",
                    "Type": "PARENT_HANDSHAKE"
                },
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                },
                {
                    "Value": "111122223333",
                    "Type": "ACCOUNT"
                }
            ]
        }
    ]
```

```
}
```

以下示例使用上一个命令中的握手 ID 来接受该握手。

```
$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
    "Handshake": {
        "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "111122223333",
                "Type": "ACCOUNT"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
        "Action": "APPROVE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "c440da758cab44068cdafc812EXAMPLE",
                "Type": "PARENT_HANDSHAKE"
            },
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            },
            {
                "Value": "111122223333",
                "Type": "ACCOUNT"
            }
        ]
    }
}
```

- AWS SDK：

- list-handshakes-for-account
- AcceptHandshake

完成流程以启用所有功能

所有受邀成员账户必须批准启用所有功能的请求。如果组织中没有受邀成员账户，Enable all features progress 页面将使用绿色横幅指示您可以完成流程。

> 最小权限
>
> 要完成为组织启用所有功能的流程，您必须拥有以下权限：
>
> - `organizations:AcceptHandshake`
> - `organizations:ListHandshakesForOrganization`
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要

AWS Management Console

完成流程以启用所有功能

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Settings (设置) 页面上，如果所有受邀账户接受启用所有功能的请求，则页面顶部将显示一个绿色框以通知您。在绿色框中，选择 Go to finalize (转到最终确定)。
3. 在 Enable all features (启用所有功能) 页面上，选择 Finalize (最终确定)，然后在确认对话框中再次选择 Finalize (最终确定)。
4. 组织现已启用所有功能。

AWS CLI & AWS SDKs

完成流程以启用所有功能

要完成该流程，您必须使用 `"Action": "ENABLE_ALL_FEATURES"` 接受握手过程。

- AWS CLI:
  - list-handshakes-for-organization

- accept-handshake

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
            "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
            "Action": "ENABLE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                }
            ]
        }
    ]
}
```

以下示例演示如何列出可用于组织的握手。输出的第四行中的 "Id" 的值是下一个命令所需的值。

```
$ aws organizations accept-handshake \
    --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
    "Handshake": {
        "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
```

```
                "Type": "ORGANIZATION"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
        "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

- AWS SDK：
  - AcceptHandshake
  - AcceptHandshake

后续步骤：

- 启用您要使用的策略类型。在此之后，您可以附加策略，管理组织中的账户。有关更多信息，请参阅在中管理策略 AWS Organizations。
- 启用与支持的服务的集成 有关更多信息，请参阅将 AWS Organizations 与其它 AWS 产品结合使用。

查看有关您的组织的详细信息

您可以执行以下任务来查看组织元素的详细信息。

主题

- 从管理账户查看组织的详细信息
- 查看根容器的详细信息
- 查看 OU 的详细信息
- 查看账户的详细信息
- 查看策略的详细信息

从管理账户查看组织的详细信息

在 AWS Organizations 控制台中登录组织的管理账户时，您可以查看组织的详细信息。

> **最小权限**
>
> 要查看组织的详细信息，您必须拥有以下权限：
>
> - `organizations:DescribeOrganization`

AWS Management Console

查看组织的详细信息

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 导航到 Settings (设置) 页面。此页面显示组织的详细信息，包括组织 ID 以及分配给组织管理账户的账户名称和电子邮件地址。

AWS CLI & AWS SDKs

查看组织的详细信息

您可以使用以下命令之一查看组织的详细信息：

- AWS CLI：describe-organization

  以下示例显示了此命令输出中包含的信息。

```
$ aws organizations describe-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
```

```
    }
}
```

> **Important**
>
> `AvailablePolicyTypes` 字段已弃用，并且不包含有关在组织中启用的策略的准确信息。要查看组织实际启用的策略类型的准确且完整的列表，请使用 `ListRoots` 命令，如以下部分的 AWS CLI 中所述。

- AWS SDK：DescribeOrganization

查看根容器的详细信息

在 AWS Organizations 控制台中登录组织的管理账户时，您可以查看根容器的详细信息。

> **最小权限**
>
> 要查看根的详细信息，您必须拥有以下权限：
>
> - `organizations:DescribeOrganization` (仅限控制台)
> - `organizations:ListRoots`

根是组织部门（OU）层次结构中最顶层的容器，通常表现为 OU。但是，由于容器位于层次结构最顶部，因此对根的更改会影响组织中的所有其他 OU 和每个AWS 账户。

AWS Management Console

查看根的详细信息

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 导航到AWS 账户页面，然后选择 Root OU（其名称，而不是单选按钮）。
3. Root (根) 详细信息页面上将显示根的详细信息。

AWS CLI & AWS SDKs

查看根的详细信息

您可以使用以下命令之一查看根的详细信息：

- AWS CLI：list-roots

  以下示例说明如何检索根的详细信息，包括组织中当前启用的策略类型：

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": [
                {
                    "Type": "BACKUP_POLICY",
                    "Status": "ENABLED"
                }
            ]
        }
    ]
}
```

- AWS SDK：ListRoots

查看 OU 的详细信息

在 AWS Organizations 控制台中登录组织的管理账户时，您可以查看组织中 OU 的详细信息。

> **最小权限**
>
> 要查看组织单元 (OU) 的详细信息，您必须拥有以下权限：
>
> - `organizations:DescribeOrganizationalUnit`
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
> - `organizations:ListOrganizationsUnitsForParent` – 仅当使用 Organizations 控制台时才需要
> - `organizations:ListRoots` – 仅当使用 Organizations 控制台时才需要

AWS Management Console

查看 OU 的详细信息

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，选择要检查的 OU（而不是其单选按钮）的名称。如果您要查看的 OU 是其他 OU 的子级，则选择其父级 OU 旁边的三角形图标以展开 OU，并查看层次结构的下一级。重复操作，直到找到所需的 OU。

   Organizational unit details (组织部门详细信息) 框显示有关 OU 的信息。

AWS CLI & AWS SDKs

查看 OU 的详细信息

您可以使用以下命令查看 OU 的详细信息：

- AWS CLI、AWS SDK：
  - list-roots
  - list-children
  - describe-organizational-unit

以下示例说明如何使用 AWS CLI 查找 OU 的 ID。使用 `list-roots` 命令开始遍历层次结构，然后在根上执行 `list-children`，并在其每个子级上迭代执行，直到找到所需的子级，从而找到 OU ID。

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type
 ORGANIZATIONAL_UNIT
```

```
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
```

获得 OU ID 后，以下示例说明如何检索有关 OU 的详细信息。

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-
f6g7h111
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h111",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
        "Name": "Production-Apps"
    }
}
```

- AWS SDK：
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

查看账户的详细信息

在 AWS Organizations 控制台中登录组织的管理账户时，您可以查看账户的详细信息。

> **最小权限**
>
> 要查看AWS 账户的详细信息，您必须拥有以下权限：
>
> - `organizations:DescribeAccount`
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
> - `organizations:ListAccounts` – 仅当使用 Organizations 控制台时才需要

AWS Management Console

查看AWS 账户的详细信息

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 导航到AWS 账户页面，然后选择要检查的账户名称（而不是单选按钮）。如果您需要的账户是 OU 的子级，则可能需要选择 OU 旁边的三角形图标  ，以展开 OU 并查看其子级。重复操作，直到找到账户。

   Account details (账户详细信息) 框显示有关该账户的信息。

AWS CLI & AWS SDKs

查看AWS 账户的详细信息

您可以使用以下命令查看账户的详细信息：

- AWS CLI:
  - list-accounts – 列出组织中全部账户的详细信息
  - describe-account – 仅列出指定账户的详细信息

  这两个命令为响应中包含的每个账户返回相同的详细信息。

  以下示例说明如何检索有关指定账户的详细信息。

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
        "Status": "ACTIVE",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00"
    }
```

```
}
```

- AWS SDK：
  - ListAccounts
  - DescribeAccount

查看策略的详细信息

在 AWS Organizations 控制台中登录组织的管理账户时，您可以查看策略的详细信息。

> **最小权限**
>
> 要查看策略的详细信息，您必须拥有以下权限：
>
> - `organizations:DescribePolicy`
> - `organizations:ListPolicies`

AWS Management Console

查看策略的详细信息

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 执行下列操作之一：
   - 导航到 Policies (策略) 页面上，然后为要检查的策略选择策略类型。
   - 导航到AWS 账户页面，然后导航到策略附加到的 OU 或账户。最后，选择 Policies (策略) 选项卡查看附加策略的列表。
3. 选择策略的名称（而不是单选按钮）。

   在策略的 Details (详细信息) 页面上，您可以查看有关策略的所有信息，包括 JSON 策略文本，以及该策略附加到的 OU 和账户的列表。

AWS CLI & AWS SDKs

查看策略的详细信息

您可以使用以下命令之一查看策略的详细信息：

- AWS CLI:
  - list-policies
  - describe-policy – 仅列出指定策略的详细信息

  以下示例说明如何查找要检查的策略的策略 ID。您必须指定策略类型，并且命令仅返回该类型的所有策略。

```
$ aws organizations list-policies --filter BACKUP_POLICY
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        }
    ]
}
```

  响应包括除 JSON 策略文档之外的所有详细信息。

  以下示例说明如何仅检索指定策略（包括 JSON 策略文档）的详细信息。

```
$ aws organizations describe-policy --policy-id p-i9j8k7l6m5
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"plans\":{\"My-Backup-Plan\":{\"regions\":{\"@@assign\":
[\"us-west-2\"]},\"rules\":{\"My-Backup-Rule\"
```

```
                    :{\"target_backup_vault_name\":{\"@@assign\":\"My-Primary-
Backup-Vault\"}}},\"selections\":{\"tags\":{
                    \"My-Backup-Plan-Resource-Assignment\":{\"iam_role_arn\":
{\"@@assign\":\"arn:aws:iam::$account:role/
                    My-Backup-Role\"},\"tag_key\":{\"@@assign\":\"Stage\"},
\"tag_value\":{\"@@assign\":[\"Production\"]}}}}}}}"
    ]
}
```

- AWS SDK：
  - ListPolicies
  - DescribePolicy

删除组织

当您不再需要组织时，可将其删除。删除组织不会导致管理账户被注销，而只是将管理账户从组织中移除，然后再删除组织本身。以前的管理账户将成为不再由 AWS Organizations 管理的独立 AWS 账户。然后，您有三个选项：可以继续使用它作为独立账户、使用它创建不同的组织，也可以接受其他组织的邀请，将该账户作为成员账户添加到该组织。

> **Important**
>
> - 如果您删除组织，则无法恢复它。如果您在组织内创建了任何策略，则也将删除这些策略，并且将不能恢复。
> - 必须先删除组织中的所有成员账户，然后才能删除组织。如果您使用 AWS Organizations 创建了一些成员账户，则可能无法删除这些账户。您只能删除拥有作为独立AWS 账户运行所需的全部信息的成员账户。有关如何提供这些信息和删除账户的更多信息，请参阅成员账户离开组织。
> - 如果您在将某个成员账户从组织中删除之前关闭该账户，则该账户会在一段时间内进入“暂停”状态，并且在最终关闭之前，您无法将其从组织中删除。这最多可能需要 90 天，并且在此之前可能会阻止您删除组织，直到所有成员账户完全关闭。

在通过删除组织来从组织中移除管理账户时，该账户会在以下方面受到影响：

- 该账户只负责支付自己的费用，不再负责支付其他任何账户产生的费用。

- 与其他服务的集成可能会被禁用。例如，AWS IAM Identity Center 需要组织才能运行，因此，如果您从支持 IAM Identity Center 的组织中移除账户，则此账户中的用户将无法再使用该服务。

组织的管理账户从来不受服务控制策略（SCP）的影响，所以当 SCP 不再可用后，权限没有任何更改。

主题

删除组织

按照以下过程删除组织，这会将以前的管理账户恢复为不再由 AWS Organizations 管理的独立 AWS 账户。

> **最小权限**
>
> 要删除组织，您必须以管理账户中的用户或角色身份登录，并且您必须拥有以下权限：
>
> - `organizations:DeleteOrganization`
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要

AWS Management Console

删除组织

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 您必须先移除组织中的所有账户，然后才能删除组织。有关更多信息，请参阅从组织中删除成员账户。
3. 导航到 Settings (设置) 页面，然后选择 Delete organization (删除组织)。
4. 在 Delete organization (删除组织) 确认对话框中，输入显示在文本框上方行中的组织 ID。然后，选择 Delete organization (删除组织)。

> **Important**
>
> 此操作不会导致管理账户被注销，但会将其恢复为独立的 AWS 账户。要注销账户，请按照 关闭组织中的成员账户 中的步骤操作。

AWS CLI & AWS SDKs

删除组织

使用以下命令之一删除组织：

- AWS CLI：delete-organization

  以下示例将删除使用其凭证的AWS 账户作为管理账户的组织。

  ```
  $ aws organizations delete-organization
  ```

  如果成功，此命令不会产生任何输出。
- AWS SDK：DeleteOrganization

管理组织中的 AWS 账户

组织是您共同管理的AWS 账户的集合。您可以执行以下任务来管理属于组织的账户：

- 查看您组织中账户的详细信息。您可以查看该账户的唯一 ID 号、其 Amazon Resource Name（ARN）以及向其附加的策略。
- 导出组织中的所有 AWS 账户列表。您可以下载一个包含组织内每个账户的账户详细信息的 .csv 文件。
- 邀请现有AWS 账户加入您的组织。创建邀请、管理您已创建的邀请以及接受或拒绝邀请。
- 创建AWS 账户作为您组织的一部分。创建和访问自动成为您组织一部分的AWS 账户。
- 更新您组织中的备用联系人。更新组织中您的 AWS 账户 的备用联系人。
- 从您的组织中删除AWS 账户。作为管理账户中的管理员，从组织中删除您不再希望管理的成员账户。作为成员账户的管理员，从其组织中删除您的账户。如果管理账户已将一个策略附加到您的成员账户，则您可能无法删除您的账户。
- 删除（或关闭）AWS 账户。您可以关闭不再使用的AWS 账户，以免产生任何使用费或应计费用。

加入组织的影响

- 对加入组织的 AWS 账户有什么影响？
- 对您在组织中创建的 AWS 账户有什么影响？

对加入组织的AWS 账户的影响？

如果您邀请一个AWS 账户加入组织，该账户的拥有者接受邀请后，AWS Organizations 将自动对新的成员账户进行如下更改：

- AWS Organizations 创建名为 `AWSServiceRoleForOrganizations` 的服务相关角色。如果您的组织支持所有功能，该账户必须具有此角色。如果组织仅支持整合账单功能集，您可以删除该角色。如果您删除该角色，然后在组织中启用所有功能，则 AWS Organizations 将为该账户重新创建该角色。
- 您可能会具备附加到组织根或包含账户的 OU 的各种策略。如果是这样，这些策略将立即应用到受邀账户中的所有用户和角色。
- 您可以为组织的其他AWS服务启用服务信任。在您这样做时，该可信服务可以在组织的任何成员账户（包括受邀账户）中创建服务相关角色或执行操作。

> **Note**
>
> 对于受邀成员账户，AWS Organizations不会自动创建 IAM 角色OrganizationAccountAccessRole。此角色授予管理账户中的用户对成员账户的管理访问权限。如果您希望对受邀账户启用该级别的管理控制权，可以手动将该角色添加到受邀账户。有关更多信息，请参阅 OrganizationAccountAccessRole 在受邀成员账户中创建。

您可以邀请账户加入仅启用整合账单功能的组织。如果您以后希望为组织启用所有功能，则受邀账户必须批准更改。

对您在组织中创建的AWS 账户的影响？

如果您在组织中创建一个AWS 账户，AWS Organizations 将自动对新成员账户进行如下更改：

- AWS Organizations 创建名为 `AWSServiceRoleForOrganizations` 的服务相关角色。如果您的组织支持所有功能，该账户必须具有此角色。如果组织仅支持整合账单功能集，您可以删除该角色。如果您删除该角色，然后在组织中启用所有功能，则 AWS Organizations 将为该账户重新创建该角色。
- AWS Organizations创建 IAM 角色OrganizationAccountAccessRole。此角色授予管理账户对新成员账户的访问权限。虽然这个角色可以被删除，但我们建议您不要删除它，以便它可用作恢复选项。
- 如果您在 OU 树的根级别附加了策略，这些策略会立即应用于新建账户中的所有用户和角色。默认情况下，新账户会添加到根 OU。
- 如果您为组织启用了对其他 AWS 服务的服务信任，则该可信服务可以在组织中的任何成员账户（包括您创建的账户）中创建服务相关角色或执行操作。

邀请一个 AWS 账户 人加入你的组织

创建组织并确认自己拥有与管理账户关联的电子邮件地址后，您可以邀请现有人员 AWS 账户 加入您的组织。

当您邀请账户时， AWS Organizations 会向账户所有者发送邀请，由其决定是接受还是拒绝邀请。您可以使用 AWS Organizations 控制台发起和管理您向其他账户发送的邀请。您只能从组织的管理账户发送邀请到其他账户。

> **Note**
>
> 所有账户的账单历史记录和报告都保存在组织中的付款人账户中。在将账户移动到新的组织之前，请下载要保留的任何成员账户的任何账单和报告历史记录。这可能包括成本和使用情况报告、详细账单报告或 Cost Explorer 服务生成的报告。

如果您是的管理员 AWS 账户，也可以接受或拒绝来自组织的邀请。如果接受，您的账户将成为该组织的成员之一。您的账户只能加入一个组织，因此，如果您收到多个加入邀请，则只能接受一个。

当账户接受加入组织的邀请时，该组织的管理账户将承担新成员账户累积的所有费用。成员账户附加的付款方式不再使用。相反，附加到组织管理账户的付款方式支付成员账户应计的所有费用。

当受邀账户加入您的组织，并且您的组织处于 “所有功能” 模式时，该管理账户将拥有对受邀成员账户的完全管理访问权限和控制权。但是，与已创建的账户不同，`OrganizationAccountAccessRole`IAM 角色不会在拥有管理账户代入权限的成员账户中自动创建。要在受邀账户成为成员后创建和配置此功能，请按照以下步骤操作 OrganizationAccountAccessRole 在受邀成员账户中创建。

> **Note**
>
> 当您在组织中创建账户而不是邀请现有账户加入时， AWS Organizations 会自动创建一个 IAM 角色（`OrganizationAccountAccessRole`默认命名），您可以使用该角色向管理账户中的用户授予对已创建账户的管理员访问权限。

AWS Organizations 确实会在受邀成员账户中自动创建与服务相关的角色，以支持与其他 AWS 服务 AWS Organizations 之间的集成。有关更多信息，请参阅 AWS Organizations 和服务相关角色。

有关每天可以发送的邀请数，请参阅最大值和最小值。已接受的邀请不计入此配额。一旦某个邀请被接受，您就可以发送另一个同一天的邀请。每个邀请必须在 15 天内回复，否则将过期。

向账户发送的邀请也计入组织的账户配额。如果受邀账户拒绝邀请、管理账户取消邀请或邀请过期，则还原此计数。

要创建自动属于组织的账户，请参阅在组织中创建成员账户。

Important

由于账单限制，您 AWS 账户 只能邀请同一 AWS 卖家（ AWS 印度为例），并且只能与管理账户进行 AWS 分区。

- 如果贵组织的管理账户是由亚马逊 Web Services India Private Limited（“AWS 印度”）（前身为亚马逊互联网服务私人有限公司）创建的，则组织中的所有账户都必须与管理账户来自同一个登记在册的卖家。例如，作为印度的 AWS 卖家，您只能邀请其他 AWS 印度账户加入您的组织。您不能合并 AWS 印度账户或任何其他 AWS 卖家的账户。
- 组织中的所有账户都必须与管理账户来自同一个 AWS 分区。商业 AWS 区域 分区中的账户不能位于拥有来自中国区域分区的账户或区域分区的账户的 AWS GovCloud (US) 组织中。

向 AWS 账户发送邀请

若要邀请账户加入您的组织，必须首先验证您与管理账户关联的电子邮件地址。有关更多信息，请参阅电子邮件地址验证。验证电子邮件地址后，请完成以下步骤来邀请账户加入您的组织。

最小权限

AWS 账户 要邀请加入您的组织，您必须具有以下权限：

- `organizations:DescribeOrganization` (仅限控制台)
- `organizations:InviteAccountToOrganization`

AWS Management Console

邀请其他账户加入组织

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 如果您已经使用验证了电子邮件地址 AWS，请跳过此步骤。

   如果您的电子邮件地址还未验证，请在创建组织后的 24 小时内按照验证电子邮件中的说明进行验证。在您接收到验证电子邮件消息之前可能会有一段延迟。未完成电子邮件地址验证前，您无法邀请其他账户加入您的组织。
3. 导航到AWS 账户页面，然后选择 Add an AWS account (添加亚马逊云科技账户)。

4. 在 Add an AWS 账户(添加亚马逊云科技账户) 页面上，选择 Invite an existing AWS account (邀请现有亚马逊云科技账户)。
5. 在邀请现有 AWS页面上，在要邀请的电子邮件地址或账户 ID 中，输入与 AWS 账户 要邀请的账户关联的电子邮件地址或其账户 ID 号。
6. （可选）对于 Message to include in the invitation email message (要包含在邀请电子邮件中的消息)，输入您要包括在发送受邀请账户拥有者的电子邮件邀请中的任意文本。
7. （可选）在 Add tags (添加标签) 部分中，指定在账户管理员接受邀请后自动应用到账户的一个或多个标签。为此，请选择 Add tag (添加标签)，然后输入键和可选值。将值留空，设置为空字符串；它并非 `null`。您最多可以将 50 个标签附加到 AWS 账户。
8. 选择 Send invitation (发送邀请)。

> **Important**
>
> 如果您收到一条消息，它指示您超出了组织的账户配额或因组织仍在初始化而无法添加账户，请联系 AWS Support。

9. 控制台会将您重定向到 Invitations (邀请) 页面，您可以在此查看所有待接受和已接受的邀请。您刚刚创建的邀请将显示在列表的顶部，其状态设置为 OPEN。

   AWS Organizations 向您邀请加入该组织的账户所有者的电子邮件地址发送邀请。此电子邮件包含指向 AWS Organizations 控制台的链接，账户所有者可以在其中查看详细信息并选择接受或拒绝邀请。或者，受邀账户的所有者可以绕过电子邮件，直接进入 AWS Organizations 控制台，查看邀请，然后接受或拒绝邀请。

   对此账户的邀请立即计入组织的最大账户数； AWS Organizations 不会等待账户接受邀请。如果受邀账户拒绝，则管理账户会取消邀请。如果受邀账户在指定的时间段内未做出响应，则邀请过期。在任一情况下，邀请均不再计入您的配额。

AWS CLI & AWS SDKs

邀请其他账户加入组织

您可以使用以下命令之一来邀请其他账户加入您的组织：

- AWS CLI: invite-account-to-organization

```
$ aws organizations invite-account-to-organization \
    --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
```

```
    --notes "This is a request for Juan's account to join Bill's organization."
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                 "Type": "ORGANIZATION"
            },
            {
                 "Id": "juan@example.com",
                 "Type": "EMAIL"
            }
        ],
        "RequestedTimestamp": 1481656459.257,
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                         "Type": "MASTER_NAME",
                         "Value": "Management Account"
                    },
                    {
                         "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "FULL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "OPEN"
```

```
    }
}
```

- AWS 软件开发工具包：InviteAccountToOrganization

管理组织的待处理邀请

登录到管理账户后，您可以查看组织中的所有关联 AWS 账户 并取消任何待处理（未结）邀请。为此，请完成以下步骤。

> **最小权限**
>
> 要管理组织的待处理邀请，您必须拥有以下权限：
>
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
> - `organizations:ListHandshakesForOrganization`
> - `organizations:CancelHandshake`

AWS Management Console

查看或取消从您的组织发送到其他账户的邀请

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 导航到 Invitations (邀请) 页面。

   此页面显示从您的组织发送的所有邀请及其当前状态。

   > **Note**
   >
   > 已接受、已取消和已拒绝的邀请将继续在列表中显示 30 天。之后，这些邀请将被删除，不再在列表中显示。

3. 选择要取消的邀请旁边的单选按钮

   然后选择 Cancel invitation (取消邀请)。如果单选按钮呈灰色，则无法取消该邀请。

   邀请的状态将从 Open (待接受) 更改为 Canceled (已取消)。

AWS 向账户所有者发送一封电子邮件，说明您取消了邀请。除非您发送新邀请，否则账户无法再加入组织。

AWS CLI & AWS SDKs

查看或取消从您的组织发送到其他账户的邀请

您可以使用以下命令来查看或取消邀请：

- AWS CLI: list-handshakes-for-organization，取消握手
- 以下示例显示了此组织向其他账户发送的邀请。

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Action": "INVITE",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1482952459.257,
            "Id": "h-examplehandshakeid111",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "juan@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1481656459.257,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type": "MASTER_EMAIL",
                            "Value": "bill@amazon.com"
                        },
                        {
                            "Type": "MASTER_NAME",
                            "Value": "Management Account"
```

```
                        },
                        {
                            "Type": "ORGANIZATION_FEATURE_SET",
                            "Value": "FULL"
                        }
                    ],
                    "Type": "ORGANIZATION",
                    "Value": "o-exampleorgid"
                },
                {
                    "Type": "EMAIL",
                    "Value": "juan@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Juan's account to join
 Bill's organization."
                }
            ],
            "State": "OPEN"
        },
        {
            "Action": "INVITE",
            "State":"ACCEPTED",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1.471797437427E9,
            "Id": "h-examplehandshakeid222",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "anika@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1.469205437427E9,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type":"MASTER_EMAIL",
```

```
                            "Value":"bill@example.com"
                        },
                        {
                            "Type":"MASTER_NAME",
                            "Value":"Management Account"
                        }
                    ],
                    "Type":"ORGANIZATION",
                    "Value":"o-exampleorgid"
                },
                {
                    "Type":"EMAIL",
                    "Value":"anika@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Anika's account to join
 Bill's organization."
                }
            ]
        }
    ]
}
```

以下示例说明如何取消对账户的邀请。

```
$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Id": "h-examplehandshakeid111",
        "State":"CANCELED",
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "susan@example.com",
                "Type": "EMAIL"
            }
```

```
        ],
        "Resources": [
            {
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid",
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@example.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                        "Value": "CONSOLIDATED_BILLING"
                    }
                ]
            },
            {
                "Type": "EMAIL",
                "Value": "anika@example.com"
            },
            {
                "Type": "NOTES",
                "Value": "This is a request for Susan's account to join Bob's
 organization."
            }
        ],
        "RequestedTimestamp": 1.47008383521E9,
        "ExpirationTimestamp": 1.47137983521E9
    }
}
```

- AWS 软件开发工具包：ListHandshakesForOrganization，CancelHandshake

接受或拒绝来自组织的邀请

您 AWS 账户 可能会收到加入组织的邀请。您可以接受或拒绝邀请。为此，请完成以下步骤。

Note

组织的账户状态影响可见的成本和使用率数据：

- 如果某个成员账户离开组织并且成为独立账户，该账户不再有权访问其属于该组织成员时的时间范围内的成本和使用率数据。该账户只能访问作为独立账户生成的数据。
- 如果某个成员账户离开组织 A 而加入组织 B，该账户不再有权访问其属于组织 A 的成员时的时间范围内的成本和使用率数据。该账户只能访问作为组织 B 的成员生成的数据。
- 如果某个账户重新加入其以前所属的组织，该账户将重新获得对其成本和使用情况历史数据的访问权限。

Note

只有成员账户和独立账户可以接受或拒绝加入组织的邀请。如果向成员账户发送了邀请，则该账户应该在接受邀请之前离开当前组织。如果向已经是 AWS 组织成员的管理账户发送邀请，则该账户将无法接受邀请，除非他们移除组织中的所有成员账户并删除该组织。

最小权限

要接受或拒绝加入 AWS 组织的邀请，您必须具有以下权限：

- `organizations:ListHandshakesForAccount`— 需要在 AWS Organizations 控制台中查看邀请列表。
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `iam:CreateServiceLinkedRole`— 只有在接受邀请时才需要在成员账户中创建服务相关角色以支持与其他 AWS 服务的集成时才需要。有关更多信息，请参阅 AWS Organizations 和服务相关角色。

AWS Management Console

接受或拒绝邀请

1. 加入组织的邀请发送到账户所有者电子邮件地址。如果您是账户拥有者，并且收到了邀请电子邮件消息，请按照电子邮件邀请中的说明操作或者在浏览器中转到 AWS Organizations 控制台，然后选择 Invitations（邀请），或直接转到 member account's Invitation（成员账户的邀请）页面。
2. 根据提示以 IAM 用户的身份登录受邀账户，担任 IAM 角色；或作为该账户的根用户登录（不推荐）。
3. member account's Invitation (成员账户的邀请) 页面显示您的账户加入组织的待接受邀请。

   根据需要选择 Accept invitation (接受邀请) 或 Decline invitation (拒绝邀请)。

   - 如果您在前面的步骤中选择 Accept invitation (接受邀请)，控制台会将您重定向到 Organization overview (Organization 概览) 页面，其中提供了有关您账户现在所属的组织的详细信息。您可以查看组织的 ID 和所有者的电子邮件地址。

     > **Note**
     >
     > 已接受的邀请将继续在列表中显示 30 天。之后，这些邀请将被删除，不再在列表中显示。

     AWS Organizations 在新成员账户中自动创建服务关联角色，以支持与其他 AWS 服务 AWS Organizations 之间的集成。有关更多信息，请参阅 AWS Organizations 和服务相关角色。

     AWS 向组织管理账户的所有者发送一封电子邮件，说明您已接受邀请。它还会发送电子邮件消息到成员账户拥有者，说明该账户现已是组织的成员。
   - 如果您在前面的步骤中选择了 Decline (拒绝)，则您的账户仍在 member account's Invitation (成员账户的邀请) 页面上，其中列出了任何其他待处理邀请。

     AWS 向组织的管理账户所有者发送一封电子邮件，说明您拒绝了邀请。

     > **Note**
     >
     > 已拒绝的邀请将继续在列表中显示 30 天。之后，这些邀请将被删除，不再在列表中显示。

AWS CLI & AWS SDKs

接受或拒绝邀请

您可以使用以下命令来接受或拒绝邀请：

- AWS CLI：accept-handshake、decline-handshake

  以下示例说明如何接受加入组织的邀请。

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "RequestedTimestamp": 1481656459.257,
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "juan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "ALL"
                    }
```

```
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "ACCEPTED"
    }
}
```

以下示例说明如何拒绝加入组织的邀请。

- AWS 软件开发工具包：AcceptHandshake，DeclineHandshake

在组织中创建成员账户

此页面介绍如何在 AWS Organizations 中您的组织内创建 AWS 账户。要了解有关AWS和创建单个 AWS 账户的入门级信息，请参阅资源中心入门。

组织是您集中管理的AWS 账户的集合。您可以执行以下过程来管理属于组织的账户：

- 创建属于组织的AWS 账户
- 访问具有管理账户访问权角色的成员账户

Important

- 当您在组织中创建成员账户时，AWS Organizations 将自动在成员账户中创建一个 AWS Identity and Access Management（IAM）角色 `OrganizationAccountAccessRole`，以允许管理账户中的用户和角色对成员账户进行完全管理控制。此角色受应用于成员账户的任何服务控制策略 (SCP) 的限制。

  此外，AWS Organizations 还会通过 `OrganizationAccountAccessRole` 角色自动向成员账户添加托管策略。这使得能够实现集中控制，以便在策略更新时，附加到相同托管策略的任何其他帐户都会自动更新。以前，在组织内创建的新账户已添加仅适用于该单个账户的内联策略。有关内联和托管策略的更多信息，请参阅 IAM 用户指南中的托管策略与内联策略。

AWS Organizations 还将自动创建一个名为 `AWSServiceRoleForOrganizations` 的服务相关角色，该角色支持与选定 AWS 服务的集成。您必须配置其他服务来允许集成。有关更多信息，请参阅AWS Organizations 和服务相关角色。

- 如果此组织使用 AWS Control Tower 进行管理，则稍后使用 AWS Control Tower 控制台或 API 中的 AWS Control Tower Account Factory 创建账户。如果您在 Organizations 中创建账户，则该账户不会使用 AWS Control Tower 注册。有关更多信息，请参阅《AWS Control Tower 用户指南》中的引用 AWS Control Tower 的外部资源。

> **Note**
>
> AWS 账户作为组织的一部分创建，不会自动订阅AWS营销电子邮件。要为您的账户选择启用接收营销电子邮件，请参阅https://pages.awscloud.com/communication-preferences。

创建属于组织的AWS 账户

登录到组织的管理账户之后，您可以创建自动属于组织的成员账户。使用以下过程创建账户时，AWS Organizations 会自动将管理账户中的以下主要联系人信息复制到新成员账户中：

- 电话号码
- 公司名称
- 网站 URL
- Address

它还会从管理账户中复制通信语言和 Marketplace 信息（在某些 AWS 区域 中是账户的供应商）。

> **Note**
>
> AWS 不会为账户自动收集作为独立成员账户使用所需的全部信息。如果您需要从组织中删除成员账户并使其成为独立账户，则您必须先提供账户的信息，然后才能删除账户。有关更多信息，请参阅成员账户离开组织。

最小权限

要在组织中创建成员账户，您必须拥有以下权限：

- `organizations:CreateAccount`
- `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
- `iam:CreateServiceLinkedRole`（向委托人 `organizations.amazonaws.com` 授权，使其能够在成员账户中创建所需的服务相关角色）。

AWS Management Console

创建自动属于组织的AWS 账户

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，选择 Add an AWS 账户 (添加亚马逊云科技账户)。
3. 在 Add an AWS 账户 (添加亚马逊云科技账户) 页面上，选择 Create an AWS 账户 (创建亚马逊云科技账户)（默认情况下选择该选项）。
4. 在 Create an AWS 账户 (创建亚马逊云科技账户) 页面上，为 AWS 账户 name (亚马逊云科技账户名称) 输入要分配给账户的名称。此名称将帮助您区分该账户与组织中的所有其他账户，并且独立于 IAM 别名或拥有者的电子邮件名称。
5. 对于 Email address of the account's owner (账户拥有者的电子邮件地址)，输入账户拥有者的电子邮件地址。此电子邮件地址不能与其他AWS 账户关联，因为它将成为账户的根用户的用户名凭据。
6. （可选）指定分配到在新账户中自动创建的 IAM 角色的名称。此角色向组织的管理账户授予访问新创建的成员账户的权限。如果您不指定名称，AWS Organizations 将为角色提供默认名称 `OrganizationAccountAccessRole`。建议您对您的所有账户使用默认名称以实现一致性。

   Important

   请记住此角色名称。稍后，您将需要使用此名称向管理账户中的用户和角色的新账户授予访问权。

7. （可选）在标签部分中，向新账户添加一个或多个标签，方法是选择添加标签，然后输入一个键和可选的值。将值留空，设置为空字符串；它并非 `null`。您最多可以向账户附加 50 个标签。

8. 选择 Create AWS 账户 (创建亚马逊云科技账户)。

   - 如果您收到错误，指明您超出了组织的账户配额，请参阅尝试向组织中添加账户时，我收到“quota exceeded (超出限额)”消息。
   - 如果您收到错误，指明由于您的组织仍在进行初始化，所以您无法添加账户，请等待一小时，然后重试。
   - 您还可以检查 AWS CloudTrail 日志以了解有关账户创建是否成功的信息。有关更多信息，请参阅AWS Organizations 中的日志记录和监控。
   - 如果错误仍然存在，请联系 AWS Support。

   此时将显示AWS 账户页面，并将您的新账户添加到列表中。
9. 现在，账户已存在，并拥有向管理账户中的用户授予管理员访问权的 IAM 角色，您可以按照访问组织中的成员账户中的步骤访问账户。

> **Note**
>
> 创建账户时，AWS Organizations 最初为根用户分配一个长（64 个字符）而复杂的随机生成的密码。您无法检索此初始密码。要首次以根用户身份访问该账户，您必须完成密码恢复过程。有关更多信息，请参阅以根用户身份访问成员账户。

AWS CLI & AWS SDKs

创建自动属于组织的AWS 账户

您可以使用以下命令之一创建账户：

- AWS CLI：create-account

```
$ aws organizations create-account \
    --email susan@example.com \
    --account-name "Production Account"
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

然后，您可以使用以下命令查看账户创建的状态。

```
$ aws organizations describe-create-account-status \
    --create-account-request-id car-examplecreateaccountrequestid111
{
  "CreateAccountStatus": {
    "State": "SUCCEEDED",
    "AccountId": "555555555555",
    "AccountName": "Production account",
    "RequestedTimestamp": 1470684478.687,
    "CompletedTimestamp": 1470684532.472,
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

- AWS SDK：CreateAccount

访问组织中的成员账户

在组织中创建账户时，除了根用户外，AWS Organizations 还会自动创建默认名为 `OrganizationAccountAccessRole` 的 IAM 角色。您可以在创建名称时指定其他名称，但我们建议您在所有账户中始终如一地命名该名称。我们在本指南中使用默认名称指代角色。AWS Organizations 不创建任何其他用户或其他角色。要访问组织中的账户，您必须使用以下方法之一：

- 创建 AWS 账户 时，最初使用的是一个对账户中所有 AWS 服务 和资源拥有完全访问权限的登录身份。此身份称为 AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。有关其他根用户安全建议，请参阅您的 AWS 账户 的根用户最佳实践。
- 如果您通过使用作为 AWS Organizations 一部分提供的工具创建一个账户，则可以使用名为 `OrganizationAccountAccessRole` 的预配置角色访问该账户，该角色存在于通过这种方式创建的所有新账户中。有关更多信息，请参阅 访问具有管理账户访问权角色的成员账户。
- 如果您邀请现有账户加入您的组织，并且该账户接受邀请，则您可以选择创建 IAM 角色来允许管理账户访问受邀成员账户。此角色应该与自动添加到使用 AWS Organizations 创建的账户中的角色相同。如需创建此角色，请参阅 OrganizationAccountAccessRole 在受邀成员账户中创建。创建角色之后，您可以使用访问具有管理账户访问权角色的成员账户中的步骤访问它。

- 使用 AWS IAM Identity Center 并为 IAM Identity Center 与 AWS Organizations 启用可信访问。这允许用户使用其公司凭证登录 AWS 访问门户并访问向其分配的管理账户或成员账户中的资源。

  有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多账户权限。有关为 IAM Identity Center 设置可信访问的信息，请参阅 AWS IAM Identity Center 和 AWS Organizations。

> **最小权限**
>
> 要从组织中的任何其他账户访问AWS 账户，必须具有以下权限：
>
> - `sts:AssumeRole` – `Resource` 元素必须设置为星号（*）或账户的账户 ID 号，该账户具有要访问新成员账户的用户。

以根用户身份访问成员账户

当您创建新账户时，AWS Organizations 最初为根用户分配一个最少为 64 字符长的密码。所有字符都是随机生成的，不保证出现特定字符集。您无法检索此初始密码。要首次以根用户身份访问该账户，您必须完成密码恢复过程。有关更多信息，请参阅《AWS登录用户指南》AWS 账户中的 “我忘记了 root 用户密码”。

> **注意事项**
>
> - 我们建议的最佳实践是，除了创建其他具有更多受限权限的用户和角色之外，不要使用根用户访问账户。然后以这些用户或角色之一的身份登录。
> - 此外，我们还建议您对根用户启用多重身份验证 (MFA)。重置密码，然后向根用户分配 MFA 设备。
> - 如果您在组织中创建了一个电子邮件地址不正确的成员账户，则无法以根用户身份登录该账户。请联系 AWS Billing and Support 以获取帮助。

OrganizationAccountAccessRole 在受邀成员账户中创建

默认情况下，如果您创建属于组织的成员账户，AWS会自动在账户中创建一个角色，将管理员权限授予管理账户中可以担任角色的 IAM 用户。默认情况下，该角色名为 `OrganizationAccountAccessRole`。有关更多信息，请参阅 访问具有管理账户访问权角色的成员账户。

但是，您邀请 加入组织中的成员账户不 自动创建管理员角色。您必须手动完成此操作，如以下过程中所示。这实际上是复制自动为所创建账户设置的角色。我们建议您为手动创建的角色使用相同的名称 `OrganizationAccountAccessRole`，以确保一致性和方便记忆。

AWS Management Console

在成员账户中创建 AWS Organizations 管理员角色

1. 通过 https://console.aws.amazon.com/iam/ 登录到 IAM 控制台。您必须以 IAM 用户身份登录，担任 IAM 角色；或以成员账户中的根用户身份登录（不推荐）。用户或角色必须具有创建 IAM 角色和策略的权限。
2. 在 IAM 控制台中，导航到角色，然后选择创建角色。
3. 选择 AWS 账户，然后选择 “其他” AWS 账户。
4. 输入您要授予管理员访问权限的管理账户的 12 位数账户 ID 号。在 “选项” 下，请注意以下内容：
   - 对于此角色，由于账户是公司的内部账户，因此，您不应选择 Require external ID (需要外部 ID)。有关外部 ID 选项的更多信息，请参阅何时应使用外部 ID？ 在 IAM 用户指南中。
   - 如果您启用了 MFA 并进行了配置，则可以选择要求使用 MFA 设备进行身份验证。有关 MFA 的更多信息，请参阅 IAM 用户指南AWS中的使用多重身份验证 (MFA)。
5. 请选择 Next（下一步）。
6. 在添加权限页面上，选择名为的AWS托管策略`AdministratorAccess`，然后选择下一步。
7. 在 “名称、查看和创建” 页面上，指定角色名称和可选描述。我们建议您使用 `OrganizationAccountAccessRole`，以便与分配给新账户中角色的默认名称保持一致。要提交您的更改，请选择 Create role (创建角色)。
8. 您的新角色将显示在可用角色列表上。选择新角色的名称以查看详细信息，特别注意提供的链接 URL。向成员账户中需要访问该角色的用户提供此 URL。此外，记下 Role ARN (角色 ARN)，因为您在步骤 15 中需要它。
9. 通过 https://console.aws.amazon.com/iam/ 登录到 IAM 控制台。此时，以管理账户中有权创建策略和将策略分配给用户或组的用户身份登录。
10. 导航到 “策略”，然后选择 “创建策略”。
11. 对于 Service，选择 STS。
12. 对于 Actions (操作)，在 Filter (筛选器) 框中开始键入 **`AssumeRole`**，然后在该角色显示后选中其旁边的复选框。
13. 在 “资源” 下，确保选择 “特定”，然后选择 “添加 ARN”。

14. 输入AWS成员账户 ID 号，然后输入您之前在步骤 1–8 中创建的角色的名称。选择添加 ARN。
15. 如果您正授予在多个成员账户中代入该角色的权限，请为每个账户重复步骤 14 和 15。
16. 请选择 Next（下一步）。
17. 在查看并创建页面上，输入新策略的名称，然后选择创建策略以保存您的更改。
18. 在导航窗格中选择 “用户组”，然后选择要用来委派成员账户管理的群组名称（不是复选框）。
19. 选择 Permissions（权限）选项卡。
20. 选择 “添加权限”，选择 “附加策略”，然后选择您在步骤 11—18 中创建的策略。

作为选定组成员的用户现在可以使用您在步骤 9 中捕获的 URL 来访问每个成员账户的角色。他们可以像访问您在组织中创建的账户一样访问这些成员账户。有关使用角色来管理成员账户的更多信息，请参阅访问具有管理账户访问权角色的成员账户。

访问具有管理账户访问权角色的成员账户

使用 AWS Organizations 控制台创建成员账户时，AWS Organizations 将自动在账户中创建 IAM 角色（名为 `OrganizationAccountAccessRole`）。此角色具有成员账户中的完整管理权限。此角色的访问范围包括管理账户中的所有主体，因此该角色将配置为授予对该组织管理账户的访问权限。您可以按照 OrganizationAccountAccessRole 在受邀成员账户中创建中的步骤，为受邀成员账户创建相同的角色。要使用此角色访问成员账户，您必须以有权担任角色的管理账户中用户的身份登录。要配置这些权限，请执行以下过程。我们建议您向组而不是用户授予权限，以便于维护。

AWS Management Console

向管理账户中 IAM 组的成员授予权限以访问角色

1. 以管理账户中具有管理员权限的用户身份，通过以下网址登录 IAM 控制台：https://console.aws.amazon.com/iam/。这是向 IAM 组委派权限所必需的，该组的用户将具有成员账户中的角色。
2. 首先，创建您稍后在???中需要的托管策略。

   在导航窗格中选择策略，然后选择创建策略。
3. 在可视化编辑器选项卡上，选择 Choose a service (选择服务)，在搜索框中键入 **STS** 以筛选列表，然后选择 STS 选项。
4. 在 “操作” 部分，**assume**在搜索框中键入以筛选列表，然后选择相应AssumeRole选项。
5. 在 “资源” 部分，选择 “特定”，选择 “添加 ARN”，然后键入您在上一节中创建的成员账号和角色名称（我们建议将其命名`OrganizationAccountAccessRole`）。

6. 当对话框显示正确的 ARN 时，选择添加 AR N。
7. （可选）如果您要求多重验证 (MFA)，或要限制此角色从指定的 IP 地址范围进行访问，请展开 Request conditions (请求条件) 部分，然后选择要强制执行的选项。
8. 请选择 Next（下一步）。
9. 在查看并创建页面上，输入新策略的名称。例如：**`GrantAccessToOrganizationAccountAccessRole`**。您还可以添加可选的说明。
10. 选择 Create policy (创建策略) 以保存新的托管策略。
11. 现在，您已有策略可用，您可以将其附加到组。

    在导航窗格中，选择 “用户组”，然后选择您希望其成员能够在成员账户中担任该角色的群组名称（不是复选框）。如果需要，您可以创建新组。
12. 请选择权限选项卡，选择添加权限，然后选择附加策略。
13. （可选）在 Search (搜索) 框中，您可以开始键入策略的名称以筛选列表，直到您可以看到刚刚在Step 2到Step 10中创建的策略的名称。您还可以通过选择 “所有类型”，然后选择 “客户AWS管理” 来筛选出所有托管策略。
14. 选中您的策略旁边的复选框，然后选择附加策略。

现在，作为组成员的 IAM 用户有权使用以下过程在 AWS Organizations 控制台中切换到新角色。

AWS Management Console

切换到成员账户的角色

使用该角色时，用户具有新成员账户中的管理权限。指示您的作为该组成员的 IAM 用户执行以下操作以切换到新角色。

1. 从 AWS Organizations 控制台的右上角，选择包含当前登录名称的链接，然后选择 Switch Role (切换角色)。
2. 输入管理员提供的账户 ID 号和角色名称。
3. 对于 Display Name (显示名称)，输入文本；在您使用角色时，该文本将显示在导航栏的右上角用于替换您的用户名。您还可选择颜色。
4. 选择 Switch Role。现在，您执行的所有操作已完成，并且已将权限授予给您切换到的角色。在切换回之前，您不再具有与原始 IAM 用户关联的权限。
5. 完成执行需要角色权限的操作后，您可以切换回普通 IAM 用户。在右上角选择角色名称（无论您指定为 “显示名称”），然后选择 “返回”。*`UserName`*

其他资源

- 有关授予切换角色权限的更多信息，请参阅 IAM 用户指南中的授予用户切换角色的权限。
- 有关使用您已获得代入权限的角色的更多信息，请参阅 IAM 用户指南中的切换到角色（控制台）。
- 有关使用角色进行跨账户访问的教程，请参阅 IAM 用户指南中的教程：AWS 账户使用 IAM 角色委派访问权限。
- 有关关闭AWS 账户的信息，请参阅关闭组织中的成员账户。

导出组织的 AWS 账户 详细信息

借助 AWS Organizations，组织的管理账户用户和委托管理员可以导出一个包含组织内所有账户详细信息的 .csv 文件。从而让组织管理员能够轻松查看账户并按状态进行筛选：ACTIVE（活动）、SUSPENDED（已暂停）或者 PENDING（待处理）。如果您的组织有许多账户，.csv 文件下载选项可让您轻松通过电子表格查看和筛选账户详细信息。

以前，查看账户的唯一方法是在 AWS Organizations 控制台中查看账户层次结构或列表显示。

> **Note**
>
> 只有管理账户中的主体才能下载账户列表。

导出组织中所有 AWS 账户的列表。

登录到组织的管理账户后，您可以将组织中所有账户的列表下载到一个 .csv 文件。该列表包含每个账户的详细信息，但没有列出账户所属的组织部门（OU）。

该 .csv 文件包含每个账户的以下信息：

- Account ID（账户 ID）– 数值形式的账户标识符。例如：123456789012
- ARN –账户的 Amazon Resource Name。例如：`arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012`
- Email（电子邮件地址）–与账户关联的电子邮件地址。例如：marymajor@example.com
- Name（名称）–账户创建者提供的账户名称。例如：stage testing account
- Status（状态）–组织内的账户状态。值可以是 PENDING（待处理）、ACTIVE（活动）或 SUSPENDED（已暂停）。
- Joined method（加入方法）–指定账户的创建方式。值可以是 INVITED 或 CREATED。

- Joined timestamp（加入时间戳）–账户加入组织的日期和时间。

> **最小权限**
>
> 要导出包含组织中所有成员账户的 .csv 文件，您必须拥有以下权限：
>
> - `organizations:DescribeOrganization`
> - `organizations:ListAccounts`

AWS Management Console

将组织中的所有 AWS 账户导出到 .csv 文件

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择 Actions（操作），然后对于 AWS 账户，选择 Export account list（导出账户列表）。页面顶部的蓝色横幅将显示 Export is in progress!（正在导出！）
3. 文件准备就绪后，横幅变为绿色并显示：Download is ready!（下载准备就绪！）选择 Download CSV。将文件 `Organization_accounts_information.csv` 下载到您的设备。

AWS CLI & AWS SDKs

导出包含账户详细信息的 .csv 文件的唯一方法是使用AWS Management Console。您不能使用 AWS CLI 来到处账户列表 .csv 文件。

从组织中删除成员账户

组织账户管理工作的一部分是删除不再需要的成员 账户。移除成员账户不会导致该账户被注销，而只是将成员账户从组织中移除。以前的成员账户将成为不再由 AWS Organizations 管理的独立 AWS 账户。移除账户后，该账户不再受任何策略约束，并自行支付账单。从组织中移除账户后，该账户应计的任何费用将不再计入该组织的管理账户。

有关删除管理账户的信息，请参阅删除组织。

主题

从组织中移除账户前的注意事项

移除账户之前，您需要注意以下事项：

- 仅当账户拥有作为独立账户运行所需的信息时，才能从组织中移除此账户。当您使用 AWS Organizations 控制台、API 或 AWS CLI 命令在组织中创建账户时，系统将不会自动收集独立账户所需的任何信息。对于您想用作独立账户的每个账户，您必须选择支持计划，提供和验证所需联系信息，并提供当前的付款方式。AWS 将使用该付款方式向账户未绑定到组织期间发生的任何可结算（非AWS免费套餐）AWS活动收费。要移除还没有此信息的账户，请按照 成员账户离开组织 中的步骤操作。
- 要删除您在组织中创建的账户，您必须等到账户创建后至少七天。邀请的账户不受此等待期限的限制。
- 当账户成功离开该组织时，AWS 账户的拥有者将负责所有新的AWS应计成本，并使用账户的付款方式。该组织的管理账户不再负责。
- 要删除的账户不得是为组织启用的任何AWS服务的委托管理员账户。如果该账户是委托管理员，则必须首先将委托管理员账户更改为组织中剩余的其他账户。要详细了解如何禁用或更改 AWS 服务的委托管理员账户，请参阅该服务的文档。
- 即使在从组织内删除已创建的账户（使用 AWS Organizations 控制台或 `CreateAccount` API 创建的账户）之后，(i) 已创建账户仍受与我们达成的创建管理账户协议条款的约束，并且 (ii) 创建管理账户将对其创建的账户执行的任何操作承担共同和单独的责任。未经我们的事先同意，不得转让或转移客户与我们之间的协议以及这些协议下的权利和义务。要获得我们的同意，请联系 AWS。
- 当某个成员账户离开组织后，该账户不再有权访问其属于该组织成员时的时间范围内的成本和使用率数据。但是，组织的管理账户仍可以访问这些数据。如果该账户重新加入组织，则其将可以再次访问这些数据。
- 当成员账户离开组织时，所有附加到该账户的标签都将被删除。
- 当您从组织中移除成员账户时，为允许该组织的管理账户访问而创建的任何 IAM 角色都不会自动删除。如果要终止以前组织的管理账户的此访问权限，则必须手动删除 IAM 角色。有关如何删除角色的信息，请参阅《IAM 用户指南》中的删除角色或实例配置文件。

从组织中删除账户的影响

当您从组织中移除账户时，不会对该账户进行任何直接更改。但会产生以下间接影响：

- 现在，该账户负责支付自己的费用，并且必须向该账户附加有效的付款方式。
- 该账户中的委托人不再受组织内应用的任何策略影响。这意味着，SCP 施加的限制将不复存在，该账户中的用户和角色将比之前拥有更多权限。其他组织策略类型不能再强制执行或处理。
- 如果您在任何策略中使用 `aws:PrincipalOrgID` 条件键，以限制只能访问组织中AWS 账户的用户和角色，那么您应该在删除成员账户之前查看并可能更新这些策略。如果不更新策略，则当账户离开组织时，账户中的用户和角色可能会失去对资源的访问权限。
- 与其他服务的集成可能会被禁用。如果您从已启用AWS服务集成的组织中删除账户，则此账户中的用户将无法再使用该服务。

从组织中移除成员账户

登录组织的管理账户后，您可以从组织中移除不再需要的成员账户。为此，请完成以下过程。以下过程仅适用于成员账户。要移除管理账户，您必须删除组织。

> **Note**
>
> 如果从组织中删除成员账户，则该成员账户将不再由组织协议所涵盖。管理账户管理员应在从组织中删除成员账户之前将此信息传达给成员账户，以便成员账户可以在必要时添加新协议。有效的组织协议列表可在 AWS Artifact 控制台的 AWS Artifact Organization Agreements (Amazon Artifact 组织协议) 页面中查看。

> **最小权限**
>
> 要从您的组织中移除一个或多个成员账户，您必须以管理账户中的用户或角色身份登录并且必须拥有以下权限：
>
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
> - `organizations:RemoveAccountFromOrganization`
>
> 如果您选择在第 5 步中以成员账户中的用户或角色身份登录，则该用户或角色必须拥有以下权限：

- `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要。
- `organizations:LeaveOrganization` – 请注意，组织管理员可以将删除此权限的策略应用到您的账户，从而阻止您从组织中删除自己的账户。
- 如果您以 IAM 用户身份登录并且账户缺少付款信息，则用户必须具有 `aws-portal:ModifyBilling` 和 `aws-portal:ModifyPaymentMethods` 权限（如果账户尚未迁移到精细权限）或 `payments:CreatePaymentInstrument` 和 `payments:UpdatePaymentPreferences` 权限（如果账户已迁移到精细权限）。此外，成员账户必须已启用对账单的 IAM 用户访问权限。如果尚未启用此权限，请参阅《AWS Billing 用户指南》中的激活对账单和成本管理控制台的访问权。

AWS Management Console

从组织中删除成员账户

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，找到并选中要从组织中删除的每个成员账户旁的复选框 ☑ 。
   您可以导航 OU 层次结构，或启用 View AWS 账户 only (仅限查看亚马逊云科技账户) 来查看没有 OU 结构的账户的平面列表。如果您有很多账户，您可能需要在列表底部选择 Load more accounts in 'ou-name' (加载使用“OU 名称”的更多账户) 以查找要移动的所有账户。

   在AWS 账户页面上，找到并选中要从组织中删除的成员账户的名称。您可能需要展开 OU（选择 ▶ ）以查找所需的账户。
3. 选择 Actions (操作)，然后在AWS 账户下，选择 Remove from organization (从组织中删除)。
4. 在 Remove account 'account-name' (#account-id-num) from organization? (是否从组织中删除账户“账户名称”(#account-id-num)？) 对话框中，选择 Remove account (删除账户)。
5. 如果 AWS Organizations 无法删除一个或多个账户，通常是因为您没有提供账户作为独立账户运行所需的全部信息。执行以下步骤：

   a. 登录失败的账户。建议您通过选择 Copy link (复制链接)，然后将它粘贴在新的无痕浏览器窗口的地址栏中来登录成员账户。如果您未使用无痕窗口，则您已注销管理账户，并且无法导航回此对话框。

b. 此浏览器会将您转至注册过程以完成此账户缺失的任何步骤。完成显示的所有步骤。步骤可能包括：

- 提供联系人信息
- 提供有效的付款方式
- 验证电话号码
- 选择支持计划选项

c. 在完成注册过程的最后一步后，AWS 会自动将您的浏览器重定向至成员账户的 AWS Organizations 控制台。选择 Leave organization，然后在确认对话框中确认您的选择。系统将您重定向到 控制台的 Getting StartedAWS Organizations 页面，在其中可以查看您的账户加入其他组织的待处理邀请。

d. 从组织中删除授予访问您账户的权限的 IAM 角色。

> **Important**
>
> 如果您的账户是在组织中创建的，Organizations 会在该账户中自动创建一个 IAM 角色，以允许组织的管理账户进行访问。如果该账户被邀请加入，则 Organizations 不会自动创建此类角色，但您或其他管理员可能已经创建了一个角色来获得相同的好处。在任何一种情况下，当您从组织中删除账户时，任何此类角色都不会被自动删除。如果要终止以前组织的管理账户的此访问权限，则必须手动删除此 IAM 角色。有关如何删除角色的信息，请参阅《IAM 用户指南》中的删除角色或实例配置文件。

AWS CLI & AWS SDKs

从组织中删除成员账户

您可以使用以下命令之一删除成员账户：

- AWS CLI：remove-account-from-organization

```
$ aws organizations remove-account-from-organization \
    --account-id 123456789012
```

如果成功，此命令不会产生任何输出。

- AWS SDK：RemoveAccountFromOrganization

从组织中删除成员账户后，请确保从组织中删除授予您账户访问权限的 IAM 角色。

> **Important**
>
> 如果您的账户是在组织中创建的，Organizations 会在该账户中自动创建一个 IAM 角色，以允许组织的管理账户进行访问。如果该账户被邀请加入，则 Organizations 不会自动创建此类角色，但您或其他管理员可能已经创建了一个角色来获得相同的好处。在任何一种情况下，当您从组织中删除账户时，任何此类角色都不会被自动删除。如果要终止以前组织的管理账户的此访问权限，则必须手动删除此 IAM 角色。有关如何删除角色的信息，请参阅《IAM 用户指南》中的删除角色或实例配置文件。

成员账户也可以使用 leave-organization 来移除自己。有关更多信息，请参阅成员账户离开组织。

成员账户离开组织

登录成员账户后，您可以将该账户从其组织中删除。为此，请完成以下过程。以下过程仅适用于成员账户。管理账户不能使用此方法离开组织。要移除管理账户，您必须删除组织。

> **Note**
>
> 组织的账户状态影响可见的成本和使用率数据：
>
> - 如果某个成员账户离开组织并且成为独立账户，该账户不再有权访问其属于该组织成员时的时间范围内的成本和使用率数据。该账户只能访问作为独立账户生成的数据。
> - 如果某个成员账户离开组织 A 而加入组织 B，该账户不再有权访问其属于组织 A 的成员时的时间范围内的成本和使用率数据。该账户只能访问作为组织 B 的成员生成的数据。
> - 如果某个账户重新加入其以前所属的组织，该账户将重新获得对其成本和使用情况历史数据的访问权限。

> **Important**
>
> 如果您离开一个组织，您将不再被该组织的管理账户代表您接受的组织协议所涵盖。您可以在 AWS Artifact 控制台的 AWS Artifact Organization Agreements (Amazon Artifact 组织协议) 页面中查看这些组织协议的列表。在离开组织之前，您应该在您的法律、隐私或合规性团队的协助下确定您是否有必要建立新的协议。

最小权限

要退出 AWS 组织，您必须拥有以下权限：

- `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要。
- `organizations:LeaveOrganization` – 请注意，组织管理员可以将删除此权限的策略应用到您的账户，从而阻止您从组织中删除自己的账户。
- 如果您以 IAM 用户身份登录并且账户缺少付款信息，则用户必须具有 `aws-portal:ModifyBilling` 和 `aws-portal:ModifyPaymentMethods` 权限（如果账户尚未迁移到精细权限）或 `payments:CreatePaymentInstrument` 和 `payments:UpdatePaymentPreferences` 权限（如果账户已迁移到精细权限）。此外，成员账户必须已启用对账单的 IAM 用户访问权限。如果尚未启用此权限，请参阅《AWS Billing 用户指南》中的激活对账单和成本管理控制台的访问权。

AWS Management Console

成员账户离开组织

1. 在 AWS Organizations 控制台处登录到 AWS Organizations 控制台。您必须以 IAM 用户身份登录，担任 IAM 角色；或以组织成员账户中的根用户身份登录（不推荐）。

   默认情况下，您无权访问使用 AWS Organizations 创建的成员账户中的根用户密码。如果需要，请按照以根用户身份访问成员账户中的步骤恢复根用户密码。
2. 在 Organizations 控制面板页面上，选择退出组织。
3. 在是否要退出组织？对话框中，选择退出组织。当系统提示进行确认时，确认您选择删除账户。确认后，您将重定向到 AWS Organizations 控制台的入门页面，可在其中查看您的账户加入其他组织的待处理邀请。

   如果显示当前无法退出组织消息，则表示您的账户尚不具备作为独立账户运行所需的所有信息。如果是这样，请继续下一步。
4. 如果是否要退出组织？对话框显示当前无法退出组织消息，选择完成账户注册步骤链接。
5. 在注册 AWS 页面上，输入成为独立账户所需的所有信息。可能涉及以下类型的信息：
   - 联系人姓名和地址
   - 有效付款方式
   - 电话号码验证

- 支持计划选项

6. 在出现一个指明注册过程已完成的对话框时，请选择 Leave organization。

   您将看到确认对话框。确认您选择删除账户。系统将您重定向到 控制台的 Getting StartedAWS Organizations 页面，在其中可以查看您的账户加入其他组织的待处理邀请。

7. 从组织中删除授予访问您账户的权限的 IAM 角色。

   > **Important**
   >
   > 如果您的账户是在组织中创建的，Organizations 会在该账户中自动创建一个 IAM 角色，以允许组织的管理账户进行访问。如果该账户被邀请加入，则 Organizations 不会自动创建此类角色，但您或其他管理员可能已经创建了一个角色来获得相同的好处。在任何一种情况下，当您从组织中删除账户时，任何此类角色都不会被自动删除。如果要终止以前组织的管理账户的此访问权限，则必须手动删除此 IAM 角色。有关如何删除角色的信息，请参阅《IAM 用户指南》中的删除角色或实例配置文件。

AWS CLI & AWS SDKs

作为成员账户退出组织

您可以使用以下命令之一离开组织：

- AWS CLI：leave-organization

  以下示例将迫使其凭据被用于运行命令的账户退出组织。

  ```
  $ aws organizations leave-organization
  ```

  如果成功，此命令不会产生任何输出。

- AWS SDK：LeaveOrganization

在成员账户离开组织后，请确保从组织中删除授予您账户访问权限的 IAM 角色。

> **Important**
>
> 如果您的账户是在组织中创建的，Organizations 会在该账户中自动创建一个 IAM 角色，以允许组织的管理账户进行访问。如果该账户被邀请加入，则 Organizations 不会自动创建此

类角色，但您或其他管理员可能已经创建了一个角色来获得相同的好处。在任何一种情况下，当您从组织中删除账户时，任何此类角色都不会被自动删除。如果要终止以前组织的管理账户的此访问权限，则必须手动删除此 IAM 角色。有关如何删除角色的信息，请参阅《IAM 用户指南》中的删除角色或实例配置文件。

管理账户中的用户也可以使用 remove-account-from-organization 来移除成员账户。有关更多信息，请参阅从组织中移除成员账户。

关闭组织中的成员账户

如果您不再需要组织中的成员帐户，则可以按照本节中的说明从AWS Organizations 控制台将其关闭。只有当您的组织处于 “所有功能” 模式时，您才能使用 AWS Organizations 控制台关闭成员账户。

您也可以在以 root 用户身份登录 AWS Management Console 后 AWS 账户 直接从 “帐户” 页面关闭。有关 step-by-step 说明，请参阅《AWS 账户管理指南》 AWS 账户中的 “关闭”。

要关闭管理账户，请参阅关闭组织中的管理账户。

如何关闭成员账户

登录到企业的管理账户时，您可以关闭属于企业的成员账户。为此，请完成以下步骤。

> **Important**
>
> 在您关闭会员账户之前，我们强烈建议您查看注意事项并了解关闭账户的影响。有关更多信息，请参阅《账户管理指南》中的 “关闭账户前须知事项” 和 “关闭账户后的AWS 注意事项”。

AWS Management Console

通过 AWS Organizations 控制台关闭成员账户

1. 登录 AWS Organizations 控制台。
2. 在 AWS 账户 页面上，找到并选择您想要关闭的成员账户的名称。您可以导航 OU 层次结构，或查看没有 OU 结构的账户的平面列表。
3. 选择页面顶部的账户名称旁边的 Close（关闭）。处于整合账单模式的 Organizations 将无法在控制台中看到 “关闭” 按钮。要以整合账单模式关闭账户，请按照《账户管理指南》中如何关闭账户中的 “独立账户” 选项卡中的AWS 步骤进行操作。

4. 选中每个复选框以确认所有必需的账户关闭报表。
5. 输入成员账户 ID，然后选择关闭账户。

> **Note**
> 您关闭的任何成员账户都将在 AWS Organizations 控制台的账户名称旁边显示一个SUSPENDED标签。

从 “账户” 页面关闭成员账户

或者，您可以直接从中的账户页面关闭 AWS 成员账户 AWS Management Console。如需 step-by-step指导，请按照《AWS 账户管理指南》 AWS 账户中关闭和中的说明进行操作。

AWS CLI & AWS SDKs

要关闭 AWS 账户

您可以使用以下命令之一关闭 AWS 账户：

- AWS CLI：close-account

```
$ aws organizations close-account \
    --account-id 123456789012
```

如果成功，此命令不会产生任何输出。

- AWS 软件开发工具包：CloseAccount

保护成员账户免遭关闭

如果您要保护成员账户免遭意外关闭，可以创建一个 IAM policy 来指定哪些账户可免于关闭。受这些策略保护的任何成员账户都无法关闭。这无法使用 SCP 实现，因为它们不会影响管理账户中的主体。

您可以通过以下两种方式之一创建拒绝关闭账户的 IAM policy：

- 通过在 `Resource` 元素中包含 `arn`，在策略中明确列出您要保护的每个账户。要查看示例，请参阅防止本策略中列出的成员账户关闭。

- 标记个人账户以防止其被关闭。在您的策略中使用 aws:ResourceTag 标记全局条件键，以防任何带有该标签的账户被关闭。要了解如何标记账户，请参阅 标记 Organizations 资源。要查看示例，请参阅 防止带标签的成员账户关闭 。

防止成员账户关闭的 IAM policy 示例

以下代码示例显示了两种不同的方法，您可以使用这些方法来限制成员账户关闭其账户。

防止带标签的成员账户关闭

您可以将以下策略附加到管理账户中的身份。此策略防止管理账户中的主体关闭任何标记为 aws:ResourceTag 标记全局条件键、AccountType 键和 Critical 标签值的成员账户。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccountForTaggedAccts",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
            }
        }
    ]
}
```

防止本策略中列出的成员账户关闭

您可以将以下策略附加到管理账户中的身份。此策略可防止管理账户中的主体关闭 Resource 元素中明确指定的成员账户。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
```

```
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
    ]
}
```

关闭组织中的管理账户

要关闭组织中的管理账户，必须先关闭或删除组织中的所有成员账户。关闭管理账户的行为还会删除该组织的实例 AWS Organizations 以及您在关闭后期限到期后在该组织内创建的任何政策。

如何关闭管理账户

使用以下步骤关闭管理账户。

> **Important**
>
> 在关闭管理账户之前，我们强烈建议您查看注意事项并了解关闭账户的影响。有关更多信息，请参阅《账户管理指南》中的 “关闭账户前须知事项” 和 “关闭账户后的AWS 注意事项”。

AWS Management Console

从 “账户” 页面关闭管理账户

> **Note**
>
> 您不能直接从 AWS Organizations 控制台关闭管理账户。

1. 以您要关闭 AWS Management Console 的管理账户的 root 用户身份登录。作为 IAM 用户或角色登录时，您无法关闭账户。
2. 确认您的组织中没有剩余的活跃成员账户。为此，请前往AWS Organizations 控制台，确保所有成员账户都显示在账户名称Suspended旁边。如果您的会员账户仍处于活动状态，则需要关闭组织中的成员账户先按照中提供的指导进行操作，然后才能进入下一步。
3. 在右上角的导航栏上，选择您的账户名或账号，然后选择账户。

4. 在 “账户” 页面上，滚动至页面底部的 “关闭账户” 部分。阅读并确保您了解账户关闭流程。
5. 选择 “关闭账户” 按钮以启动账户关闭流程。
6. 几分钟后，您应该会收到一封电子邮件，确认您的账户已关闭。

AWS CLI & AWS SDKs

其中一个 AWS 软件开发工具包 AWS CLI 的 API 操作不支持此任务。您只能使用来执行此任务 AWS Management Console。

更新您组织中的备用联系人

您可以使用 AWS Organizations 控制台，或者以编程方式使用 AWS CLI 或 AWS SDK，为组织中的账户更新备用联系人。要了解如何更新备用联系人，请参阅《AWS 账户管理参考》中的访问或更新备用联系人。

更新您组织中的主要联系人信息

您可以使用 AWS Organizations 控制台，或者以编程方式使用 AWS CLI 或 AWS SDK，为组织中的账户更新主要联系人信息。要了解如何更新主要联系人信息，请参阅《AWS 账户管理参考》中的访问或更新主要账户联系人。

更新您组织中已启用 AWS 区域

您可以通过 AWS Organizations 控制台为组织内的账户更新已启用 AWS 区域。要了解如何更新已启用 AWS 区域，请参阅 AWS 账户管理参考中的 Specifying which AWS 区域 your account can use（指定您的账户可以使用哪些 AWS 区域）。

在中管理策略 AWS Organizations

中的策略 AWS Organizations 使您能够对组织 AWS 账户 中的应用其他类型的管理。您可以在组织中启用所有功能的情况下使用策略。

AWS Organizations 控制台显示每种策略类型的启用或禁用状态。在 Organize accounts (组织账户) 选项卡上，选择左侧导航窗格中的 Root。屏幕右侧的详细信息窗格显示了所有可用的策略类型。该列表指示在该组织根中已启用和禁用哪些策略。如果出现 Enable (启用) 类型的选项，该类型当前为禁用状态。如果出现 Disable (禁用) 类型的选项，该类型当前为启用状态。

策略类型

Organizations 提供了以下两大类的策略类型：

授权策略

授权策略可帮助您集中管理组织中 AWS 账户 的安全性。

- 服务控制策略 (SCP) 为您组织中的所有账户提供对最大可用权限的集中控制。

管理策略

管理策略使您能够集中配置和管理 AWS 服务及其功能。

- 使用人工智能（AI）服务选择退出政策控制所有组织账户的 AWS AI 服务数据收集设置。
- Backup 策略可帮助您集中管理备份计划并将其应用于组织账户中的 AWS 资源。
- 标签策略可帮助您标准化附加到组织账户中 AWS 资源的标签。

下表总结了每种策略类型的一些特性。有关这些策略类型的其他特性，请参阅 的配额 AWS Organizations。

策略类型	影响管理账户	可附加到根、OU 或账户的最大数量	最大大小	支持查看 OU 或账户的有效策略
SCP	否	5	5120 个字符	否
AI 服务选择退出策略	是	5	2500 个字符	是
备份策略	是	10	10,000 个字符	是
标签策略	是	10	10,000 个字符	是

在组织中使用策略

- 启用和禁用策略类型
- 获取有关组织策略的信息
- 的委派管理员 AWS Organizations
- 管理策略
- 服务控制策略 (SCP)

启用和禁用策略类型

启用策略类型

在创建策略并将其附加到组织之前，必须启用该策略类型才能使用。启用策略类型是组织根上的一次性任务。您只能从组织的管理账户启用策略类型。

最小权限

要启用策略类型，您需要运行以下操作的权限：

- `organizations:EnablePolicyType`
- `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
- `organizations:ListRoots` – 仅当使用 Organizations 控制台时才需要

AWS Management Console

启用策略类型

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Policies (策略) 页面上，选择要启用的策略的名称。
3. 在策略类型页面上，选择 Enable ***policy type*** (启用策略类型)。

   该页面会被指定类型的可用策略列表替换。

AWS CLI & AWS SDKs

启用策略类型

您可以使用以下命令之一启用策略类型：

- AWS CLI：enable-policy-type

  以下示例说明如何为组织启用备份策略。请注意，您必须指定组织根的 ID。

```
$ aws organizations enable-policy-type \
    --root-id r-a1b2 \
```

```
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": [
            {
                "Type": "BACKUP_POLICY",
                "Status": "ENABLED"
            }
        ]
    }
}
```

输出中的 PolicyTypes 列表现在包含指定的策略类型，其 Status 为 ENABLED。

- AWS SDK：EnablePolicyType

禁用策略类型

如果您不想再在组织中使用某种策略类型，则可以禁用该类型以防止其意外使用。您只能从组织的管理账户禁用策略类型。

Important

- 禁用策略类型时，指定类型的所有策略都会自动从组织根中的所有实体分离。策略不会 被删除。
- （仅限服务控制策略类型）如果稍后重新启用 SCP 策略类型，则组织根中的所有实体最初仅附加到默认 FullAWSAccess SCP。当组织中禁用 SCP 时，SCP 到实体的附件将丢失。如果以后要重新启用 SCP，则必须根据需要将其重新附加到组织的根、OU 和账户。

最小权限

要禁用 SCP，您需要运行以下操作的权限：

- organizations:DisablePolicyType
- organizations:DescribeOrganization – 仅当使用 Organizations 控制台时才需要

- `organizations:ListRoots` – 仅当使用 Organizations 控制台时才需要

AWS Management Console

禁用策略类型

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Policies (策略) 页面上，选择要禁用的策略的名称。
3. 在策略类型页面上，选择 Disable ***policy type*** (禁用策略类型)。
4. 在确认对话框中，输入单词 **disable**，然后选择 Disable (禁用)。

   指定类型的可用策略列表将消失。

AWS CLI & AWS SDKs

禁用策略类型

可以使用以下命令之一禁用策略类型：

- AWS CLI：disable-policy-type

  以下示例说明如何为组织禁用备份策略。请注意，您必须指定组织根的 ID。

```
$ aws organizations disable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": []
    }
}
```

  输出中的 `PolicyTypes` 列表不再包含指定的策略类型。

- AWS SDK：DisablePolicyType

获取有关组织策略的信息

本部分介绍了各种方法来获取有关您组织中的策略的详细信息。这些过程适用于所有 策略类型。您必须先在组织根中启用一个策略类型，然后才能将该类型的策略附加到组织根中的任何实体。

列出所有策略

> **最小权限**
>
> 要列出组织中的策略，您必须拥有以下权限：
>
> - `organizations:ListPolicies`

您可以在AWS Management Console中或通过使用 AWS Command Line Interface（AWS CLI）命令或 AWS SDK 操作来查看您组织中的策略。

AWS Management Console

列出组织中的所有策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Policies (策略) 页面上，选择要列出的策略。

   如果启用了指定的策略类型，则控制台将显示组织中当前可用的该类型所有策略的列表。
3. 返回到 Policies (策略) 页面，然后对每种策略类型重复此操作。

AWS CLI & AWS SDKs

列出组织中的所有策略

可以使用以下命令之一列出组织中的策略：

- AWS CLI：list-policies

  以下示例说明了如何获取您组织中所有服务控制策略的列表。您必须指定要查看的策略类型。对要包含的每个策略类型重复使用以下命令。

```
$ aws organizations list-policies \
```

```
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS SDK：ListPolicies

列出附加到根、OU 或账户的策略

> **最小权限**
>
> 要列出附加到您组织中的根、组织部门（OU）或账户的策略，您必须拥有以下权限：
>
> - `organizations:ListPoliciesForTarget`，且同一条策略语句中有一个 `Resource` 元素包含所指定目标的 Amazon Resource Name（ARN）（或“*”）。

AWS Management Console

列出直接附加到所指定根、OU 或账户的所有策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，选择要查看其策略的根、OU 或账户的名称。您可能需要展开 OU（选择 ▶ ）以查找所需的 OU。
3. 在根、OU 或账户页面上，选择 Policies (策略) 选项卡。

   Policies (策略) 选项卡显示附加到该根、OU 或账户的所有策略，并按策略类型分组。

AWS CLI & AWS SDKs

列出直接附加到所指定根、OU 或账户的所有策略

可以使用以下命令之一列出附加到实体的策略：

- AWS CLI：list-policies-for-target

  以下示例列出了附加到指定 OU 的所有服务控制策略。您必须同时指定根、OU 或账户的 ID，以及要列出的策略类型。

```
$ aws organizations list-policies-for-target \
    --target-id ou-a1b2-f6g7h222 \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS SDK：ListPoliciesForTarget

列出策略附加到的所有根、OU 和账户

最小权限

要列出策略附加到的实体，您必须拥有以下权限：

- `organizations:ListTargetsForPolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。

AWS Management Console

列出拥有附加的所指定策略的所有根、OU 和账户

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Policies (策略) 页面上，选择策略类型，然后选择要检查其附件的策略的名称。
3. 选择 Targets (目标) 选项卡，以显示所选策略附加到的每个根、OU 和账户的表。

AWS CLI & AWS SDKs

列出拥有附加的所指定策略的所有根、OU 和账户

可以使用以下命令之一列出具有策略的实体：

- AWS CLI：list-targets-for-policy

  以下示例显示指定策略的根、OU 和账户的所有附件。

```
$ aws organizations list-targets-for-policy \
    --policy-id p-FullAWSAccess
{
    "Targets": [
        {
            "TargetId": "ou-a1b2-f6g7h111",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
            "Name": "testou2",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "ou-a1b2-f6g7h222",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
            "Name": "testou1",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
```

```
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
        }
    ]
}
```

- AWS SDK：ListTargetsForPolicy

获取有关策略的详细信息

> **最小权限**
>
> 要显示策略的详细信息，您必须拥有以下权限：
>
> - `organizations:DescribePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。

AWS Management Console

获取有关策略的详细信息

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Policies (策略) 页面上，选择要检查的策略类型，然后选择策略的名称。

   策略页面显示有关策略的可用信息，包括 ARN、描述和附加项。

   - Content (内容) 选项卡以 JSON 格式显示策略的当前内容。
   - Targets (目标) 选项卡显示策略附加到的根、OU 和账户的列表。
   - Tags (标签) 选项卡显示附加到策略的标签。注意：Tags (标签) 选项卡不可用于AWS托管式策略。

要编辑策略，请选择 Edit policy (编辑策略)。由于每种策略类型都有不同的编辑要求，因此请参阅有关指定策略类型的创建和更新策略相关说明。

AWS CLI & AWS SDKs

获取有关策略的详细信息

可以使用以下命令之一获取有关策略的详细信息：

- AWS CLI：describe-policy

  以下示例显示指定策略的详细信息。

```
$ aws organizations describe-policy \
    --policy-id p-FullAWSAccess
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        },
        "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n
      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*
\"\n    }\n  ]\n}"
    }
}
```

- AWS SDK：DescribePolicy

的委派管理员 AWS Organizations

我们建议您仅将 AWS Organizations 管理账户及其用户和角色用于必须由该账户执行的任务。此外，我们还建议您将所有的 AWS 资源存储在组织的其他成员账户中，而非保存在管理账户中。这是因为，Organizations 服务控制策略（SCP）等安全功能不会限制管理账户中的用户或角色。

您可以从组织的管理账户中，将 Organizations 的策略管理委托给指定的成员账户，来执行默认情况下仅管理账户才可执行的策略操作。

创建或更新基于资源的委托策略

在管理账户中，为您的组织创建或更新基于资源的委托策略，并添加一条语句，指定哪些成员账户可以对策略执行操作。您可以在策略中添加多个语句来表示成员账户的不同权限集。

最小权限

要创建或更新基于资源的委托策略，您需要运行以下操作的权限：

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

此外，您必须向委托管理员账户中的角色和用户授予相应的 IAM 权限，以执行所需操作。如果没有 IAM 权限，则假设调用方委托人没有管理 AWS Organizations 策略所需的权限。

AWS Management Console

使用下列方法之一在 AWS Management Console 中向基于资源的委托策略中添加语句：

- JSON 策略：粘贴和自定义基于资源的委托策略示例，以便在您的账户中使用，或者在 JSON 编辑器中键入您自己的 JSON 策略文档。
- 可视化编辑器：在可视化编辑器中构建新的委托策略，其可指导您创建委托策略，而无需编写 JSON 语法。

使用 JSON 策略编辑器创建或更新委托策略

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择设置。
3. 在 AWS Organizations的委托管理员部分中，选择委托以创建 Organizations 委托策略。要更新现有的委托策略，请选择 Edit（编辑）。
4. 键入或粘贴一个 JSON 策略文档。有关 IAM policy 语言的详细信息，请参阅 IAM JSON 策略参考。

5. 解决策略验证过程中生成的任何安全警告、错误或常规警告，然后选择 Create policy（创建策略）以保存工作。

使用可视化编辑器创建或更新委托策略

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择设置。
3. 在 AWS Organizations的委托管理员部分中，选择委托以创建 Organizations 委托策略。要更新现有的委托策略，请选择 Edit（编辑）。
4. 在 Create Delegation policy（创建委托策略）页面上，选择 Add new statement（添加新语句）。
5. 将 Effect 设置为 `Allow`。
6. 添加 `Principal` 以定义要委托的成员账户。有关语法的详细信息，请参阅 基于资源的委托策略示例。
7. 从 Actions（操作）列表中选择要委托的操作。您可使用 Filter actions（筛选操作）缩小所选内容的范围。
8. 要指定委托成员账户是否可以将策略附加到组织根或组织单元（OU），请设置 `Resources`。您还必须选择 `policy` 作为资源类型。有关其他详细信息，请参阅 基于资源的委托策略示例。您可以通过以下方式指定资源：

   - 选择 Add a resource（添加资源），并按照对话框中的提示构建 Amazon 资源名称（ARN）。
   - 在编辑器中手动列出资源 ARN。有关 ARN 语法的更多信息，请参阅《通用参考指南》中的 Amazon 资源名称 (ARN)。 AWS 有关在策略的资源元素中使用 ARN 的信息，请参阅 IAM JSON 策略元素：Resource。
9. 选择 Add a condition（添加条件）以指定其他条件，包括要委托的策略类型。选择条件的 Condition key（条件键）、Tag key（标签键）、Qualifier（限定词）和 Operator（运算符），然后键入 **`Value`**。有关其他详细信息，请参阅基于资源的委托策略示例。完成后，选择 Add condition（添加条件）。有关 Condition 元素的更多信息，请参阅 IAM JSON 策略参考中的 IAM JSON 策略元素：Condition。
10. 要添加更多权限块，请选择 Add new statement（添加新语句）。对于每个块，重复步骤 5 到步骤 9。
11. 解决策略验证过程中生成的任何安全警告、错误或常规警告，然后选择 Create policy（创建策略）以保存工作。

AWS CLI & AWS SDKs

创建或更新委托策略

可以使用以下命令创建或更新委托策略：

- AWS CLI: put-resource-policy

  以下为创建或更新委托策略的示例。

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            }
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
```

```
        }
    ]
}
```

- AWS 软件开发工具包：PutResourcePolicy

支持的委托策略操作

委托策略支持以下操作：

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount

- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy
- TagResource
- UntagResource
- UpdatePolicy

支持的条件键

只有支持的条件键 AWS Organizations 才能用于委托策略。有关更多信息，请参阅《服务授权参考》AWS Organizations中的条件密钥。

查看基于资源的委托策略

在管理账户中，查看贵组织基于资源的委托策略，以了解哪些委托管理员有权管理哪些策略类型。

> **最小权限**
>
> 要查看基于资源的委托策略，您需要运行以下操作的权限：organizations:DescribeResourcePolicy。

AWS Management Console

查看委托策略

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择设置。

3. 在 AWS Organizations的委托管理员部分中，滚动查看完整的委托策略。

AWS CLI & AWS SDKs

查看委托策略

可以使用以下命令查看委托策略：

- AWS CLI: describe-resource-policy

  以下为检索策略的示例。

```
$ aws organizations describe-resource-policy
```

- AWS 软件开发工具包：DescribeResourcePolicy

删除基于资源的委托策略

当您不再需要委托组织中的策略管理时，可以从组织的管理账户中删除基于资源的委托策略。

> **Important**
> 如果您删除基于资源的委托策略，将无法恢复。

> **最小权限**
> 要删除基于资源的委托策略，您需要运行以下操作的权限：`organizations:DeleteResourcePolicy`。

AWS Management Console

删除委托策略

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择设置。

3. 在 AWS Organizations的委托管理员部分中，选择删除。
4. 在 Delete policy（删除策略）确认对话框中，键入 **delete**。然后，选择 Delete policy（删除策略）。

AWS CLI & AWS SDKs

删除委托策略

可以使用以下命令删除委托策略：

- AWS CLI: delete-resource-policy

  以下为删除策略的示例。

  ```
  $ aws organizations delete-resource-policy
  ```

- AWS 软件开发工具包：DeleteResourcePolicy

基于资源的委托策略示例

以下代码示例说明如何使用基于资源的委托策略。

示例

- 示例：查看组织、OU、账户和策略
- 示例：管理组织备份策略所需的合并权限

示例：查看组织、OU、账户和策略

在委托策略管理之前，必须委托浏览组织结构并查看组织单元（OU）、账户及其附加策略的权限。

此示例说明如何将这些权限包含在成员账户 *AccountId* 的基于资源的委托策略中。

> **Important**
>
> 建议您仅包含对所需最低操作的权限，如示例所示，但可以使用此策略委托任何 Organizations 只读操作。

此示例委托策略授予以编程方式通过 AWS API 或 AWS CLI 完成此操作的必要权限。要使用此委托策略，请将 *AccountId* 的 AWS 占位符文本替换为您自己的信息。然后，按照 的委派管理员 AWS Organizations 中的说明进行操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

示例：管理组织备份策略所需的合并权限

此示例说明如何创建基于资源的委托策略，该策略允许管理账户委托管理组织内部备份策略所需的全部权限，包括 create、read、update 和 delete 操作以及 attach 和 detach 策略操作。要了解每项操作、资源和条件的重要性，请参阅 基于资源的委托策略示例。

> **Important**
>
> 此策略允许委托管理员对组织中任何账户（包括管理账户）创建的策略执行指定操作。

此示例委托策略授予 AWS 通过 API 或 AWS CLI以编程方式完成操作所需的权限。要使用此委托策略，请将、*MemberAccountIdManagementAccountIdOrganizationId*、和*RootId*的 AWS 占位符文本替换为您自己的信息。然后，按照 的委派管理员 AWS Organizations 中的说明进行操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "BACKUP_POLICY"
        }
      }
    },
```

```
    {
      "Sid": "DelegatingAllActionsForBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/r-RootId",
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

管理策略

管理策略使您能够集中配置和管理 AWS 服务及其功能。对于继承那些策略的 OU 和账户而言，策略对它们产生的影响取决于您在 AWS Organizations 中应用的管理策略的类型。查看此部分中的主题，了解有关管理策略的相关术语和概念。

主题

- 了解管理策略继承
- AI 服务选择退出策略
- 备份策略
- 标签策略

了解管理策略继承

> **Note**
>
> 此部分中的信息不适用于 SCP，因为 SCP 同时管理允许和拒绝 IAM 操作。尽管 SCP 附加到根、OU 和账户，但在从根到账户直接路径中的每个 OU（包括目标账户本身），允许操作在每个级别的 SCP 中都需要显式 `allow` 语句。有关 SCP 如何在 AWS Organizations 层次结构中工作的详细信息，请参阅 SCP 评估。

您可以将某个管理策略附加到组织中的组织实体（组织根、组织部门 (OU) 或账户）：

- 当您将某个管理策略附加到组织根时，组织中的所有 OU 和账户都将继承该策略。
- 当您将某个管理策略附加到特定 OU 时，直接位于该 OU 下的账户或任何子 OU 都将继承该策略。
- 当您将某个管理策略附加到特定账户时，它仅影响该账户。

由于您可以将管理策略附加到组织中的多个级别，因此账户可以继承多个策略。

此部分介绍如何将父策略和子策略转换为账户的有效策略。

主题

继承术语

本主题在讨论管理策略继承时将使用以下术语。

策略继承

组织内不同级别的策略之间的交互，从组织的顶层根下移经过组织单位 (OU) 层次结构直到单个账户。

您可以将策略附加到组织根、OU、单个账户以及这些组织实体的任意组合。策略继承是指附加到组织根或 OU 的管理策略。管理策略所附加到的组织根或 OU 的所有成员账户都将继承该策略。

例如，当管理策略附加到组织根时，组织中的所有账户都将继承该策略。这是因为组织中的所有账户始终位于组织根之下。当您将某个策略附加到特定 OU 时，直接位于该 OU 下的账户或任何子 OU 将继承该策略。由于您可以将策略附加到组织中的多个级别，因此账户可以继承单个策略类型的多个策略文档。

父策略

附加到组织树中的策略，其位置高于附加到树中较低位置实体的策略。

例如，如果您将管理策略 A 附加到组织根，则它只是一个策略。如果您还将策略 B 附加到根下的一个 OU，则策略 A 是策略 B 的父策略。策略 B 是策略 A 的子策略。策略 A 和策略 B 合并以便为该 OU 中的账户创建有效标签策略。

子策略

在组织树中附加的级别低于父策略的策略。

有效策略

最后，指定应用于账户的规则的单个策略文档。有效策略是账户继承的任何策略以及直接附加到账户的任何策略的聚合。例如，通过标签策略，您可以查看适用于任何账户的有效标签策略。有关更多信息，请参阅查看有效标签策略。

继承运算符

控制继承策略如何合并到单个有效策略中的运算符。这些运算符被视为是一项高级功能。经验丰富的策略作者可以使用它们来限制子策略可以进行的更改以及如何合并策略中的设置。有关更多信息，请参阅继承运算符。

管理策略类型的策略语法和继承

对于继承策略的 OU 和账户而言，策略对它们产生的影响取决于您选择的管理策略的类型：管理策略类型包括：

- 人工智能 (AI) 服务选择退出策略
- 备份策略
- 标签策略

管理策略类型的语法包括 继承运算符，这使您能够精细地指定应用父策略中的哪些元素以及子 OU 和账户继承时可以哪些覆盖或修改哪些元素。

有效策略 是从组织根和 OU 继承的规则以及直接附加到账户的规则的集合。有效策略指定适用于账户的最终规则集。您可以查看账户的有效策略，其中包含所应用策略中所有继承运算符的效果。有关更多信息，请参阅查看有效标签策略。

继承运算符

继承运算符控制继承的策略和账户策略如何合并到账户的有效策略中。这些运算符包括值设置运算符和子控制运算符。

在 AWS Organizations 控制台中使用可视化编辑器时，您只能使用 @@assign 运算符。其他运算符被视为高级功能。要使用其他运算符，您必须手动编写 JSON 策略。经验丰富的策略作者可以使用继承运算符来控制应用于有效策略的值，并限制子策略可以进行的更改。

值设置运算符

您可以使用以下值设置运算符来控制策略与其父策略交互的方式：

- @@assign – 用指定设置覆盖任何继承的策略设置。如果未继承指定的设置，则此运算符会将该设置添加到有效策略中。此运算符可以应用于任何类型的任何策略设置。
  - 对于单值设置，此运算符将继承的值替换为指定值。
  - 对于多值设置（JSON 数组），此运算符将删除所有继承的值，并将其替换为此策略指定的值。
- @@append – 向继承的设置添加指定的设置（而不删除任何设置）。如果未继承指定的设置，则此运算符会将该设置添加到有效策略中。只能将此运算符用于多值设置。
  - 此运算符将指定的值添加到继承数组中的任何值。
- @@remove – 从有效策略中删除指定的继承设置（如果存在）。只能将此运算符用于多值设置。
  - 此运算符仅从继承自父策略的值数组中删除指定值。其他值可以继续存在于数组中，并且可由子策略继承。

子控制运算符

使用子控制运算符是可选的。您可以使用 @@operators_allowed_for_child_policies 运算符控制子策略可以使用哪些值设置运算符。您可以允许所有运算符、一些特定运算符或不允许运算符。默认情况下，允许所有运算符 (@@all)。

- "@@operators_allowed_for_child_policies":["@@all"] – 子 OU 和账户可以在策略中使用任何运算符。默认情况下，子策略中允许使用所有运算符。

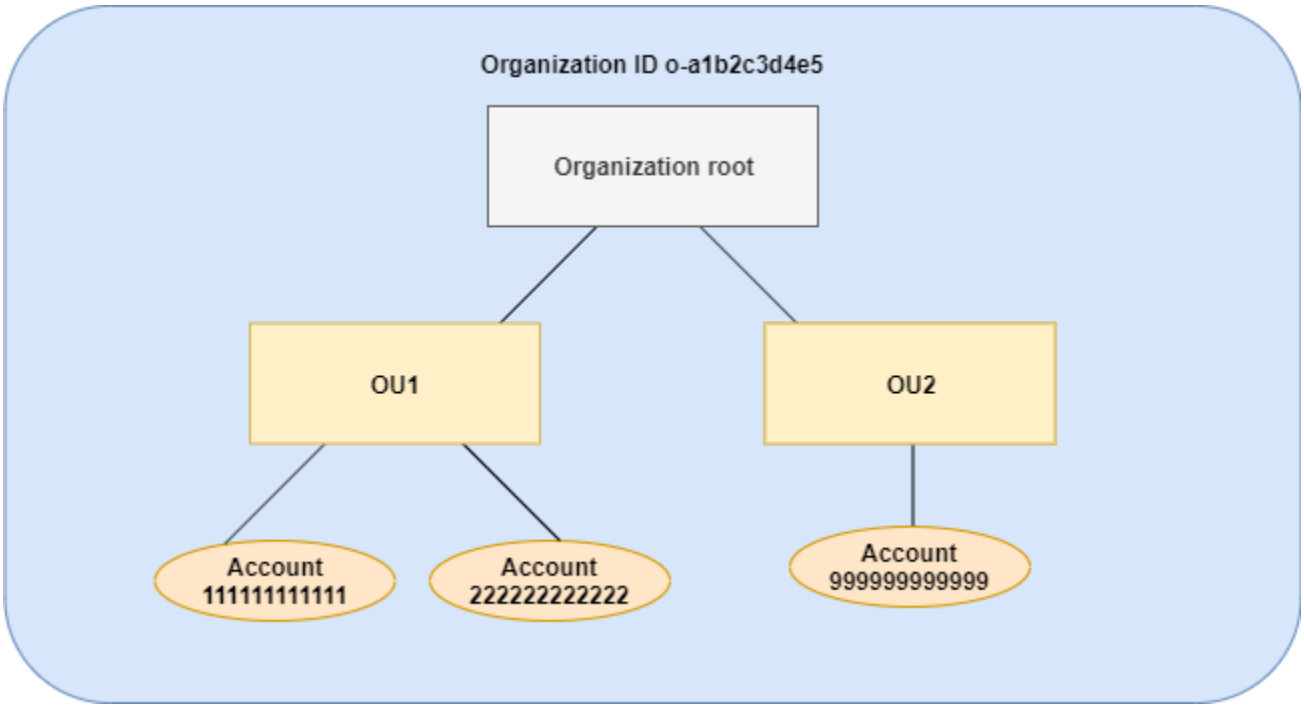
- `"@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"]` – 子 OU 和账户只能在子策略中使用指定的运算符。您可以在此子控制运算符中指定一个或多个值设置运算符。
- `"@@operators_allowed_for_child_policies":["@@none"]` – 子 OU 和账户不能在策略中使用运算符。可以使用此运算符有效锁定在父策略中定义的值，以使子策略无法添加、追加或删除这些值。

> **Note**
>
> 如果继承的子控制运算符限制使用某个运算符，您无法在子策略中反转该规则。如果您在父策略中包括子控制运算符，则它们会在所有子策略中限制值设置运算符。

继承示例

这些示例通过演示如何将父标签策略和子标签策略合并到某个账户的有效标签策略，来说明策略继承的工作原理。

这些示例假定您具有下图所示的组织结构。



示例

- 示例 1：允许子策略仅 覆盖标签值

示例 1：允许子策略仅 覆盖标签值

以下标签策略定义了 CostCenter 标签键和可接受的值，即 Development 和 Support。如果您将其附加到组织根，则标签策略对组织中的所有账户都有效。

策略 A – 组织根标签策略

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

假定您希望 OU1 中的用户为某个键使用不同的标签值，并且您希望对特定资源类型强制使用此标签策略。由于策略 A 没有指定允许使用哪些子控制运算符，因此允许所有运算符。您可以使用 @@assign 运算符并创建类似于以下内容的标签策略，将其附加到 OU1。

策略 B – OU1 标签策略

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
```

```
            },
            "tag_value": {
                "@@assign": [
                    "Sandbox"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

在策略 A 和策略 B 合并以形成账户的有效标签策略时，为标签指定 `@@assign` 运算符会执行以下操作：

- 策略 B 覆盖在父策略（即策略 A）中指定的两个标签值。最终，`Sandbox` 成为了 `CostCenter` 标签键唯一的合规值。
- 添加 `enforced_for` 以指定 `CostCenter` 标签必须是所有 Amazon Redshift 资源和 Amazon DynamoDB 表上的指定标签值。

如图所示，OU1 包括两个账户：111111111111 和 222222222222。

产生的账户 111111111111 和 222222222222 的有效标签策略

> **Note**
>
> 您不能直接将显示的有效策略的内容用作新策略的内容。语法不包括控制与其他子策略和父策略合并所需的运算符。展示的有效政策只是为了了解合并的结果。

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Sandbox"
            ],
```

```
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

示例 2：将新值附加到继承的标签

在某些情况下，您可能希望为组织中的所有账户指定一个标签键以及可接受值的短列表。对于一个 OU 中的账户，您可能希望允许只有这些账户在创建资源时才能指定的其他值。此示例指定如何使用 @@append 运算符来执行此操作。@@append 运算符是一个高级功能。

与示例 1 类似，此示例从用于组织根标签策略的策略 A 开始。

策略 A – 组织根标签策略

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

对于此示例，将策略 C 附加到 OU2。此示例的区别在于，在策略 C 中使用 @@append 运算符会添加而不是覆盖可接受值和 enforced_for 规则的列表。

策略 C – 用于附加值的 OU2 标签策略

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
```

```
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
            },
            "enforced_for": {
                "@@append": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

当策略 A 和策略 C 合并以形成账户的有效标签策略时，将策略 C 附加到 OU2 具有以下效果：

- 由于策略 C 包含 @@append 运算符，它允许添加 而不是覆盖在策略 A 中指定的可接受标签值列表。
- 与在策略 B 中一样，添加 enforced_for 以指定 CostCenter 标签必须用作所有 Amazon Redshift 资源和 Amazon DynamoDB 表上的指定标签值。如果父策略不包含限制子策略可指定值的子控制运算符，则覆盖 (@@assign) 和添加 (@@append) 具有相同的效果。

如图所示，OU2 包括一个账户：999999999999。策略 A 和策略 C 合并以便为账户 999999999999 创建有效标签策略。

适用于账户 999999999999 的有效标签策略

> **Note**
>
> 您不能直接将显示的有效策略的内容用作新策略的内容。语法不包括控制与其他子策略和父策略合并所需的运算符。展示的有效政策只是为了了解合并的结果。

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
```

```
            "tag_value": [
                "Development",
                "Support",
                "Marketing"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

示例 3：从继承标签中删除值

在某些情况下，附加到组织的标签策略定义的标签值数量多于您希望账户使用的数量。此示例说明如何使用 @@remove 运算符修改标签策略。@@remove 是一项高级功能。

与其他示例类似，此示例从用于组织根标签策略的策略 A 开始。

策略 A – 组织根标签策略

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

对于此示例，将策略 D 附加到账户 999999999999。

策略 D – 账户 999999999999 标签策略，用于删除值

```
{
```

```
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@remove": [
                    "Development",
                    "Marketing"
                ],
                "enforced_for": {
                    "@@remove": [
                        "redshift:*",
                        "dynamodb:table"
                    ]
                }
            }
        }
    }
}
```

当策略 A、策略 C 和策略 D 合并以形成有效标签策略时，将策略 D 附加到账户 999999999999 具有以下效果：

- 假设您执行了前面的所有示例策略 B、C，并且 C 是 A 的子策略。策略 B 仅附加到 OU1，因此它对账户 9999999999999 没有任何影响。
- 对于账户 9999999999999，`CostCenter` 标签键的唯一可接受值是 `Support`。
- 不对 `CostCenter` 标签键强制执行合规性。

适用于账户 999999999999 的新有效标签策略

> **Note**
>
> 您不能直接将显示的有效策略的内容用作新策略的内容。语法不包括控制与其他子策略和父策略合并所需的运算符。展示的有效政策只是为了了解合并的结果。

```
{
    "tags": {
        "costcenter": {
```

```
            "tag_key": "CostCenter",
            "tag_value": [
                "Support"
            ]
        }
    }
}
```

如果您以后向 OU2 添加更多账户，其有效标签策略将与账户 999999999999 不同。这是因为限制性更强的策略 D 仅在账户级别附加，而不附加到 OU。

示例 4：限制对子策略的更改

在某些情况下，您可能希望限制子策略中的更改。此示例说明如何使用子控制运算符来执行此操作。

此示例从新的组织根标签策略开始，并假定标签策略尚未附加到组织实体。

策略 E – 用于限制子策略中的更改的组织根标签策略

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "Project"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance",
                    "Escalations"
                ]
            }
        }
    }
}
```

将策略 E 附加到组织根时，该策略会阻止子策略更改 `Project` 标签键。但是，子策略可以覆盖或附加标签值。

假定您随后将以下策略 F 附加到 OU。

策略 F – OU 标签策略

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": [
                    "Escalations - research"
                ]
            }
        }
    }
}
```

合并策略 E 和策略 F 会对 OU 的账户产生以下效果：

- 策略 F 是策略 E 的子策略。
- 策略 F 尝试更改案例处理，但无法完成。这是因为策略 E 为标签键包含了 `"@@operators_allowed_for_child_policies": ["@@none"]` 运算符。
- 但是，策略 F 可以为键附加标签值。这是因为策略 E 为标签值包含了 `"@@operators_allowed_for_child_policies": ["@@append"]`。

OU 中账户的有效策略

> **Note**
>
> 您不能直接将显示的有效策略的内容用作新策略的内容。语法不包括控制与其他子策略和父策略合并所需的运算符。展示的有效政策只是为了了解合并的结果。

```
{
    "tags": {
        "project": {
            "tag_key": "Project",
            "tag_value": [
                "Maintenance",
                "Escalations",
                "Escalations - research"
```

```
            ]
        }
    }
}
```

示例 5：与子控制运算符的冲突

附加到组织层次结构中同一级别的标签策略中可以存在子控制运算符。发生这种情况时，在合并策略以形成账户的有效策略时，使用允许运算符的交集。

假定策略 G 和策略 H 附加到组织根。

策略 G – 组织根标签策略 1

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance"
                ]
            }
        }
    }
}
```

策略 H – 组织根标签策略 2

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
            }
        }
    }
}
```

在此示例中，位于组织根的一个策略定义只能附加标签键的值。附加到组织根的另一个策略允许子策略附加和删除值。为子策略使用这两个权限的交集。结果是子策略可以附加值，但不能删除值。因此，子策略可以将值附加到标签值的列表，但不能删除 Maintenance 值。

示例 6：在相同层次结构级别附加值的冲突

您可以将多个标签策略附加到每个组织实体。执行此操作时，附加到同一组织实体的标签策略可能包含冲突的信息。将按照这些策略附加到组织实体的顺序来评估这些策略。要更改首先评估哪个策略，您可以分离策略，然后重新附加策略。

假定策略 J 第一个附加到组织根，然后将策略 K 附加到组织根。

策略 J – 附加到组织根的第一个标签策略

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
}
```

策略 K – 附加到组织根的第二个标签策略

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "project"
            }
        }
    }
}
```

在此示例中，标签键 PROJECT 在有效标签策略中使用，因为定义它的策略首先附加到组织根。

策略 JK – 账户的有效标签策略

账户的有效策略如下。

> **Note**
>
> 您不能直接将显示的有效策略的内容用作新策略的内容。语法不包括控制与其他子策略和父策略合并所需的运算符。展示的有效政策只是为了了解合并的结果。

```
{
    "tags": {
        "project": {
            "tag_key": "PROJECT",
            "tag_value": [
                "Maintenance"
            ]
        }
    }
}
```

AI 服务选择退出策略

AWS 人工智能（AI）服务（例如 Amazon Rekognition、Amazon CodeWhisperer、Amazon Transcribe 和 Contact Lens for Amazon Connect）可能会存储这些服务处理的客户内容并用于开发和持续改进其他 AWS 服务。作为 AWS 的客户，您可以选择不存储您的内容，或不将您的内容用于改进服务。

> **Note**
>
> 即便您拒绝 AWS 将您的数据用于改进服务，AWS 人工智能（AI）服务也可能需要存储您的内容才能提供服务。有关详细信息，请参阅您使用的 AI 服务的文档。

您可以配置一个组织策略，该策略在组织成员的所有账户上强制执行您的设置选择，而不必为每个 AWS 账户配置此设置。您可以选择退出内容存储，并将其用于单个 AI 服务，或同时用于所有覆盖的服务。您可以查询适用于每个账户的有效策略，以查看设置选择的效果。

> **Important**
>
> - 当您为服务指定“选择启用”或“选择退出”首选项时，该设置是全局设置并应用于所有AWS 区域。从一个AWS 区域设置值将复制到所有其他区域。

- 当您选择退出 AWS AI 服务所用的内容时，该服务将删除您设置该选项前与AWS关联的所有历史内容。此删除应当仅对非提供服务功能所必须的已存储数据生效。

AI 服务选择退出策略入门

请按照以下步骤操作，开始使用人工智能（AI）服务选择退出策略。

1. 为您的组织启用 AI 服务选择退出策略。
2. 创建 AI 服务选择退出策略。
3. 将 AI 服务选择退出策略附加到组织根、OU 或账户。
4. 查看应用于账户的合并的有效 AI 服务选择退出策略。

对于上述所有步骤，您必须以 AWS Identity and Access Management（IAM）用户的身份登录，担任 IAM 角色，或在组织的管理账户中以根用户的身份登录（不推荐）。

其他信息

- 了解 AI 服务选择退出策略的策略语法，并查看策略示例

创建、更新和删除 AI 服务选择退出策略

本主题内容：

- 为组织启用 AI 服务选择退出策略后，您可以创建策略。
- 当选择退出要求发生变化时，您可以更新现有策略。
- 当您不再需要策略并将其与所有组织部门（OU）和账户分离后，您可以删除策略。

创建 AI 服务选择退出策略

> **最小权限**
>
> 要创建 AI 服务选择退出策略，您需要运行以下操作的权限：
>
> - `organizations:CreatePolicy`

AWS Management Console

创建 AI 服务选择退出策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 AI services opt-out policies (AI 服务选择退出策略) 页面上，选择 Create policy (创建策略)。
3. 在 Create new AI services opt-out policy（创建新的 AI 服务选择退出策略）页面上，输入 Policy name（策略名称）和可选 Policy description（策略说明）。
4. （可选）您可以向策略添加一个或多个标签，方法是选择 Add tag (添加标签)，然后输入一个键和可选的值。将值留空，设置为空字符串；它并非 null。您最多可以向策略附加 50 个标签。有关更多信息，请参阅为 AWS Organizations 资源添加标签。
5. 输入策略文本或将其粘贴到 JSON 选项卡。有关 AI 服务选择退出策略语法的信息，请参阅AI 服务选择退出策略语法和示例。有关可用作起始点的策略的示例，请参阅AI 服务选择退出策略示例。
6. 编辑完策略后，选择位于页面右下角的 Create policy (创建策略)。

AWS CLI & AWS SDKs

创建 AI 服务选择退出策略

您可以使用以下方法之一来创建标签策略：

- AWS CLI：create-policy

1. 创建如下所示的 AI 服务选择退出策略，并将其存储在文本文件中。请注意，“optOut”和“optIn”区分大小写。

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
```

```
            }
        }
    }
}
```

此 AI 服务选择退出策略指定所有受策略影响的账户都选择退出除 Amazon Rekognition 之外的所有 AI 服务。

2. 导入 JSON 策略文件以在组织中创建新的策略。在本示例中，上一个 JSON 文件名为 `policy.json`。

```
$ aws organizations create-policy \
    --type AISERVICES_OPT_OUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign
\":\"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn
\"}}}}",
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "AISERVICES_OPT_OUT_POLICY"
        }
    }
}
```

- AWS SDK：CreatePolicy

后续操作

创建 AI 服务选择退出策略后，您可以使选择退出的选项生效。为此，您可以附加策略到组织根、组织部门（OU）、组织内的AWS 账户或所有这些项的组合。

更新 AI 服务选择退出策略

最小权限

要更新 AI 服务选择退出策略，您必须具有运行以下操作的权限：

- `organizations:UpdatePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。
- `organizations:DescribePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 Amazon Resource Name（ARN）（或“*”）。

AWS Management Console

更新 AI 服务选择退出策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 AI services opt-out policies (AI 服务选择退出策略) 页面上，选择要更新的策略的名称。
3. 在策略的详细信息页面上，选择 Edit policy (编辑策略)。
4. 您可以输入一个新的 Policy name (策略名称)、Policy description (策略说明)，或编辑 JSON 策略文本。有关 AI 服务选择退出策略语法的信息，请参阅AI 服务选择退出策略语法和示例。有关可用作起始点的策略的示例，请参阅AI 服务选择退出策略示例。
5. 完成更新策略后，选择保存更改。

AWS CLI & AWS SDKs

更新策略

您可以使用以下命令之一来更新策略：

- AWS CLI：update-policy

以下示例重命名 AI 服务选择退出策略。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
```

```
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

以下示例添加或更改 AI 服务选择退出策略的说明。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

以下示例更改附加到 AI 服务选择退出策略的 JSON 策略文档。在此示例中，内容取自一个名为 `policy.json` 的文件，使用以下文本：

```
{
    "services": {
        "default": {
            "opt_out_policy": {
```

```
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
         "Content": "{\n\"services\": {\n\"default\": {\n\"   ....TRUNCATED FOR
 BREVITY....    ": \"optIn\"\n}\n}\n}\n}\n"}
}
```

- AWS SDK：UpdatePolicy

编辑附加到 AI 服务选择退出策略的标签

当您登录到组织的管理账户时，您可以添加或删除附加到 AI 服务选择退出策略的标签。有关标记的更多信息，请参阅为 AWS Organizations 资源添加标签。

最小权限

要编辑附加到AWS组织中 AI 选择退出策略的标签，您必须拥有以下权限：

- `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
- `organizations:DescribePolicy` – 仅当使用 Organizations 控制台时才需要
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

编辑附加到 AI 服务选择退出策略的标签

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 AI services opt-out policies (AI 服务选择退出策略) 页面上，选择带有您想要编辑的标签的策略名称。
3. 在所选策略的详细信息页面上，选择 Tags (标签) 选项卡，然后选择 Manage tags (管理标签)。
4. 您可以在此页面上执行以下操作：
   - 编辑任何标签的值，方法是在旧标签上输入新值。您不能修改键。要更改键，您必须删除带有旧键的标签，然后添加使用新键的标签。
   - 删除任何现有的标签，方法是选择 Remove (删除)。
   - 添加新的标签键和值对。选择 Add tag (添加标签)，然后在提供的框中输入新的键名称和可选值。如果您将 Value (值) 框留空，则值是空字符串；它并非 `null`。
5. 在完成所有要进行的添加、删除和编辑操作之后，选择 Save changes (保存更改)。

AWS CLI & AWS SDKs

编辑附加到 AI 服务选择退出策略的标签

您可以使用以下命令之一编辑附加到 AI 服务选择退出策略的标签：

- AWS CLI：tag-resource 和 untag-resource
- AWS SDK：TagResource 和 UntagResource

删除 AI 服务选择退出策略

当登录到您组织的管理账户时，您可以删除您的组织中不再需要的策略。

必须先将某个策略从所有附加实体中分离，然后才能删除该策略。

> **最小权限**
>
> 要删除策略，您必须具有运行以下操作的权限：
>
> - `organizations:DescribePolicy`（仅限控制台 – 导航到策略）
> - `organizations:DeletePolicy`

AWS Management Console

删除 AI 服务选择退出策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 AI services opt-out policies (AI 服务选择退出策略) 页面上，选择要删除的策略的名称。
3. 要删除的策略必须先从所有根、OU 和账户分离。选择 Targets (目标) 选项卡，选择显示在 Targets (目标) 列表中的每个根、OU 或账户旁边的单选按钮，然后选择 Detach (分离)。在确认对话框中，选择 Detach (分离)。重复操作，直到删除所有目标。
4. 在页面的顶部，选择 Delete (删除)。
5. 在确认对话框上，输入策略的名称，然后选择 Delete (删除)。

AWS CLI & AWS SDKs

删除 AI 服务选择退出策略

您可以使用以下命令之一来删除策略：

- AWS CLI：delete-policy

  以下示例删除指定策略。仅当策略未附加到任何根、OU 或账户时，它们才有效。

```
$ aws organizations delete-policy \
```

```
    --policy-id p-i9j8k7l6m5
```

如果成功，此命令不会产生任何输出。

- AWS SDK：DeletePolicy

附加和分离 AI 服务选择退出策略

您可以在整个组织以及组织部门（OU）和单个账户上使用人工智能（AI）服务选择退出策略。AI 服务选择退出策略适用于什么取决于您将其附加到哪个组织元素：

- 将 AI 服务选择退出策略附加到组织根时，该策略将应用于该根的所有成员 OU 和账户。
- 将 AI 服务选择退出策略附加到 OU 时，该策略将应用于属于该 OU 或它的任何子 OU 的账户。这些账户还受附加到组织根的所有策略的约束。
- 当您将 AI 服务选择退出策略附加到某个账户时，该策略仅应用于该账户。该账户还受附加到组织根和该账户所属的所有 OU 的任何策略的约束。

该账户从根和父 OU 继承的所有 AI 服务选择退出策略以及直接附加到该账户的所有策略的聚合是有效策略。有关如何将策略合并为有效策略的信息，请参阅 了解管理策略继承。

> 最小权限
>
> 要附加 AI 服务选择退出策略，您必须具有运行以下操作的权限：
>
> - `organizations:AttachPolicy`

AWS Management Console

您可以导航到要附加策略的根、OU 或账户，为其附加 AI 服务选择退出策略。

通过导航到根、OU 或账户来附加 AI 服务选择退出策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，导航到要将策略附加到的根、OU 或账户的相应名称并选择其名称。您可能需要展开 OU（选择 ▶ ）以查找所需的 OU 或账户。

3. 在 Policies (策略) 选项卡上的 AI service opt-out policies (AI 服务选择退出策略) 条目中，选择 Attach (附加)。
4. 找到所需的策略，然后选择 Attach policy (附加策略)。

   Policies (策略) 选项卡上的附加的 AI 服务选择退出策略列表会更新，以包含新添加的内容。策略更改会立即生效。

通过导航到策略来附加 AI 服务选择退出策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 AI services opt-out policies (AI 服务选择退出策略) 页面上，选择要附加的策略的名称。
3. 在 Targets (目标) 选项卡上，选择 Attach (附加)。
4. 选择要附加策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OU（选择 ）以查找所需的 OU 或账户。
5. 选择 Attach policy（附上策略）。

   Targets (目标) 选项卡上的附加的 AI 服务选择退出策略列表会更新，以包含新添加的内容。策略更改会立即生效。

AWS CLI & AWS SDKs

将 AI 服务选择退出策略附加到组织根、OU 或账户

您可以使用以下方法之一附加 AI 服务选择退出策略：

- AWS CLI：attach-policy

  以下示例将策略附加到 OU。

```
$ aws organizations attach-policy \
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

  如果成功，此命令不会产生任何输出。

- AWS SDK：AttachPolicy

策略更改会立即生效。

分离 AI 服务选择退出策略

当您登录到组织的管理账户时，您可以从 AI 服务选择退出策略所附加到的组织根、OU 或账户分离策略。从某个实体分离 AI 服务选择退出策略后，该策略将不再应用于以前受现在已与之分离的实体影响的任何账户。要分离策略，请完成以下步骤。

> **最小权限**
>
> 要从组织根、OU 或账户分离 AI 服务选择退出策略，您必须具有运行以下操作的权限：
>
> - `organizations:DetachPolicy`

AWS Management Console

您可以导航到要分离策略的根、OU 或账户，为其分离 AI 服务选择退出策略。

通过导航到已附加策略的根、OU 或账户来分离 AI 服务选择退出策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面导航到要分离策略的根、OU 或账户。您可能需要展开 OU（选择 ▶ ）以查找所需的 OU 或账户。选择根、OU 或账户的名称。
3. 在 Policies (策略) 选项卡上，选择要分离的 AI 服务选择退出策略旁边的单选按钮，然后选择 Detach (分离)。
4. 在确认对话框中，选择 Detach policy (分离策略)。

   附加的 AI 服务选择退出策略的列表会更新。策略更改会立即生效。

通过导航到策略来分离 AI 服务选择退出策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 AI services opt-out policies (AI 服务选择退出策略) 页面上，选择要从根、OU 或账户分离的策略的名称。

3. 在 Targets (目标) 选项卡上，选择要分离策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OU（选择 ▶ ）以查找所需的 OU 或账户。
4. 选择分离。
5. 在确认对话框中，选择 Detach (分离)。

   附加的 AI 服务选择退出策略的列表会更新。策略更改会立即生效。

AWS CLI & AWS SDKs

将 AI 服务选择退出策略从组织根、OU 或账户中分离

您可以使用以下方法之一分离 AI 服务选择退出策略：

- AWS CLI：detach-policy

  以下示例将策略与 OU 分离。

  ```
  $ aws organizations detach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  如果成功，此命令不会产生任何输出。
- AWS SDK：DetachPolicy

策略更改会立即生效。

查看有效的 AI 服务选择退出策略

确定组织中的账户存在有效人工智能（AI）服务选择退出策略。

什么是有效的 AI 服务选择退出策略？

有效的 AI 服务选择退出政策指定应用到AWS 账户的最终规则。它是账户继承的任何 AI 服务选择退出策略与直接附加到账户的任何 AI 服务选择退出策略的聚合。将 AI 服务选择退出策略附加到组织根时，它应用到组织中的所有账户。将 AI 服务选择退出策略附加到 OU 时，它应用到属于该 OU 的所有账户和 OU。将策略直接附加到某个账户时，它仅应用到这一个AWS 账户。

例如，附加到组织根的 AI 服务选择退出策略可能指定组织中的所有账户选择退出所有AWS机器学习服务。直接附加到一个成员账户的单独 AI 服务选择退出策略指定它只为 Amazon Rekognition 选择启用内容使用服务。这些 AI 服务选择退出策略的组合构成了有效的 AI 服务选择退出策略。结果是，组织中的所有账户都选择退出所有AWS服务，但选择启用 Amazon Rekognition 的一个账户除外。

有关如何将策略组合到最终有效策略中的信息，请参阅了解管理策略继承。

如何查看 AI 服务选择退出策略

您可以从 AWS Management Console、AWS API 或 AWS Command Line Interface 查看账户的有效 AI 服务选择退出策略。

最小权限

若要查看账户的有效 AI 服务选择退出策略，您必须具有运行以下操作的权限：

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要

AWS Management Console

查看账户的有效 AI 服务选择退出策略的步骤

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，选择要查看其有效 AI 服务选择退出策略的账户的名称。您可能需要展开 OU（选择 ）以查找所需的账户。
3. 在 Policies (策略) 选项卡上的 AI services opt-out policies (AI 服务选择退出策略) 部分，选择 View the effective AI policy for this AWS 账户 (查看此亚马逊云科技账户的有效 AI 策略)。

   控制台显示应用于指定账户的有效策略。

> **Note**
>
> 如果没有重大更改，您无法复制和粘贴有效策略并将其用作其他 AI 服务选择退出策略的 JSON。AI 服务选择退出策略文档必须包含继承运算符，这些运算符指定如何将每个设置合并到最终有效策略中。

AWS CLI & AWS SDKs

查看账户的有效 AI 服务选择退出策略的步骤

您可以使用以下方法之一查看有效 AI 服务选择退出策略：

- AWS CLI：describe-effective-policy

  以下示例显示了账户的有效 AI 服务选择退出策略。

```
$ aws organizations describe-effective-policy \
    --policy-type AISERVICES_OPT_OUT_POLICY \
    --target-id 123456789012
{
    "EffectivePolicy": {
        "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":
\"optOut\"},   ....TRUNCATED FOR BREVITY....   "opt_out_policy\":\"optIn\"}}}",
        "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
        "TargetId": "123456789012",
        "PolicyType": "AISERVICES_OPT_OUT_POLICY"
    }
}
```

- AWS SDK：DescribeEffectivePolicy

AI 服务选择退出策略语法和示例

本主题介绍人工智能（AI）服务选择退出策略语法并提供示例。

AI 服务选择退出策略的语法

AI 服务选择退出策略是一个纯文本文件，根据 JSON 的规则设置结构。AI 服务选择退出策略的语法遵循管理策略类型的语法。有关该语法的完整讨论，请参阅了解管理策略继承。本主题重点介绍如何将该常规语法应用于 AI 服务选择退出策略类型的特定要求。

> **Important**
>
> 本部分中讨论的值的大写十分重要。使用大写和小写字母输入值，如本主题所示。如果您使用意外的大写，则策略不起作用。

以下策略显示了基本的 AI 服务选择退出策略语法。如果此示例直接附加到账户，则该账户将被明确选择退出一个服务，然后选择启用另一个服务。从更高级别（OU 或根策略）继承的策略可以选择启用或选择退出其他服务。

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

设想附加到组织根的以下策略示例。它设置组织选择退出所有 AI 服务的默认设置。这将自动包括任何未明确豁免的 AI 服务，包括 AWS 可能会在以后部署的任何 AI 服务。您可以将子策略附加到 OU 或直接附加到账户，以覆盖除 Amazon Comprehend 之外的任何 AI 服务的此设置。以下示例中的第二个条目使用 `@@operators_allowed_for_child_policies` 将该设置设为 `none` 以防止覆盖。示例中的第三个条目在整个组织范围内为 Amazon Rekognition 提供豁免。它在整个组织中选择启用该服务，但策略确实允许在适当的情况下覆盖子策略。

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
```

```
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

AI 服务选择退出策略语法包括以下元素：

- `services` 元素。AI 服务选择退出策略由此固定名称标识为最外层包含元素的 JSON。

  AI 服务选择退出策略可以在 `services` 元素下拥有一个或多个语句。每个语句包含以下元素：

  - 标识 AWS AI 服务的服务名称密钥。以下键名称是此字段的有效值：
    - **`default`** – 代表所有当前可用的 AI 服务，并隐式和自动包括将来可能添加的任何 AI 服务。
    - `awssupplychain`
    - `chimesdkvoiceanalytics`
    - `cloudwatch`
    - `codeguruprofiler`
    - `codewhisperer`
    - `comprehend`
    - `connectamd`
    - `connectoptimization`
    - `contactlens`
    - `datazone`
    - `entityresolution`
    - `frauddetector`
    - `glue`
    - `guardduty`
    - `lex`
    - `polly`

- q
- quicksightq
- rekognition
- securitylake
- textract
- transcribe
- translate

由服务名称键标识的每个策略语句都可以包含以下元素：

- opt_out_policy 密钥。此键必须存在。这是您可以放置在服务名称键下的唯一键。

  opt_out_policy 键仅包含具有以下值之一的 @@assign 运算符：

  - optOut – 您可以选择退出指定 AI 服务的内容使用。
  - optIn – 您可以选择启用指定 AI 服务的内容使用。

  > **注意**
  >
  > - 您不能在 AI 服务选择退出策略中使用 @@append 和 @@remove 继承运算符。
  > - 您不能在 AI 服务选择退出策略中使用 @@enforced_for 运算符。

- 在任何级别上，您都可以指定 @@operators_allowed_for_child_policies 运算符来控制子策略可以执行哪些操作来覆盖父策略施加的设置。可以指定以下值之一：

  - @@assign – 此策略的子策略可以通过 @@assign 运算符使用其他值来覆盖继承值。
  - @@none – 此策略的子策略不能更改该值。

  @@operators_allowed_for_child_policies 的行为取决于您放置它的位置。您可以使用以下位置：

  - services 键下 – 控制子策略是否可以添加或更改有效策略中的服务列表。
  - 在特定 AI 服务的键或 default 键下 – 控制子策略是否可以添加或更改此特定条目下的键列表。
  - 特定服务的 opt_out_policies 键下 – 控制子策略是否只能更改此特定服务的设置。

AI 服务选择退出策略示例

下面的示例策略仅供参考。

示例 1：选择退出组织中所有账户的所有 AI 服务

以下示例显示了一个策略，您可以将该策略附加到组织的根，以选择退出组织中的账户的 AI 服务。

> **Tip**
>
> 如果您使用示例右上角的复制按钮复制以下示例，则副本不包括行号。它已准备好粘贴。

```
    | {
    |     "services": {
[1] |         "@@operators_allowed_for_child_policies": ["@@none"],
    |         "default": {
[2] |             "@@operators_allowed_for_child_policies": ["@@none"],
    |             "opt_out_policy": {
[3] |                 "@@operators_allowed_for_child_policies": ["@@none"],
    |                 "@@assign": "optOut"
    |             }
    |         }
    |     }
    | }
```

- [1] – services 下的 "@@operators_allowed_for_child_policies": ["@@none"] 会阻止任何子策略为单个服务添加除已存在 default 部分之外的任何新部分。Default 是表示“所有 AI 服务”的占位符。
- [2] – default 下的 "@@operators_allowed_for_child_policies": ["@@none"] 会阻止任何子策略添加除已存在 opt_out_policy 部分之外的任何新部分。
- [3] – opt_out_policy 下的 "@@operators_allowed_for_child_policies": ["@@none"] 会阻止子策略更改 optOut 设置的值或添加任何其他设置。

示例 2：为所有服务设置组织默认设置，但允许子策略覆盖单个服务的设置

以下示例策略为所有 AI 服务设置了组织范围内的默认设置。default 的值阻止子策略更改 optOut 服务的 default 值，它是所有 AI 服务的占位符。如果通过将此策略附加到根策略或 OU 而将其作为父策略应用，则子策略仍然可以更改单个服务的选择退出设置，如第二个策略所示。

- 因为 services 键没有 "@@operators_allowed_for_child_policies": ["@@none"]，子策略可以为单个服务添加新部分。

- default 下的 "@@operators_allowed_for_child_policies": ["@@none"] 会阻止任何子策略添加除已存在 opt_out_policy 部分之外的任何新部分。
- opt_out_policy 下的 "@@operators_allowed_for_child_policies": ["@@none"] 会阻止子策略更改 optOut 设置的值或添加任何其他设置。

组织根用户 AI 服务选择退出父策略

```
{
    "services": {
        "default": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        }
    }
}
```

以下示例策略假定上一个示例策略已附加到组织根或父 OU，并且您将此示例附加到受父策略影响的账户。它会覆盖默认的选择退出设置，并明确仅选择启用 Amazon Lex 服务。

AI 服务选择退出子策略

```
{
    "services": {
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

由此产生的有效政策 AWS 账户 是，账户只能选择加入 Amazon Lex，而选择退出所有其他 AWS AI 服务，因为继承了父政策的default选择退出设置。

示例 3：为单个服务定义组织范围内的 AI 服务选择退出策略

以下示例显示了 AI 服务选择退出策略，该策略定义了单个 AI 服务的 `optOut` 设置。如果此策略附加到组织的根，则会阻止任何子策略覆盖此服务的 `optOut` 设置。此策略不涉及其他服务，但可能会受到其他 OU 或账户中的子策略的影响。

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

备份策略

AWS Backup 使您能够创建备份计划，并定义如何备份AWS资源。计划中的规则包括各种设置，例如备份频率、进行备份的时段、包含要备份的资源的AWS 区域以及存储备份的文件库。然后，您可以将备份计划应用于使用标签标识的 AWS 资源组。您还必须标识一个 AWS Identity and Access Management（IAM）角色，该角色授予 AWS Backup 代表您执行备份操作的权限。

AWS Organizations 中的备份策略将所有这些部分合并到 JSON 文本文档中。您可以将备份策略附加到组织结构中的任何元素，例如根、组织部门（OU）和单个账户。Organizations 应用继承规则来合并组织根、任何父 OU 中的策略，或合并附加到账户的策略。这将为每个账户生成有效备份策略。此有效策略将指示 AWS Backup 如何自动备份您的 AWS 资源。

备份策略使您能够精确地控制在组织需要的任何级别上备份资源。例如，您可以在附加到组织根的策略中指定必须备份所有 Amazon DynamoDB 表。此策略可以包含默认备份频率。然后，您可以将一个备份策略附加到 OU，此策略根据每个 OU 的要求覆盖此备份频率。例如，`Developers` OU 可能指定每周一次的备份频率，而 `Production` OU 指定每天一次。

您可以创建部分备份策略，这些策略分别只包含成功备份资源所需的部分信息。您可以将这些策略附加到组织树的不同部分（例如根或父 OU），以便这些部分策略由较低级别的 OU 和账户继承。当 Organizations 通过使用继承规则合并账户的所有策略时，生成的有效策略必须具有所有必需元素。否则 AWS Backup 将认为该策略无效且不备份受影响的资源。

> **Important**
>
> AWS Backup 只有在被具有所有必需元素的完整 有效策略调用时才能成功执行备份。虽然前面所述的部分策略可以起作用，但如果某个账户的有效策略不完整，则会生成错误或未成功备份的资源。作为备选策略，请考虑要求所有备份策略本身都完整且有效。使用层次结构中较高的附加策略提供的默认值，并通过包括继承子控制运算符在子策略中根据需要覆盖这些默认值。

组织中每个AWS 账户的有效备份计划在 AWS Backup 控制台中显示为该账户的不可变计划。您可以查看该计划，但不能更改。

当 AWS Backup 基于策略创建的备份计划开始备份时，您可以在 AWS Backup 控制台中查看备份作业的状态。成员账户中的用户可以查看该成员账户中的备份作业的状态和任何错误。如果您还启用对 AWS Backup 的信任服务访问，则组织管理账户中的用户可以查看组织中所有备份作业的状态和错误。有关更多信息，请参阅《AWS Backup 开发人员指南》中的启用跨账户管理。

备份策略入门

请按照以下步骤开始使用备份策略。

1. 了解执行备份策略任务所必须具备的权限。
2. 了解我们在使用备份策略时建议的一些最佳实践。
3. 为您的组织启用备份策略。
4. 创建备份策略。
5. 将备份策略附加到组织根、OU 或账户。
6. 查看应用于账户的合并的有效备份策略。

对于上述所有步骤，您必须以 IAM 用户的身份登录，担任 IAM 角色，或在组织的管理账户中以根用户的身份登录（不推荐）。

其他信息

- 了解备份策略语法并查看示例策略

管理备份策略的先决条件和权限

本页介绍在 AWS Organizations 中管理备份策略的先决条件和所需的权限。

主题

管理备份策略的先决条件

要管理组织中的备份策略，需要满足以下条件：

- 您的组织必须已启用所有功能。
- 您必须登录到组织的管理账户。
- 您的 AWS Identity and Access Management（IAM）用户或角色必须具备以下部分中列出的权限。

管理备份策略的权限

以下 IAM 策略示例提供了管理组织中备份策略的所有方面的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageBackupPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
```

```
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

有关 IAM 策略与权限的更多一般信息，请参阅 IAM 用户指南。

使用备份策略的最佳实践

AWS 推荐以下使用备份策略的最佳实践。

决定备份策略

您可以创建不完整的备份策略，然后继承并合并这些策略以便为每个成员账户生成完整的策略。这样做后，如果您在一个级别进行更改，而没有仔细考虑该更改对该级别以下的所有账户的影响，则最终会出现有效策略不完整的风险。为防止出现这种情况，我们建议您改为确保在所有级别实施的备份策略本身完整。将父策略视为可由子策略中指定的设置覆盖的默认策略。这样，即使子策略不存在，继承的策略也是完整的，并使用默认值。您可以使用子控制继承运算符来控制可以添加到子策略、由子策略更改或删除的设置。

使用 **GetEffectivePolicy** 验证对备份策略的更改

更改备份策略后，请检查有效策略中低于您进行更改的级别的代表账户。您可以使用 AWS Management Console 查看有效策略，或者使用 GetEffectivePolicy API 操作或其 AWS CLI 或 AWS SDK 变体之一来查看有效策略。确保您所做的更改对有效策略产生预期影响。

简单开始并进行一些小更改

要简化调试，请先从简单策略开始，然后一次更改一个项目。在进行下一个更改之前，验证每个更改的行为和影响。此方法可以减少出现错误或意外结果时必须考虑的变量数量。

将备份的副本存储在其他AWS 区域和您组织中的账户中

为了增强灾难恢复能力，您可以存储备份的副本。

- 其他区域 – 如果您将备份的副本存储在其他AWS 区域，这有助于保护备份，防止原始区域中的意外损坏或删除。使用策略的 copy_actions 部分，在运行备份计划的同一账户的一个或多个区域中指定文件库。若要执行此操作，请在指定要在其中存储备份副本的备份文件库的 ARN 时，使用 $account 变量来识别账户。$account 变量会在运行时自动替换为运行备份策略的账户 ID。
- 其他账户 – 如果您将备份的副本存储在其他AWS 账户中，您可以添加一个安全屏障，以帮助防止恶意行为者损害您的某个账户。使用策略的 copy_actions 部分，在组织中的一个或多个账户中指定文件库，该账户与运行备份计划的账户分开。若要执行此操作，请在指定要在其中存储备份副本的备份文件库的 ARN 时，使用其实际账户 ID 号来识别账户。

限制每个策略的计划数量

包含多个计划的策略的问题排查更加复杂，因为必须全部验证的输出数量更多。相反，让每个策略包含一个且只有一个备份计划，以简化调试和问题排查。然后，您可以添加别的具有其他计划的策略以满足其他要求。此方法有助于将某个计划的任何问题隔离到一个策略中，并防止这些问题使其他策略及其计划的问题的排查复杂化。

使用堆栈套创建所需的备份文件库和 IAM 角色

使用与 Organizations 的 AWS CloudFormation 堆栈套集成可以在您组织的每个成员账户中自动创建所需的备份文件库和 AWS Identity and Access Management（IAM）角色。您可以创建一个堆栈套，其中包括您希望在组织的每个AWS 账户中自动可用的资源。此方法使您能够在运行备份计划时确保已满足依赖关系。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的创建具有自行管理权限的堆栈套。

通过查看在每个账户中创建的第一个备份来检查您的结果

当您对策略进行一项更改时，请检查该更改后创建的下一个备份，以确保该更改产生了预期的影响。此步骤不仅仅是保证有效策略，而且还可以确保 AWS Backup 按照预期的方式解释您的策略并实施备份计划。

创建、更新和删除备份策略

本主题内容：

- 为组织启用备份策略后，您可以创建策略。
- 当备份要求发生变化时，您可以更新现有策略。
- 当您不再需要策略并将其与所有组织部门（OU）和账户分离后，您可以删除策略。

创建备份策略

最小权限

要创建备份策略，您需要运行以下操作的权限：

- `organizations:CreatePolicy`

AWS Management Console

您可以通过以下两种方式之一在 AWS Management Console 中创建备份策略：

- 可视化编辑器，允许您选择选项并为您生成 JSON 策略文本。
- 文本编辑器，允许您自己直接创建 JSON 策略文本。

可视化编辑器使过程变得简单，但会限制您的灵活性。这是创建您的第一批策略并使其习惯使用的好方法。了解策略的工作原理并开始受到可视化编辑器所提供功能的限制之后，您可以通过自己编辑 JSON 策略文本将高级功能添加到策略中。可视化编辑器仅使用 @@assign 值设置运算符，不提供对子控制运算符的任何访问权限。只有在手动编辑 JSON 策略文本时，才能添加子控制运算符。

创建备份策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Backup policies (备份策略) 页面上，选择 Create policy (创建策略)。
3. 在 Create policy (创建策略) 页面上，输入策略的 Policy name (策略名称) 和可选 Policy description (策略说明)。
4. （可选）您可以向策略添加一个或多个标签，方法是选择 Add tag (添加标签)，然后输入一个键和可选的值。将值留空，设置为空字符串；它并非 `null`。您最多可以向策略附加 50 个标签。有关标记的更多信息，请参阅为 AWS Organizations 资源添加标签。
5. 您可以使用可视化编辑器构建策略，如此过程中所述。您也可以在 JSON 选项卡中输入或粘贴策略文本。有关备份策略语法的信息，请参阅备份策略语法和示例。

   如果选择使用可视化编辑器，请选择适合您的场景的备份选项。备份计划由三部分组成。有关这些备份计划元素的更多信息，请参阅《AWS Backup 开发人员指南》中的创建备份计划和分配资源。

a. Backup 计划一般详细信息

- 备份文计划名称只能由字母数字、连字符和下划线字符组成。
- 您必须从列表中至少选择一个备份计划区域。该计划只能备份所选AWS 区域。

b. 一个或多个指定 AWS Backup 的操作方式和时间的备份规则。每个备份规则定义以下项目：

- 包含备份频率和可以进行备份的时间窗口的计划。
- 要使用的备份文件库的名称。备份文件库名称只能由字母数字、连字符和下划线字符组成。备份文件库必须存在，才能成功运行计划。可以使用 AWS Backup 控制台或 AWS CLI 命令创建文件库。
- （可选）一个或多个复制到区域规则，以同时将备份复制到其他AWS 区域中的文件库。
- 一个或多个标签键值对，要附加到每次运行此备份计划时创建的备份恢复点。
- 生命周期选项，它们指定备份过渡到冷存储的时间以及备份到期时间。

选择 Add rule (添加规则) 将您需要的每个规则添加到计划中。

有关备份规则的更多信息，请参阅《AWS Backup 开发人员指南》中的备份规则。

c. 一种资源分配，它指定 AWS Backup 应使用此计划备份的资源。该分配是通过指定 AWS Backup 用于查找和匹配资源的标签对来制定的

- 资源分配名称只能由字母数字、连字符和下划线字符组成。
- 为 AWS Backup 指定 IAM 角色，用于按其名称执行备份。

  在控制台中，您不能指定整个 Amazon Resource Name（ARN）。必须同时包含角色名称及其指定角色类型的前缀。前缀通常是 `role` 或者 `service-role`，且它们用正斜杠（“/”）与角色名称分隔。例如，您可以输入 `role/MyRoleName` 或者 `service-role/MyManagedRoleName`。当存储在底层 JSON 中时，这将转换为完整 ARN。

  > **Important**
  >
  > 指定的 IAM 角色必须已存在于应用策略的账户中。如果不存在，则备份计划可能会成功启动备份作业，但这些备份作业将失败。

- 指定一个或多个资源标签键和标签值对来确定要备份的资源。如果有多个标签值，请用逗号分隔它们。

选择 Add assignment (添加分配)，将每个已配置的资源分配添加到备份计划。

有关更多信息，请参阅《AWS Backup 开发人员指南》中的将资源分配给备份计划。

6. 创建完策略后，选择 Create policy (创建策略)。该策略将显示在可用备份策略的列表中。

AWS CLI & AWS SDKs

创建备份策略

您可以使用以下方法之一创建备份策略：

- AWS CLI：create-policy

  将备份计划创建为类似于以下内容的 JSON 文本，并将其存储在文本文件中。有关语法的完整规则，请参阅备份策略语法和示例。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                }
            },
            "selections": {
```

```
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

此备份计划指定 AWS Backup 应备份受影响的AWS 账户中的所有资源，这些资源位于指定AWS 区域且标签 dataType 的值为 PII。

接下来，导入 JSON 策略文件备份计划以在组织中创建新的备份策略。记下输出中策略 ARN 末尾的策略 ID。

```
$ aws organizations create-policy \
    --name "MyBackupPolicy" \
    --type BACKUP_POLICY \
    --description "My backup policy" \
    --content file://policy.json{
    "Policy": {
        "PolicySummary": {
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
            "Description": "My backup policy",
            "Name": "MyBackupPolicy",
            "Type": "BACKUP_POLICY"
        }
        "Content": "...a condensed version of the JSON policy document you
 provided in the file...",
    }
}
```

- AWS SDK：CreatePolicy

后续操作

创建备份策略后，您可以使策略生效。为此，您可以附加策略到组织根、组织部门（OU）、组织内的 AWS 账户或所有这些项的组合。

更新备份策略

登录到组织的管理账户后，您可以编辑需要在组织中进行更改的策略。

> **最小权限**
>
> 要更新备份策略，您必须具有运行以下操作的权限：
>
> - `organizations:UpdatePolicy`，且同一条策略语句中有一个 `Resource` 元素包含要更新的策略的 ARN（或“*”）
> - `organizations:DescribePolicy`，且同一条策略语句中有一个 `Resource` 元素包含要更新的策略的 ARN（或“*”）

AWS Management Console

更新备份策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Backup policies (备份策略) 页面上，选择要更新的策略的名称。
3. 选择编辑策略。
4. 您可以输入一个新的 Policy name (策略名称)、Policy description (策略说明)。您可以通过使用可视化编辑器或通过直接编辑 JSON 来更改策略内容。
5. 完成更新策略后，选择保存更改。

AWS CLI & AWS SDKs

更新备份策略

您可以使用以下命令之一来更新备份策略：

- AWS CLI：update-policy

以下示例重命名备份策略。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

以下示例添加或更改备份策略的说明。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
       "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

以下示例更改附加到备份策略的 JSON 策略文档。在此示例中，内容取自一个名为 `policy.json` 的文件，使用以下文本：

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

```
$ aws organizations update-policy \
```

```
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
}
```

- AWS SDK：UpdatePolicy

编辑附加到备份策略的标签

当您登录到组织的管理账户时，您可以添加或删除附加到备份策略的标签。有关标记的更多信息，请参阅为 AWS Organizations 资源添加标签。

> 最小权限
>
> 要编辑附加到AWS组织中备份策略的标签，您必须拥有以下权限：
>
> - organizations:DescribeOrganization（仅限控制台 – 导航到策略）
> - organizations:DescribePolicy（仅限控制台 – 导航到策略）
> - organizations:TagResource
> - organizations:UntagResource

AWS Management Console

编辑附加到备份策略的标签

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。

2. Backup policies (备份策略) 页
3. 选择具有要修改的标签的策略名称。

   此时将显示策略详细信息页面。
4. 在 Tags (标签) 选项卡上，选择 Manage tags (管理标签)。
5. 您可以在此页面上执行以下操作：

   - 编辑任何标签的值，方法是在旧标签上输入新值。您不能修改键。要更改键，您必须删除带有旧键的标签，然后添加使用新键的标签。
   - 删除任何现有的标签，方法是选择 Remove (删除)。
   - 添加新的标签键和值对。选择 Add tag (添加标签)，然后在提供的框中输入新的键名称和可选值。如果您将 Value (值) 框留空，则值是空字符串；它并非 null。
6. 在完成所有要进行的添加、删除和编辑操作之后，选择 Save changes (保存更改)。

AWS CLI & AWS SDKs

编辑附加到备份策略的标签

您可以使用以下命令之一编辑附加到备份策略的标签：

- AWS CLI：tag-resource 和 untag-resource
- AWS SDK：TagResource 和 UntagResource

删除备份策略

当登录到您组织的管理账户时，您可以删除您的组织中不再需要的策略。

必须先将某个策略从所有附加实体中分离，然后才能删除该策略。

> 最小权限
>
> 要删除策略，您必须具有运行以下操作的权限：
>
> - `organizations:DeletePolicy`，且同一条策略语句中有一个 `Resource` 元素包含要删除的策略的 ARN（或“*”）

AWS Management Console

删除备份策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Backup policies (备份策略) 页面上，选择要删除的备份策略。
3. 要删除的备份策略必须先从所有根、OU 和账户分离。选择 Targets (目标) 选项卡，选择显示在 Targets (目标) 列表中的每个根、OU 或账户旁边的单选按钮，然后选择 Detach (分离)。在确认对话框中，选择 Detach (分离)。重复操作，直到删除所有目标。
4. 在页面的顶部，选择 Delete (删除)。
5. 在确认对话框上，输入策略的名称，然后选择 Delete (删除)。

AWS CLI & AWS SDKs

删除备份策略

您可以使用以下命令之一来删除策略：

- AWS CLI：delete-policy

  以下示例删除指定策略。仅当策略未附加到任何根、OU 或账户时，它们才有效。

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  如果成功，此命令不会产生任何输出。

- AWS SDK：DeletePolicy

附加和分离备份策略

您可以在整个组织以及组织部门 (OU) 和单个账户上使用备份策略。请记住以下几点：

- 将备份策略附加到组织根 时，该策略将应用于该根的所有成员 OU 和账户。
- 将备份策略附加到 OU 时，该策略将应用于属于该 OU 或它的任何子 OU 的账户。这些账户还受附加到组织根的所有策略的约束。

- 当您将备份策略附加到某个账户时，该策略仅应用于该账户。该账户还受附加到组织根和该账户所属的所有 OU 的任何策略的约束。

该账户从根和父 OU 继承的所有备份策略以及直接附加到该账户的所有策略的聚合是有效策略。有关如何将策略合并为有效策略的信息，请参阅 了解管理策略继承。

附加备份策略

登录到组织的管理账户后，您可以将备份策略附加到组织根、OU 或直接附加到账户。

> 最小权限
>
> 要附加备份策略，您必须具有运行以下操作的权限：
>
> - `organizations:AttachPolicy`

AWS Management Console

您可以导航到要附加策略的根、OU 或账户，为其附加备份策略。

通过导航到根、OU 或账户来附加备份策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，导航到要将策略附加到的根、OU 或账户的相应名称并选择其名称。您可能需要展开 OU（选择 ▶ ）以查找所需的 OU 或账户。
3. 在 Policies (策略) 选项卡上的 Backup policies (备份策略) 中，选择 Attach (附加)。
4. 找到所需的策略，然后选择 Attach policy (附加策略)。

   Policies (策略) 选项卡上的附加的备份策略列表会更新，以包含新添加的内容。策略更改会立即生效。

通过导航到策略来附加备份策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。

2. 在 Backup policies (备份策略) 页面上，选择要附加的策略的名称。
3. 在 Targets (目标) 选项卡上，选择 Attach (附加)。
4. 选择要附加策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OU（选择 ▶ ）以查找所需的 OU 或账户。
5. 选择 Attach policy（附上策略）。

   Targets (目标) 选项卡上的附加的备份策略列表会更新，以包含新添加的内容。策略更改会立即生效。

AWS CLI & AWS SDKs

将备份策略附加到组织根、OU 或账户

可以使用以下命令之一附加备份策略：

- AWS CLI：attach-policy

```
$ aws organizations attach-policy \
    --target-id 123456789012 \
    --policy-id p-i9j8k7l6m5
```

- AWS SDK：AttachPolicy

策略更改会立即生效。

分离备份策略

当您登录到组织的管理账户时，您可以从备份策略所附加到的组织根、OU 或账户分离策略。从某个实体分离备份策略后，该策略将不再应用于以前受现在已与之分离的实体影响的任何账户。要分离策略，请完成以下步骤。

> **最小权限**
>
> 要从组织根、OU 或账户分离备份策略，您必须具有运行以下操作的权限：
>
> - `organizations:DetachPolicy`

AWS Management Console

您可以导航到要分离策略的根、OU 或账户，为其分离备份策略。

通过导航到已附加策略的根、OU 或账户来分离备份策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面导航到要分离策略的根、OU 或账户。您可能需要展开 OU（选择 ▶ ）以查找所需的 OU 或账户。选择根、OU 或账户的名称。
3. 在 Policies (策略) 选项卡上，选择要分离的备份策略旁边的单选按钮，然后选择 Detach (分离)。
4. 在确认对话框中，选择 Detach policy (分离策略)。

   附加的备份策略的列表将更新。策略更改会立即生效。

通过导航到策略来分离备份策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Backup policies (备份策略) 页面上，选择要从根、OU 或账户分离的策略的名称。
3. 在 Targets (目标) 选项卡上，选择要分离策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OU（选择 ▶ ）以查找所需的 OU 或账户。
4. 选择分离。
5. 在确认对话框中，选择 Detach (分离)。

   附加的备份策略的列表将更新。策略更改会立即生效。

AWS CLI & AWS SDKs

从组织根、OU 或账户分离备份策略

可以使用以下命令之一分离备份策略：

- AWS CLI：detach-policy

以下示例将策略与 OU 分离。

```
$ aws organizations detach-policy \
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

如果成功，此命令不会产生任何输出。

- AWS SDK：DetachPolicy

策略更改会立即生效。

查看有效备份策略

您可以从AWS管理控制台、AWS API，或AWS命令行界面查看账户的有效备份策略。以下部分简要概述了有效备份策略，其中包含示例。

什么是有效备份策略？

有效备份策略指定应用于AWS 账户的最终备份计划设置。它是账户继承的任何备份策略与直接附加到账户的任何备份策略的聚合。将备份策略附加到组织根时，它应用到组织中的所有账户。将备份策略附加到组织部门（OU）时，它应用到属于该 OU 的所有账户和 OU。将策略直接附加到某个账户时，它仅应用到这一个AWS 账户。

例如，附加到组织根的备份策略可能指定组织中的所有账户以每周一次的默认备份频率备份所有 Amazon DynamoDB 表。直接附加到一个成员账户的单独备份策略（在表中包含关键信息）可以用每天一次的值覆盖该频率。这些备份策略的组合构成有效备份策略。该有效备份策略是为组织中的每个账户单独确定的。此示例中的结果是，组织中的所有账户每周备份一次自己的 DynamoDB 表，但有一个账户每天备份它的表。

有关如何将备份策略组合到最终有效备份策略中的信息，请参阅了解管理策略继承。

查看有效备份策略

您可以使用AWS Management Console、AWS API 或 AWS Command Line Interface 查看账户的有效备份策略。

> **最小权限**
>
> 要查看账户的有效备份策略，您必须具有运行以下操作的权限：

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要

AWS Management Console

查看账户的有效备份策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，选择要查看其有效备份策略的账户的名称。您可能需要展开 OU（选择 ）以查找所需的账户。
3. 在 Policies (策略) 选项卡上的 Backup policies (备份策略) 部分，选择 View the effective backup policy for this AWS 账户 (查看此亚马逊云科技账户的有效备份策略)。

   控制台显示应用于指定账户的有效策略。

   > **Note**
   >
   > 如果没有重大更改，您无法复制和粘贴有效策略并将其用作其他备份策略的 JSON。备份策略文档必须包含继承运算符，指定如何将每个设置合并到最终有效策略中。

AWS CLI & AWS SDKs

查看账户的有效备份策略

您可以使用以下命令之一查看有效备份策略：

- AWS CLI：describe-effective-policy

  以下示例显示备份策略的详细信息。

```
$ aws organizations describe-effective-policy \
--policy-type BACKUP_POLICY \
--target-id 123456789012{
    "EffectivePolicy": {
        "LastUpdatedTimestamp": "2020-06-22T14:31:50.748000-07:00",
```

```
        "TargetId": "123456789012",
        "PolicyType": "BACKUP_POLICY",
        "PolicyContent": "{\"plans\":{\"pii_backup_plan\":{\"regions\":[\"ap-
northeast-2\",\"us-east-1\",\"eu-north-1\"],\
"selections\":{\"tags\":{\"datatype\":{\"iam_role_arn\":\"arn:aws:iam::
$account:role/MyIamRole\",\"tag_value\":[\"PII\"],\
"tag_key\":\"dataType\"}}},\"rules\":{\"hourly\":{\"complete_backup_window_minutes
\":\"10080\",\"target_backup_vault_name\
":\"FortKnox\",\"start_backup_window_minutes\":\"480\",\"schedule_expression\":
\"cron(0 5/1 ? * * *)\",\"lifecycle\":{\"mo
ve_to_cold_storage_after_days\":\"180\",\"delete_after_days\":\"270\"},
\"copy_actions\":{\"arn:aws:backup:us-east-1:$accou
nt:backup-vault:secondary-vault\":{\"lifecycle\":
{\"move_to_cold_storage_after_days\":\"10\",\"delete_after_days\":\"100\"
}}}}}}}"
    }
}
```

- AWS SDK：DescribeEffectivePolicy

使用 AWS CloudTrail 事件监控组织中的备份策略

您可以使用 AWS CloudTrail 事件来监控何时创建、更新或从 AWS 组织的任何账户中删除备份策略，或者何时存在无效的组织备份计划。有关更多信息，请参阅《AWS Backup 开发人员指南》中的记录跨账户管理事件。

备份策略语法和示例

本页介绍备份策略语法并提供示例。

备份策略的语法

备份策略是一个纯文本文件，根据 JSON 的规则设置结构。备份策略的语法遵循所有管理策略类型的语法。有关该语法的完整讨论，请参阅管理策略类型的策略语法和继承。本主题重点介绍如何将该常规语法应用于备份策略类型的特定要求。

备份策略的这一部分是备份计划及其规则。备份策略中备份计划的语法在结构上与使用的语法相同 AWS Backup，但密钥名称不同。 AWS Organizations 在下面对策略密钥名称的描述中，每个名称都包含等效的 AWS Backup 计划密钥名称。有关 AWS Backup 套餐的更多信息，请参阅CreateBackupPlan《AWS Backup 开发人员指南》。

> **Note**
>
> 使用 JSON 时，重复的密钥名称将被拒绝。如果您想在单个策略中包含多个计划、规则或选项，请确保每个密钥的名称都是唯一的。

有效备份策略要完整而实用，必须不仅仅包括备份计划及其时间安排和规则。该策略还必须确定要备份的 AWS 区域 和资源，以及 AWS Backup 可用于执行备份的 AWS Identity and Access Management (IAM) 角色。

以下功能完整的策略显示了基本备份策略语法。如果此示例直接关联到账户，则 AWS Backup 会备份该账户在us-east-1和eu-north-1区域中标签值dataType为PII或的所有资源RED。它每天上午 5:00 将这些资源备份到 My_Backup_Vault 中，同时将副本存储在 My_Secondary_Vault 中。这两个文件库与资源位于同一个账户中。它还会将备份的副本存储在另一个明确指定的账户中的 My_Tertiary_Vault 中。这些文件库必须已经存在于每个接收有效策略 AWS 区域 的指定文件库中。 AWS 账户 如果任何备份资源都是 EC2 实例，则会对这些实例上的备份启用对 Microsoft 卷影复制服务（VSS）的支持。该备份将标签 Owner:Backup 应用到每个恢复点。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "rules": {
                "My_Hourly_Rule": {
                    "schedule_expression": {"@@assign": "cron(0 5 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "complete_backup_window_minutes": {"@@assign": "604800"},
                    "enable_continuous_backup": {"@@assign": false},
                    "target_backup_vault_name": {"@@assign": "My_Backup_Vault"},
                    "recovery_point_tags": {
                        "Owner": {
                            "tag_key": {"@@assign": "Owner"},
                            "tag_value": {"@@assign": "Backup"}
                        }
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "delete_after_days": {"@@assign": "270"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault": {
```

```
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        },
                        "arn:aws:backup:us-east-1:$account:backup-
vault:My_Tertiary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
east-1:111111111111:backup-vault:My_Tertiary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        }
                    }
                }
            },
            "regions": {
                "@@append": [
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "selections": {
                "tags": {
                    "My_Backup_Assignment": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
```

```
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {"@@assign": "enabled"}
                }
            },
            "backup_plan_tags": {
                "stage": {
                    "tag_key": {"@@assign": "Stage"},
                    "tag_value": {"@@assign": "Beta"}
                }
            }
        }
    }
}
```

备份策略语法包括以下组件：

- $account 变量 – 在策略的某些文本字符串中，可以使用 $account 变量来表示当前 AWS 账户。在有效策略中 AWS Backup 运行计划时，它会自动将此变量替换为有效策略及其计划正在运行的当前 AWS 账户 变量。

  > **Important**
  >
  > 您只能在可以包含 Amazon Resource Name（ARN）的策略元素中使用 $account 变量，例如指定要存储备份的备份文件库的元素或具有执行备份的权限的 IAM 角色。

  例如，以下内容要求该策略适用的每个文件库中都 AWS 账户 必须My_Vault存在名为的文件库。

  ```
  arn:aws:backup:us-west-2:$account:vault:My_Vault"
  ```

  我们建议您使用 AWS CloudFormation 堆栈集及其与 Organizations 的集成，为组织中的每个成员账户自动创建和配置备份库和 IAM 角色。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的创建具有自行管理权限的堆栈套。

- 继承运算符 – 备份策略可以同时使用继承值设置运算符和子控制运算符。

- plans

  策略的顶级键是 plans 键。在策略文件顶部，备份策略必须始终以此固定键名称开头。在此键下，您可以有一个或多个备份计划。

- plans 顶级键下的每个计划都有一个由用户分配的备份计划名称组成的键名称。在前面的示例中，备份计划名称为 PII_Backup_Plan。一个策略中可以有多个计划，每个计划都有自己的 rules、regions、selections 和 tags。

  备份策略中的此备份计划密钥名称映射到 AWS Backup 计划中该BackupPlanName密钥的值。

  每个计划可以包含以下元素：

  - rules – 此键包含规则集合。每个规则都转换为一个计划任务，其中包含有效备份策略中由 selections 和 regions 元素标识的资源的开始时间和时段。
  - regions— 此密钥包含一个数组列表，其中列出了此策略可以备份 AWS 区域 其资源。
  - selections – 此键包含一个或多个按指定 rules 备份的资源集合（在指定的 regions 内）。
  - advanced_backup_settings – 此键包含特定于在某些资源上运行的备份的设置。
  - backup_plan_tags – 此键指定附加到备份计划本身的标签。
- rules

  rules 策略键映射到 AWS Backup 计划中的 Rules 键。rules 键下可以有一个或多个规则。每个规则都会成为执行选定资源备份的计划任务。

  每个规则都包含一个其名称是规则名称的键。在前一个示例中，规则名称为“My_Hourly_Rule”。规则键的值是以下规则元素集合：

  - schedule_expression— 此策略密钥映射到 AWS Backup 计划中的ScheduleExpression密钥。

    指定备份的开始时间。此键包含@@assign继承值运算符和带有 CRON 表达式的字符串值，该表达式指定何时 AWS Backup 启动备份作业。CRON 字符串的一般格式为：“cron( )”。每一项都是一个数字或通配符。例如，cron(0 5 ? * 1,3,5 *) 表示在每个星期一、星期三和星期五的上午 5 点开始备份。cron(0 0/1 ? * * *) 表示在每周中的每天中的每小时开始一次备份。
  - target_backup_vault_name— 此策略密钥映射到 AWS Backup 计划中的TargetBackupVaultName密钥。

    指定要在其中存储备份的备份文件库的名称。您可以通过使用来创造价值 AWS Backup。此键包含 @@assign 继承值运算符和一个具有文件库名称的字符串值。

    > **Important**
    >
    > 首次启动备份计划时，该文件库必须已存在。我们建议您使用 AWS CloudFormation 堆栈集及其与 Organizations 的集成，为组织中的每个成员账户自动创建和配置备份库和 IAM

角色。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的创建具有自行管理权限的堆栈集。

- `start_backup_window_minutes`— 此策略密钥映射到 AWS Backup 计划中的`StartWindowMinutes`密钥。

  （可选）指定在取消未成功启动的作业之前等待的分钟数。此键包含 @@assign 继承值运算符和一个具有整数分钟数的值。

- `complete_backup_window_minutes` – 此策略键映射到 AWS Backup 计划中的 `CompletionWindowMinutes` 键。

  （可选）指定备份作业成功启动之后到备份作业必须完成或由 AWS Backup取消之前的分钟数。此键包含 @@assign 继承值运算符和一个具有整数分钟数的值。

- `enable_continuous_backup`— 此策略密钥映射到 AWS Backup 计划中的`EnableContinuousBackup`密钥。

  （可选）指定是否 AWS Backup 创建连续备份。 `True`导致创建 AWS Backup 能够 point-in-time 恢复的连续备份 (PITR)。 `False`（或未指定）创建快照备份的原因 AWS Backup 。

  > **Note**
  >
  > 由于启用 PITR 的备份最多可以保留 35 天，因此如果设置了以下选项之一，您必须选择 `False` 或不指定值：
  >
  > - 将 `delete_after_days` 设置为大于 35。
  > - 将 `move_to_cold_storage_after_days` 设置为任何值。

  有关连续备份的更多信息，请参阅《AWS Backup 开发人员指南》中的 P re oint-in-time co very。

- `lifecycle`— 此策略密钥映射到 AWS Backup 计划中的`Lifecycle`密钥。

  （可选）指定何 AWS Backup 时将此备份转换为冷存储以及何时过期。

  - `move_to_cold_storage_after_days` — 此策略密钥映射到 AWS Backup 计划中的`MoveToColdStorageAfterDays`密钥。

    指定备份发生之后到 AWS Backup 将恢复点移到冷存储之前的天数。此键包含 @@assign 继承值运算符和一个具有整数天数的值。

  - ~~`delete_after_days`— 此策略密钥映射到 AWS Backup 计划中的`DeleteAfterDays`密钥。~~

指定备份发生之后到 AWS Backup 删除恢复点之前的天数。此键包含 @@assign 继承值运算符和一个具有整数天数的值。如果将备份过渡到冷存储，则备份必须至少保持冷存储 90 天，因此该值必须至少比 move_to_cold_storage_after_days 值多 90 天。

- copy_actions— 此策略密钥映射到 AWS Backup 计划中的CopyActions密钥。

  （可选）指定 AWS Backup 应将备份复制到一个或多个其他位置。每个备份副本位置描述如下：

  - 其名称唯一标识此复制操作的键。目前，键名称必须是备份文件库的 Amazon Resource Name（ARN）。此键包含两个条目。
    - target_backup_vault_arn – 此策略键映射到 AWS Backup 计划中的 DestinationBackupVaultArn 键。

      （可选）指定 AWS Backup 存储额外备份副本的存储库。此键的值包含 @@assign 继承值运算符和文件库的 ARN。

      - 要在中 AWS 账户 引用运行备份策略的文件库，请使用 ARN 中的$account变量代替账户 ID 号。 AWS Backup 运行备份计划时，它会自动将变量替换为运行策略 AWS 账户 的账户 ID 号。这样，当备份策略应用于组织中的多个账户时，备份就可以正确运行。
      - 要在同一组织内的不同 AWS 账户 中引用文件库，请使用 ARN 中的实际账户 ID 号。

      > **Important**
      >
      > - 如果缺少此键，则使用父键名称中所有小写版本的 ARN。由于 ARN 区分大小写，因此此字符串可能与故障的实际 ARN 不匹配，因此计划失败。为此，我们建议您始终提供此键和值。
      > - 首次启动备份计划时，您希望复制的备份文件库必须已存在。我们建议您使用 AWS CloudFormation 堆栈套及其与 Organizations 的集成，为组织中的每个成员账户自动创建和配置备份文件库和 IAM 角色。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的创建具有自行管理权限的堆栈套。

    - lifecycle— 此策略密钥映射到 AWS Backup 计划中CopyAction密Lifecycle钥下的密钥。

      （可选）指定何 AWS Backup 时将此备份副本转换为冷存储以及何时过期。

      - move_to_cold_storage_after_days – 此策略键映射到 AWS Backup 计划中的 MoveToColdStorageAfterDays 键。

指定备份后在将恢复点 AWS Backup 移至冷存储之前的天数。此键包含 @@assign 继承值运算符和一个具有整数天数的值。

- delete_after_days – 此策略键映射到 AWS Backup 计划中的 DeleteAfterDays 键。

  指定备份发生后在 AWS Backup 删除恢复点之前的天数。此键包含 @@assign 继承值运算符和一个具有整数天数的值。如果将备份过渡到冷存储，则备份必须至少保持冷存储 90 天，因此该值必须至少比 move_to_cold_storage_after_days 值多 90 天。

- recovery_point_tags— 此策略密钥映射到 AWS Backup 计划中的RecoveryPointTags密钥。

  （可选）指定 AWS Backup 附加到根据该计划创建的每个备份的标签。此键的值包含以下一个或多个元素：

  - 此键名称和值对的标识符。recovery_point_tags 下的每个元素的此名称都是全部小写的标签键名称，即使 tag_key 具有不同的大小写处理方式也是如此。此标识符不 区分大小写。在前一个示例中，此键对由名称 Owner 标识。每个键对都包含以下元素：

    - tag_key – 指定要附加到备份计划的标签键名称。此键包含 @@assign 继承值运算符和一个字符串值。 值区分大小写。
    - tag_value：指定附加到备份计划并与 tag_key 关联的值。此键包含任何继承值运算符以及一个或多个要在有效策略中替换、追加或删除的值。这些值区分大小写。

- regions

  regions策略密钥指定 AWS 区域 在哪些资源中 AWS Backup 查找与selections密钥中的条件相匹配的资源。此键包含任何继承值运算符以及 AWS 区域 代码的一个或多个字符串值，例如：["us-east-1", "eu-north-1"]。

- selections

  selections 策略键指定由此策略中的计划规则备份的资源。此键大致对应于中的BackupSelection对象 AWS Backup。资源由匹配标签键名称和值的查询指定。selections 键下面包含一个键 – tags。

  - tags – 指定标识资源以及具有查询和备份资源权限的 IAM 角色的标签。此键的值包含以下一个或多个元素：

    - 此标签元素的标识符。tags 下的此标识符是全部小写的标签键名称，即使要查询的标签具有不同的大小写处理方式也是如此。此标识符不 区分大小写。在前一个示例中，一个元素是由名称 My_Backup_Assignment 标识的。tags 下的每个标识符都包含以下元素：

- `iam_role_arn` – 指定有权访问资源（由 `regions` 键指定的 AWS 区域 中的标签查询标识）的 IAM 角色。此值包含@@assign继承值运算符和包含角色的 ARN 的字符串值。 AWS Backup 使用此角色查询和发现资源以及执行备份。

  您可以使用 ARN 中的 `$account` 变量来代替账户 ID 号。当备份计划由运行时 AWS Backup，它会自动将变量替换为运行该策略的实际账户 ID 号。 AWS 账户

  > **Important**
  >
  > 首次启动备份计划时，该角色必须已存在。我们建议您使用 AWS CloudFormation 堆栈集及其与 Organizations 的集成，为组织中的每个成员账户自动创建和配置备份库和 IAM 角色。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的创建具有自行管理权限的堆栈套。

- `tag_key` – 指定要搜索的标签键名称。此键包含 @@assign 继承值运算符和一个字符串值。值区分大小写。
- `tag_value`— 指定必须与匹配的键名关联的值`tag_key`。 AWS Backup 只有当`tag_key`和都`tag_value`匹配时，才会将资源包含在备份中。此键包含任何继承值运算符以及一个或多个要在有效策略中替换、追加或删除的值。这些值区分大小写。

- `advanced_backup_settings` – 指定特定备份方案的设置。此键包含一个或多个设置。每个设置都是一个 JSON 对象字符串，其中包含以下元素：
  - 对象键名称 – 一个字符串，它指定应用以下高级设置的资源类型。
  - 对象值 – 一个 JSON 对象字符串，包含特定于关联资源类型的一个或多个备份设置。

  目前，唯一支持的高级备份设置为在 Amazon EC2 实例上运行的，为 Windows 或 SQL Server 启用的 Microsoft 卷影复制服务（VSS）备份。键名称必须是 `"ec2"` 资源类型，而值指定在这些 Amazon EC2 实例上执行备份时 `"windows_vss"` 支持为 `enabled` 或 `disabled`。有关此功能的更多信息，请参阅《AWS Backup 开发人员指南》中的创建启用 VSS 的 Windows Backup。

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
    }
}
```

- backup_plan_tags – 指定附加到备份计划本身的标签。这不会影响任何规则或选择中指定的标签。

  （可选）您可以将标签附加到备份计划。此键的值是元素的集合。

  backup_plan_tags 下的每个元素的键名称都是全部小写的标签键名称，即使要查询的标签具有不同的大小写处理方式也是如此。此标识符不 区分大小写。这些条目中的每一个条目的值都由以下键组成：

  - tag_key – 指定要附加到备份计划的标签键名称。此键包含 @@assign 继承值运算符和一个字符串值。此值区分大小写。
  - tag_value：指定附加到备份计划并与 tag_key 关联的值。此键包含 @@assign 继承值运算符和一个字符串值。此值区分大小写。

备份策略示例

下面的示例备份策略仅供参考。在以下某些示例中，可能会压缩 JSON 空白格式以节省空间。

示例 1：分配给父节点的策略

以下示例显示了分配给账户的父节点之一的备份策略。

父策略 – 此策略可以附加到组织根，或附加到作为所有预期账户父级的任何 OU。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "480"
                    },
```

```
                    "complete_backup_window_minutes": {
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                }
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                }
                            }
```

```
                        }                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {
                        "@@assign": "enabled"
                    }
                }
            }
        }
    }
}
```

如果账户没有继承或附加其他保单，则每个适用政策中提供的有效政策如下例所 AWS 账户示。CRON 表达式会使备份每小时运行一次。账户 ID 123456789012 将是每个账户的实际账户 ID。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
```

```
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
```

```
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": "enabled"
                }
            }
        }
    }
}
```

示例 2：父策略与子策略合并

在以下示例中，继承的父级策略和子级策略要么继承，要么直接附加到 AWS 账户 合并，形成有效的策略。

父策略 – 此策略可以附加到组织根或任何父 OU。

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "to_delete_after_days": { "@@assign": "180" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "to_delete_after_days": { "@@assign": "180" }
                            }
                        }
                    }
```

```
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII", "RED" ] }
                    }
                }
            }
        }
    }
}
```

子策略 – 此策略可以直接附加到账户，或附加到父策略所附加到的级别以下的任何级别的 OU。

```
{
    "plans": {
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "to_delete_after_days": { "@@assign": "365" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "to_delete_after_days": { "@@assign": "365" }
                            }
```

```
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "MonthlyDatatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                        "tag_key": { "@@assign": "BackupType" },
                        "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                    }
                }
            }
        }
    }
}
```

生成的有效策略 – 应用于账户的有效策略包含两个计划，每个计划都有自己的规则集以及要应用这些规则的资源集。

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
```

```
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
                    }
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "to_delete_after_days": "365"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "monthlydatatype": {
```

```
                        "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                        "tag_key": "BackupType",
                        "tag_value": [ "MONTHLY", "RED" ]
                    }
                }
            }
        }
    }
}
```

示例 3：父策略阻止子策略进行任何更改

在以下示例中，继承的父策略使用子控制运算符强制执行所有设置，并防止它们被子策略更改或覆盖。

父策略 – 此策略可以附加到组织根或任何父 OU。策略的每个节点都存在 `"@@operators_allowed_for_child_policies": ["@@none"]` 意味着，子策略不能对计划进行任何类型的更改。子策略也不能将其他计划添加到有效策略。此策略将成为其附加到的每个 OU 以及 OU 下的账户的有效策略。

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
```

```
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "to_delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "to_delete_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "180"
                                }
                            }
                        }
                    }
                }
            },
            "selections": {
```

```
                "@@operators_allowed_for_child_policies": ["@@none"],
                "tags": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "datatype": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "iam_role_arn": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "ec2": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "windows_vss": {
                        "@@assign": "enabled",
                        "@@operators_allowed_for_child_policies": ["@@none"]
                    }
                }
            }
        }
    }
}
```

生成的有效策略 – 如果存在任何子备份策略，则会忽略这些策略，而父策略将成为有效策略。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
```

```
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "to_delete_after_days": "180"
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
    }
}
```

示例 4：父策略阻止子策略对一个备份计划进行更改

在以下示例中，继承的父策略使用子控制运算符强制执行单个计划的设置，并防止它们被子策略更改或覆盖。子策略仍然可以添加其他计划。

父策略 – 此策略可以附加到组织根或任何父 OU。此示例与前一个示例类似，所有子继承运算符都被阻止，但 plans 顶级处除外。该级别的 @@append 设置使子策略能够将其他计划添加到有效策略中的集合。对继承计划的任何更改仍被阻止。

为清楚起见，截断了计划中的相应部分。

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        }
    }
}
```

子策略 – 此策略可以直接附加到账户，或附加到父策略所附加到的级别以下的任何级别的 OU。此子策略定义一个新计划。

为清楚起见，截断了计划中的相应部分。

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

生成的有效策略 – 有效策略包括这两个计划。

```
{
```

```
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

示例 5：子策略覆盖父策略中的设置

在以下示例中，子策略使用值设置运算符来覆盖从父策略继承的某些设置。

父策略 – 此策略可以附加到组织根或任何父 OU。子策略可以覆盖任何设置，因为在没有阻止子策略的子控制运算符的情况下，默认行为是允许子策略执行 @@assign、@@append 或 @@remove。父策略包含有效备份计划所需的所有元素，因此，如果它按原样继承，则会成功备份您的资源。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "lifecycle": {
                        "to_delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:t2": {
```

```
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "to_delete_after_days": {"@@assign": "180"}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
    }
}
```

子策略 – 子策略仅包含需要与继承的父策略不同的设置。必须有一个继承的父策略，该策略在合并到有效策略时提供其他所需设置。否则，有效备份策略会包含无效的备份计划，无法按预期备份您的资源。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
```

```
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "to_delete_after_days": {"@@assign": "365"}
                    }
                }
            }
        }
    }
}
```

生成的有效策略 – 有效策略包括来自这两个策略的设置，由子策略提供的设置将覆盖从父级继承的设置。在此示例中，将发生以下更改：

- 区域列表替换为完全不同的列表。如果要将区域添加到继承的列表中，请在子策略中使用 @@append 而不是 @@assign。
- AWS Backup 每隔一小时执行一次，而不是每小时执行一次。
- AWS Backup 允许开始备份的时间为 80 分钟，而不是 60 分钟。
- AWS Backup 使用保Default管库而不是FortKnox。
- 向冷存储转移和最终删除备份的生命周期都会延长。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
```

```
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

标签策略

您可以使用标签策略来维护一致的标签，包括标签键和标签值的首选大小写处理。

标签是什么？

标签 是您分配的自定义属性标签，或者是 AWS 分配给 AWS 资源的标签。每个标签具有两个部分：

- 标签键（例如，CostCenter、Environment 或 Project）。标签键区分大小写。
- 一个称为标签值 的可选字段（例如，111122223333 或 Production）。省略标签值与使用空字符串效果相同。与标签键一样，标签值区分大小写。

本页的其余部分描述了标签策略。有关标签的更多信息，请参阅以下资源：

- 有关标签的一般信息，包括命名和使用惯例，请参阅《标记AWS资源用户指南》。
- 有关支持使用标签的服务的列表，请参阅《Resource Groups 标记 API 参考》。
- 有关使用标签对资源进行分类的信息，请参阅《标记AWS资源的最佳实践》白皮书。
- 有关标记 Organizations 资源的信息，请参阅为 AWS Organizations 资源添加标签。
- 有关在其他AWS服务中标记资源的信息，请参阅该服务的文档。

什么是标签策略？

标签策略 是策略的一种类型，可帮助您在组织账户中跨资源标准化标签。在标签策略中，您可以指定在标记资源时适用于资源的标记规则。

例如，标签策略可以指定当 `CostCenter` 标签附加到资源时，它必须使用标签策略定义的大小写处理和标签值。标签策略还可以指定在指定资源类型上强制执行 不合规的标记操作。换句话说，阻止在指定的资源类型上完成不合规的标记操作。不会评估未标记的资源或未在标签策略中定义的标签是否符合标签策略。

使用标签策略涉及使用多个 AWS 服务：

- 使用 AWS Organizations 管理标签策略。登录到组织的管理账户时，您可以使用 Organizations 启用标签策略功能。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。然后，您可以创建标签策略并将其附加到组织实体，以使这些标记规则生效。
- 使用 AWS Resource Groups 管理与标签策略的合规性。登录组织中的账户时，您可以使用 Resource Groups 查找账户中资源的不合规标签。您可以在创建资源的 AWS 服务中更正不合规的标签。

  如果您登录组织的管理账户，则可以查看组织所有账户的合规性信息。

标签策略仅在启用所有功能的组织中可用。有关使用标签策略所需条件的更多信息，请参阅管理标签策略的先决条件和权限。

> **Important**
>
> 要开始使用标签策略，AWS 强烈建议您先按照标签策略入门中介绍的示例工作流操作，再继续使用更多高级标签策略。在将标签策略扩展到整个 OU 或组织之前，最好了解将一个简单标签策略附加到单个账户的效果。在强制实施 与任何标签策略的合规性之前，了解某个标签策略的影响尤为重要。标签策略入门页面上的表还提供了更多高级策略相关任务的说明的链接。

管理标签策略的先决条件和权限

本页介绍了在 AWS Organizations 中管理标签策略的先决条件和所需的权限。

主题

管理标签策略的先决条件

使用标签策略需要满足以下条件：

- 您的组织必须已启用所有功能。
- 您必须登录到组织的管理账户。
- 您需要管理标签策略的权限中列出的权限。

要评估标签策略的合规性，请使用 AWS Resource Groups。有关评估合规性的要求的信息，请参阅《AWS Resource Groups 用户指南》中的先决条件和权限。

管理标签策略的权限

以下示例 IAM 策略提供了用于管理标签策略的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageTagPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribePolicy",
                "organizations:ListRoots",
                "organizations:DisableAWSServiceAccess",
                "organizations:DetachPolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DisablePolicyType",
```

```
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListPolicies",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:UpdatePolicy",
                "organizations:EnablePolicyType",
                "organizations:DescribeOrganizationalUnit",
                "organizations:AttachPolicy",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:CreatePolicy",
                "organizations:DescribeCreateAccountStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

有关 IAM 策略与权限的更多信息，请参阅 IAM 用户指南。

使用标签策略的最佳实践

AWS为使用标签策略推荐以下最佳实践。

确立标签大小写策略

确定您希望如何设定标签的大小写并在所有资源类型中一致地实施该策略。例如，决定是使用 `Costcenter`、`costcenter` 还是 `CostCenter`，以及是否对所有标签使用相同的约定。为了在合规性报告中获得一致的结果，请避免使用具有不一致大小写处理的类似标签。此策略将帮助您定义组织的标签策略。

使用推荐的工作流程

从小事开始做，创建一个简单的标签策略。然后将其附加到用于测试用途的会员账户。使用标签策略入门中描述的工作流。

确定标记规则

这将取决于您组织的需求。例如，建议您指定当 `CostCenter` 标签附加到 AWS Secrets Manager 密钥时，它必须使用指定的大小写处理。创建定义合规标签的标签策略，并将其附加到希望这些标记规则生效的组织实体。

培训账户管理员

当您准备扩展标签策略的使用时，请按照以下方式对账户管理员进行培训：

- 沟通您的标签策略。
- 强调管理员需要对特定资源类型使用标签。

  这一点很重要，因为未标记的资源在合规性结果中不会显示为不合规。
- 提供有关使用标签策略检查合规性的指导。指导管理员使用《AWS Resource Groups 用户指南》中评估账户的合规性内所述的过程寻找并纠正其账户内资源的不合规标签错误。告知他们您希望的合规性检查频率。

在强制执行合规性时要谨慎

强制执行合规性可能会阻止组织账户中的用户标记他们所需的资源。查看了解强制执行中的信息。另请参阅标签策略入门中描述的工作流。

考虑创建 SCP 以围绕资源创建请求设置防护机制

从未附加标签的资源在报告中不会显示为不合规。账户管理员仍然可以创建未标记的资源。在某些情况下，您可以使用服务控制策略 (SCP) 来设置有关资源创建请求的防护机制。有关 SCP 的示例，请参阅 需要在指定的已创建资源上使用标签。如需了解 AWS 服务是否支持使用标签控制访问权限，请参阅《IAM 用户指南》中的使用 IAM 的 AWS 服务。在基于标签的授权列中查找标为 Yes (是) 的服务。选择服务名称以查看该服务的授权和访问控制文档。

标签策略入门

使用标签策略涉及使用多个 AWS 服务。要开始使用，请查看以下页面。然后按照此页面上的工作流来熟悉标签策略及其效果。

- 管理标签策略的先决条件和权限
- 使用标签策略的最佳实践

首次使用标签策略

首次使用标签策略时，请按照以下步骤开始。

任务	要登录的账户	AWS 要使用的服务控制台
步骤 1：为您的组织启用标签策略。	组织的管理账户。[1]	AWS Organizations
步骤 2：创建标签策略。 保持第一个标签策略简单。输入您要使用的一个大小写处理标签键，并将所有其他选项保留为默认值。	组织的管理账户。[1]	AWS Organizations
步骤 3：将标签策略附加到可用于测试的单个成员账户。 在下一步中您需要登录此账户。	组织的管理账户。[1]	AWS Organizations
步骤 4：创建一些具有合规标签的资源，以及一些具有不合规标签的资源。	您用于测试目的的成员账户。	任何您满意的 AWS 服务。例如，您可以使用 AWS Secrets Manager 并按照创建基本密钥中的过程创建具有合规和不合规密钥的密钥。
步骤 5：查看有效标签策略并评估账户的合规性状态。	您用于测试目的的成员账户。	R esource AWS Groups 和创建资源的服务。 如果您创建了具有合规和不合规标签的资源，则应在结果中看到不合规标签。
步骤 6：重复查找和纠正合规性问题的过程，直到测试账户中的资源均符合标签策略。	您用于测试目的的成员账户。	R esource AWS Groups 和创建资源的服务。

任务	要登录的账户	AWS 要使用的服务控制台
您可以随时评估组织级的合规性。	组织的管理账户。[1]	资源组

[1] 您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。

扩大标签策略的使用

您可以按任意顺序执行以下任务以扩展标签策略的使用范围。

高级任务	要登录的账户	AWS 要使用的服务控制台
创建更多高级标签策略。 遵循与初次用户相同的流程，但尝试其他任务。例如，定义其他键或值，或为标签键指定不同的大小写处理。 您可以使用了解管理策略继承和标签策略语法中的信息创建更详细的标签策略。	组织的管理账户。[1]	AWS Organizations
将标签策略附加到其他账户或 OU。 在将更多策略附加到账户或账户是其成员的任何 OU 之后，检查账户的有效标签策略。	组织的管理账户。[1]	AWS Organizations
创建 SCP，以便在任何人创建新资源时要求标签。有关示例，请参阅 需要在指定的已创建资源上使用标签。	组织的管理账户。[1]	AWS Organizations

高级任务	要登录的账户	AWS 要使用的服务控制台
当账户更改时，继续根据有效标签策略评估账户的合规性状态。更正不合规标签。	具有有效标签策略的成员账户。	R esource AWS Groups 和创建资源的服务。
评估组织级的合规性。	组织的管理账户。[1]	资源组

[1] 您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。

首次强制执行标签策略

要首次强制执行标签策略，请遵循类似于首次使用标签策略使用测试账户的工作流。

> **Warning**
>
> 在强制执行合规性时要谨慎。请确保您了解使用标签策略的效果并遵循推荐的工作流。在将强制执行扩展到更多账户之前，在测试账户中测试强制执行的影响。否则，您可能会阻止组织账户中的用户标记他们所需的资源。有关更多信息，请参阅 了解强制执行。

强制执行任务	要登录的账户	AWS 要使用的服务控制台
步骤 1：创建标签策略。 保持第一个强制执行的标签策略简单。输入您要使用的一个大小写处理标签键，然后选择 Prevent noncompliant operations for this tag (防止此标签的不合规操作) 选项。然后指定要在其上强制执行的资源类型。继续我们之前的例子，您可以选择在 Secrets Manager 密钥上强制执行它。	组织的管理账户。[1]	AWS Organizations

强制执行任务	要登录的账户	AWS 要使用的服务控制台
步骤 2：将标签策略附加到单个测试账户。	组织的管理账户。[1]	AWS Organizations
步骤 3：尝试创建一些具有合规标签的资源，一些具有不合规标签的资源。不允许在标签策略中指定的带有不兼容标签类型的资源上创建标签。	您用于测试目的的成员账户。	任何您满意的 AWS 服务。例如，您可以使用 AWS Secrets Manager 并按照创建基本密钥中的过程创建具有合规和不合规密钥的密钥。
步骤 4：根据有效标签策略评估账户的合规性状态，并更正不合规的标签。	您用于测试目的的成员账户。	Resource AWS Groups 和创建资源的服务。
步骤 5：重复查找和纠正合规性问题的过程，直到测试账户中的资源均符合标签策略。	您用于测试目的的成员账户。	R esource AWS Groups 和创建资源的服务。
您可以随时评估组织级的合规性。	组织的管理账户。[1]	资源组

[1] 您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。

创建、更新和删除标签策略

本主题内容：

- 为组织启用标签策略后，您可以创建策略。
- 当标记要求发生变化时，您可以更新现有策略。
- 当您不再需要策略并将其与所有组织部门（OU）和账户分离后，您可以删除策略。

> **Important**
>
> 未标记的资源不会在结果中显示为不合规。

创建标签策略

> **最小权限**
>
> 要创建标签策略，您需要运行以下操作的权限：
>
> - `organizations:CreatePolicy`

您可以通过以下两种方式之一在 AWS Management Console 中创建标签策略：

- 可视化编辑器，允许您选择选项并为您生成 JSON 策略文本。
- 文本编辑器，允许您自己直接创建 JSON 策略文本。

可视化编辑器使过程变得简单，但会限制您的灵活性。这是创建您的第一批策略并使其习惯使用的好方法。了解策略的工作原理并开始受到可视化编辑器所提供功能的限制之后，您可以通过自己编辑 JSON 策略文本将高级功能添加到策略中。可视化编辑器仅使用 @@assign 值设置运算符，不提供对子控制运算符的任何访问权限。只有在手动编辑 JSON 策略文本时，才能添加子控制运算符。

AWS Management Console

创建标签策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Tag policies (标签策略) 页面上，选择 Create policy (创建策略)。
3. 在 Create policy (创建策略) 页面上，输入策略的 Policy name (策略名称) 和可选 Policy description (策略说明)。
4. （可选）您可以向策略对象本身添加一个或多个标签。这些标签不是策略的一部分。为此，请选择 Add tag (添加标签)，然后输入键和可选值。将值留空，设置为空字符串；它并非 `null`。您最多可以向策略附加 50 个标签。有关更多信息，请参阅为 AWS Organizations 资源添加标签。
5. 您可以使用可视化编辑器构建标签策略，如此过程中所述。您也可以在 JSON 选项卡中键入或粘贴标签策略。有关标签策略语法的信息，请参阅标签策略语法。

   对于 New tag key (新标签键 1)，指定要添加的标签键的名称。
6. 对于 Tag key capitalization compliance (标签键大小写合规性)，请保留此选项（默认值）以指定继承的父标签策略（如果存在）应定义标签键的大小写处理。

如果要使用此策略规定标签键的特定大写，请启用此选项。如果选择此选项，则您为 Tag Key (标签键) 指定的大小写将覆盖继承的父策略中指定的大小写处理。

如果父策略不存在且您没有启用此选项，则仅全小写字符的标签键将被视为符合要求。有关从父策略继承的更多信息，请参阅了解管理策略继承。

> **Tip**
>
> 在创建定义标签键及其大小写处理的标签策略时，请考虑使用示例 1：定义组织级的标签键大小写中显示的示例标签策略作为指南。将其附加到组织根。稍后，您可以创建其他标记策略并将其附加到 OU 或账户，以创建其他标记规则。

7. 对于 Tag value compliance (标签值合规性)，如果要将此标签键的允许值添加到从父策略继承的任何值，请启用此选项。

   默认情况下，将清除此选项，这意味着仅将从父策略定义和继承的这些值视为符合要求。如果父策略不存在并且您没有指定标签值，则任何值（包括没有值）都视为符合要求。

   要更新可接受的标签值列表，请选择 Specify allowed values for this tag key (为此标签键指定允许的值)，然后选择 Specify values (指定值)。出现提示时，输入新值（每个框一个值）然后选择 Save changes (保存更改)。

8. 对于 Prevent noncompliant operations for this tag (防止此标签的不合规操作)，我们建议您保留不选择此选项（默认设置），除非您有丰富的使用标签策略经验。请确保您已查看了解强制执行中的建议并测试技术。否则，您可能会阻止组织账户中的用户标记他们所需的资源。

   如果要强制实施此标签键的合规性，请选中该复选框，然后选择 Specify resource types (指定资源类型)。出现提示后，选择要包含在策略中的资源类型。然后选择 Save changes (保存更改)。

> **Important**
>
> 选择此选项后，只有在操作生成符合策略的标签时，操作指定类型资源的标签的任何操作才会成功。

9. （可选）要向此标签策略添加另一个标签键，请选择 Add tag key (添加标签键)。然后执行步骤 6–9 来定义标签键。

10. 完成标签策略构建后，选择 Save changes (保存更改)。

AWS CLI & AWS SDKs

创建标签策略

您可以使用以下方法之一来创建标签策略：

- AWS CLI：create-policy

  您可使用任何文本编辑器创建标签策略。使用 JSON 语法并将标签策略以任意名称和扩展名在您选择的位置另存为文件。标签策略最多可具有 2,500 个字符，包括空格。有关标签策略语法的信息，请参阅标签策略语法。

  创建标签策略

  1. 在文本文件中创建类似于以下内容的标签策略：

     testpolicy.json 的内容：

     ```
     {
         "tags": {
             "CostCenter": {
                 "tag_key": {
                     "@@assign": "CostCenter"
                 }
             }
         }
     }
     ```

     此标签策略定义 CostCenter 标签键。该标签可以接受任何值或不接受值。类似这样的策略意味着附加 CostCenter 标签（有没有值均可）的资源是合规的。

  2. 创建包含文件中策略内容的策略。为了便于阅读，输出中的额外空格已被截断。

     ```
     $ aws organizations create-policy \
         --name "MyTestTagPolicy" \
         --description "My Test policy" \
         --content file://testpolicy.json \
         --type TAG_POLICY
     {
         "Policy": {
             "PolicySummary": {
                 "Id": "p-a1b2c3d4e5",
     ```

```
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-a1b2c3d4e5",
            "Name": "MyTestTagPolicy",
            "Description": "My Test policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign
\":\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

- AWS SDK：CreatePolicy

后续操作

创建标签策略后，您可以使标记规则生效。为此，请将策略附加到组织根、组织部门（OU）、组织内的AWS 账户或组织实体的组合。

更新标签策略

> **最小权限**
>
> 要更新标签策略，您必须具有运行以下操作的权限：
>
> - `organizations:UpdatePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。
> - `organizations:DescribePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。

AWS Management Console

更新标签策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Tag policies (标签策略) 页面上，选择要更新的标签策略。
3. 选择编辑策略。

4. 您可以输入一个新的 Policy name (策略名称)、Policy description (策略说明)。您可以通过使用可视化编辑器或通过编辑 JSON 来更改策略内容。
5. 完成更新标签策略后，选择 Save changes (保存更改)。

AWS CLI & AWS SDKs

更新策略

您可以使用以下命令之一来更新策略：

- AWS CLI：update-policy

以下示例重命名标签策略。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n\n"
    }
}
```

以下示例添加或更改标签策略的说明。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
```

```
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

以下示例更改附加到 AI 服务选择退出策略的 JSON 策略文档。在此示例中，内容取自一个名为 policy.json 的文件，使用以下文本：

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
```

```
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage
\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":
{\"@@assign\":[\"ec2:instance\"]}}}}"
}
```

- AWS SDK：UpdatePolicy

编辑附加到标记策略的标签

当您登录到组织的管理账户时，您可以添加或删除附加到标签策略的标签。为此，请完成以下步骤。

> **最小权限**
>
> 要编辑附加到AWS组织中备份策略的标签，您必须拥有以下权限：
>
> - `organizations:DescribeOrganization`（仅限控制台 – 导航到策略）
> - `organizations:DescribePolicy`（仅限控制台 – 导航到策略）
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

编辑附加到 AI 服务选择退出策略的标签

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Tag policies (标签策略) 页面上，选择带有您想要编辑的标签的策略名称。
3. 在所选策略的详细信息页面上，选择 Tags (标签) 选项卡，然后选择 Manage tags (管理标签)。
4. 您可以在此页面上执行以下操作：
   - 编辑任何标签的值，方法是在旧标签上输入新值。您不能修改键。要更改键，您必须删除带有旧键的标签，然后添加使用新键的标签。
   - 删除任何现有的标签，方法是选择 Remove (删除)。

- 添加新的标签键和值对。选择 Add tag (添加标签)，然后在提供的框中输入新的键名称和可选值。如果您将 Value (值) 框留空，则值是空字符串；它并非 null。

5. 在完成所有要进行的添加、删除和编辑操作之后，选择 Save changes (保存更改)。

AWS CLI & AWS SDKs

编辑附加到标签策略的标签

您可以使用以下命令之一编辑附加到标签策略的标签：

- AWS CLI：tag-resource 和 untag-resource
- AWS SDK：TagResource 和 UntagResource

删除标签策略

当登录到您组织的管理账户时，您可以删除您的组织中不再需要的策略。

必须先将某个策略从所有附加实体中分离，然后才能删除该策略。

最小权限

要删除标签策略，您必须具有运行以下操作的权限：

- `organizations:DeletePolicy`

AWS Management Console

删除标签策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2.
3. 从 Tag policies (标签策略) 页面选择要删除的策略。
4. 要删除的策略必须先从所有根、OU 和账户分离。选择 Targets (目标) 选项卡，选择显示在 Targets (目标) 列表中的每个根、OU 或账户旁边的单选按钮，然后选择 Detach (分离)。在确认对话框中，选择 Detach (分离)。

5. 在页面的顶部，选择 Delete (删除)。
6. 在确认对话框上，输入策略的名称，然后选择 Delete (删除)。

AWS CLI & AWS SDKs

删除标签策略

您可以使用以下命令之一来删除策略：

- AWS CLI：delete-policy

  以下示例删除指定策略。仅当策略未附加到任何根、OU 或账户时，它们才有效。

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  如果成功，此命令不会产生任何输出。
- AWS SDK：DeletePolicy

附加和分离标签策略

您可以在整个组织以及组织单元 (OU) 和单独账户上使用标签策略。

- 将标签策略附加到组织根 时，标签策略将应用于该根的所有成员 OU 和账户。
- 当您将标签策略附加到某个 OU 时，该标签策略将应用到属于该 OU 的账户。这些账户还受附加到组织根的所有标签策略的约束。
- 当您将标签策略附加到某个账户 时，该标签策略将应用到账户。此外，该账户受附加到组织根的任何标签策略的约束，并且 受附加到该账户所属 OU 的任何标签策略的约束。

账户继承的任何标签策略以及直接附加到账户的任何标签策略的聚合称为有效标签策略。有关更多信息，请参阅了解管理策略继承。

> **Important**
>
> 未标记的资源不会在结果中显示为不合规。

最小权限

要附加标签策略，您必须具有运行以下操作的权限：

- `organizations:AttachPolicy`

AWS Management Console

您可以导航到要附加策略的根、OU 或账户，为其附加标签策略。

通过导航到根、OU 或账户来附加标签策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，导航到要将策略附加到的根、OU 或账户的相应名称并选择其名称。您可能需要展开 OU（选择 ）以查找所需的 OU 或账户。
3. 在 Policies (策略) 选项卡上的 Tag policies (标签策略) 中，选择 Attach (附加)。
4. 找到所需的策略，然后选择 Attach policy (附加策略)。

   Policies (策略) 选项卡上的附加的标签策略列表会更新，以包含新添加的内容。策略更改会立即生效。

通过导航到策略来附加标签策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Tag policies (标签策略) 页面上，选择要附加的策略的名称。
3. 在 Targets (目标) 选项卡上，选择 Attach (附加)。
4. 选择要附加策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OU（选择 ）以查找所需的 OU 或账户。
5. 选择 Attach policy（附上策略）。

Targets (目标) 选项卡上的附加的标签策略列表会更新，以包含新添加的内容。策略更改会立即生效。

AWS CLI & AWS SDKs

将标签策略附加到组织根、OU 或账户

您可以使用以下方法之一附加标签策略：

- AWS CLI：attach-policy

  以下过程显示如何将您刚创建的标签策略附加到单个测试账户。

  - 通过运行类似于下文的命令，将标签策略附加到您的测试账户：

    ```
    $ aws organizations attach-policy \
        --target-id <account-id> \
        --policy-id p-a1b2c3d4e5
    ```

    如果成功，此命令没有输出。
- AWS SDK：AttachPolicy

策略更改会立即生效。

后续操作

附加标签策略后，您可以了解该您的资源与标签策略的合规程度如何。为此，请使用 Resource Groups 控制台。有关更多信息，请参阅《AWS Resource Groups 用户指南》中的评估账户的合规性。

分离标签策略

当您登录到组织的管理账户时，您可以从标签策略所附加到的组织根、OU 或账户分离标签策略。从某个实体分离标签策略后，该策略将不再应用于现在已与之分离的实体所影响的任何账户。要分离策略，请完成以下步骤。

> **最小权限**
>
> 要从组织根、OU 或账户分离标签策略，您必须具有运行以下操作的权限：

- organizations:DetachPolicy

AWS Management Console

您可以导航到要分离策略的根、OU 或账户，为其分离标签策略。

通过导航到已附加策略的根、OU 或账户来分离标签策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面导航到要分离策略的根、OU 或账户。您可能需要展开 OU（选择 ）以查找所需的 OU 或账户。选择根、OU 或账户的名称。
3. 在 Policies (策略) 选项卡上，选择要分离的标签策略旁边的单选按钮，然后选择 Detach (分离)。
4. 在确认对话框中，选择 Detach policy (分离策略)。

   附加的标签策略的列表将更新。策略更改会立即生效。

通过导航到策略来分离标签策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Tag policies (标签策略) 页面上，选择要从根、OU 或账户分离的策略的名称。
3. 在 Targets (目标) 选项卡上，选择要分离策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OU（选择 ）以查找所需的 OU 或账户。
4. 选择分离。
5. 在确认对话框中，选择 Detach (分离)。

   附加的标签策略的列表将更新。策略更改会立即生效。

AWS CLI & AWS SDKs

从组织根、OU 或账户分离标签策略

您可以使用以下方法之一来分离标签策略：

- AWS CLI：detach-policy
- AWS SDK：DetachPolicy

策略更改会立即生效。

查看有效标签策略

在开始检查账户中已标记资源的合规性状态之前，首先确定账户的有效标签策略会很有帮助。

什么是有效标签策略？

有效标签策略 指定应用到账户的标记规则。这是账户继承的任何标签策略以及直接附加到账户的任何标签策略的聚合。将标签策略附加到组织根时，它应用到组织中的所有账户。将标签策略附加到 OU 时，它应用到属于该 OU 的所有账户和 OU。

例如，附加到组织根的标签策略可以定义具有四个合规值的 `CostCenter` 标签。附加到账户的单独标签策略可能会将 `CostCenter` 限制为四个合规值中的两个。这些标签策略的组合组成了有效标签策略。结果是，在组织根标签策略中定义的四个合规标签值中，只有两个符合该账户的要求。

有关如何生成有效标签策略的更多信息和高级示例，请参阅了解管理策略继承。

如何查看有效标签策略

您可以从 AWS Management Console、AWS API 或 AWS Command Line Interface 查看账户的有效标签策略。

> 最小权限
>
> 若要查看账户的有效标签策略，您必须具有运行以下操作的权限：
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization`

AWS Management Console

查看账户的有效标签策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，选择要查看其有效标签策略的账户的名称。您可能需要展开 OU（选择 ）以查找所需的账户。
3. 在 Policies (策略) 选项卡上的 Tag policies (标签策略) 部分，选择 View the effective tag policy for this AWS 账户 (查看此亚马逊云科技账户的有效标签策略)。

   控制台显示应用于指定账户的有效策略。

   > **Note**
   >
   > 如果没有重大更改，您无法复制和粘贴有效策略并将其用作其他标签策略的 JSON。标签策略文档必须包含继承运算符，这些运算符指定如何将每个设置合并到最终有效策略中。

AWS CLI & AWS SDKs

查看账户的有效标签策略

您可以使用以下方法之一查看有效标签策略：

- AWS CLI：describe-effective-policy

  要确定账户中继承或附加了哪些标记规则，请从账户运行以下命令并将结果保存到文件中：

```
$ aws organizations describe-effective-policy \
    --policy-type TAG_POLICY
{
    "EffectivePolicy": {
        "PolicyContent": "{\"tags\":{\"costcenter\":{\"tag_value\":[\"*\"],
\"tag_key\":\"CostCenter\"}}}",
        "LastUpdatedTimestamp": "2020-06-09T08:34:25.103000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "TAG_POLICY"
    }
```

```
}
```

如果某个标签策略附加到账户以及根或 OU，则所有继承策略的组合定义该账户的有效标签策略。在这些情况下，从账户运行 `describe-effective-policy` 将返回账户层次结构中的所有标签策略的合并内容。

- AWS SDK：DescribeEffectivePolicy

使用 Amazon EventBridge 监控不合规标签

您可以使用 Amazon EventBridge（之前称为 Amazon CloudWatch Events）监控何时引入了不合规标签。在以下示例事件中，`tag-policy-compliant` 的 `"false"` 值表示新标签不符合有效标签策略。

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
}
```

您可以订阅事件并指定要监控的字符串或模式。有关 EventBridge 的详细信息，请参阅《Amazon EventBridge 用户指南》。

了解强制执行

标签策略可以指定在指定资源类型上强制执行 不合规的标记操作。换句话说，阻止在指定的资源类型上完成不合规的标记操作。

> **Important**
>
> 强制执行不会对创建时不带标签的资源造成影响。

要强制遵守标签策略，请在创建标签策略时执行以下操作之一：

- 从 Visual editor (可视化编辑器) 选项卡中，选择 Prevent noncompliant operations for this tag (防止此标签的不合规操作)。
- 在 JSON 选项卡中，使用 `enforced_for` 字段。有关标签策略语法的信息，请参阅标签策略语法和示例。

在对标签策略强制执行合规性时，请遵循以下最佳实践：

- 请谨慎强制执行合规性 – 确保您了解使用标签策略的影响，并遵循标签策略入门中推荐的工作流。在将强制执行扩展到更多账户之前，在测试账户中测试强制执行的影响。否则，您可能会阻止组织账户中的用户标记他们所需的资源。
- 了解可以对哪些资源类型强制执行 – 您只能对支持资源类型上的标签策略强制执行合规性。当您使用可视化编辑器构建标签策略时，将列出支持强制执行合规性的资源类型。
- 了解与某些服务的交互 — 有些 AWS 服务具有类似容器的资源分组，可以自动为您创建资源，标签可以从一项服务中的资源传播到另一项服务。例如，Amazon EC2 Auto Scaling 组和 Amazon EMR 集群上的标签可以自动传播到其中包含的 Amazon EC2 实例。您的 Amazon EC2 标签策略可能会比 Auto Scaling 组或 EMR 集群更严格。如果您启用强制执行，则标签策略会阻止对标记资源，并可能会阻止动态扩展和预配置。

以下各部门介绍如何查找不符合要求的资源，以及如何将其更正为合规。

查找账户的不合规资源

对于每个账户，您可以获取有关不合规资源的信息。您应该从账户拥有资源的每个区域运行此命令。

要查找具有标签策略的账户的不合规资源，请运行以下命令将结果保存到文件中：

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

更正资源中的不合规标签

找到不符合标签后，请使用以下任意方法进行更正。您必须登录到具有不合规标签的资源的账户：

- 使用创建不合规资源的 AWS 服务的控制台或标记 API 操作。
- 使用 AWS Resource Groups TagResources和UntagResources操作添加符合有效策略的标签或删除不合规的标签。

查找和更正其他不合规问题

查找和更正合规性问题是一个迭代过程。重复前面两部分中的步骤，直到您关注的资源符合标签策略。

生成组织级的合规性报告

您可以随时生成一份报告，列出 AWS 账户 整个组织中所有已标记的资源。报告显示每个资源是否符合有效标签策略。请注意，您对标签策略或资源所做的更改，最多可能需要 48 小时才能反映在组织范围内的合规性报告中。例如，假定您有一个标签策略，为某个资源类型定义新的标准化标签。没有此标签的该类型的资源最多需要 48 小时在报告中显示为合规。

您可以从 us-east-1 区域中的组织管理账户生成报告，前提是该账户具有对 Amazon S3 存储桶的访问权限。存储桶必须具有附加的存储桶策略，如用于存储报告的 Amazon S3 存储桶策略中所示。若要生成报告，请运行以下命令：

```
$ aws resourcegroupstaggingapi get-compliance-summary --region us-east-1
{
    "SummaryList": [
        {
            "LastUpdated": "2020-06-09T18:40:46Z",
            "NonCompliantResources": 0
        }
    ]
}
```

您一次可以生成一个报告。

完成报告可能需要一些时间。您可以通过运行以下命令来检查状态：

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

当上述命令返回 SUCCEEDED 时，您可以从 Amazon S3 存储桶打开报告。

支持强制执行的服务和资源类型

以下服务和资源类型支持使用标签策略强制执行：

服务名称	资源类型	JSON 语法
Amazon API Gateway	• API 密钥 • 域名 • REST API 操作 • 阶段	• "apigateway:apikeys" • "apigateway:domainnames" • "apigateway:restapis" • "apigateway:restapis/stages"
AWS Amplify	• 组件 • 主题	• "amplifyuibuilder:app/environment/components" • "amplifyuibuilder:app/environment/themes"
AWS AppConfig	• 应用程序 • 配置文件 • 部署 • 部署策略 • 环境	• "appconfig:application" • "appconfig:application/configurationprofile" • "appconfig:application/environment/deployment" • "appconfig:deploymentstrategy" • "appconfig:application/environment"
AWS App Mesh	• 全部 • 网关路由 • Mesh • 路线 • 虚拟网关 • 虚拟节点 • 虚拟路由器 • 虚拟服务	• "appmesh:*" • "appmesh:mesh/virtualGateway/gatewayRoute" • "appmesh:mesh" • "appmesh:mesh/virtualRouter/route" • "appmesh:mesh/virtualGateway" • "appmesh:mesh/virtualNode"

服务名称	资源类型	JSON 语法
		• "appmesh:mesh/virtualRouter" • "appmesh:mesh/virtualService"
Amazon Athena	• 全部 • 工作组	• "athena:*" • "athena:workgroup"
AWS Audit Manager	• 评测 • 评估框架 • 控件	• "auditmanager:assessment " • "auditmanager:assessmentFramework " • "auditmanager:control "
AWS Backup	• 备份计划 • 文件库 • Gateway • Hyper Visor • VM	• "backup:backup-plan" • "backup:backup-vault" • "backup-gateway:gateway" • "backup-gateway:hypervisor" • "backup-gateway:vm"
AWS Batch	• 作业 • 作业定义 • 作业队列	• "batch:job" • "batch:job-definition" • "batch:job-queue"
AWS BugBust	• 事件	• "bugbust:event"
AWS Certificate Manager	• 全部 • 证书 • Private Certificate Authority	• "acm:*" • "acm:certificate" • "acm-pca:certificate-authority"

服务名称	资源类型	JSON 语法
Amazon Chime	• 应用程序实例 • 频道 • 媒体管线 • 会议 • SIP 媒体应用程序 • 用户应用程序实例 • 语音连接器	• "chime:app-instance" • "chime:app-instance/channel" • "chime:media-pipeline" • "chime:meeting" • "chime:sma" • "chime:app-instance/user" • "chime:vc"
AWS Clean Rooms	• 协作 • 已配置的表 • 成员资格 • 已配置的表关联	• "cleanrooms:collaboration" • "cleanrooms:configuredtable" • "cleanrooms:membership" • "cleanrooms:membership/configuredtableassociation"
AWS Cloud9	• 环境	• "cloud9:environment"
Amazon CloudFront	• 全部 • 分配 • 串流分配	• "cloudfront:*" • "cloudfront:distribution" • "cloudfront:streaming-distribution"
AWS CloudTrail	• 全部 • 试用	• "cloudtrail:*" • "cloudtrail:trail"
Amazon CloudWatch	• 全部 • 警报 • Contributor Insights 规则 • 指标流	• "cloudwatch:*" • "cloudwatch:alarm" • "cloudwatch:insight-rule" • "cloudwatch:metric-stream"
Amazon CloudWatch 互联网监视器	• 监控	• "internetmonitor:monitor"

服务名称	资源类型	JSON 语法
Amazon CloudWatch 日志	• 目标位置 • 日志组	• "logs:destination" • "logs:log-group"
Amazon CloudWatch 可观察性访问管理器	• 链接 • sink	• "oam:link" • "oam:sink"
AWS CodeBuild	• 全部 • 项目	• "codebuild:*" • "codebuild:project"
Amazon CodeCatalyst	• 连接	• "codecatalyst:connections"
AWS CodeCommit	• 全部 • 存储库	• "codecommit:*" • "codecommit:repository"
AWS CodePipeline	• 全部 • 操作类型 • 管道 • Webhook	• "codepipeline:*" • "codepipeline:actiontype" • "codepipeline:pipeline" • "codepipeline:webhook"
Amazon Cognito Identity	• 全部 • 身份池	• "cognito-identity:*" • "cognito-identity:identitypool"
Amazon Cognito 用户群体	• 全部 • 用户群体	• "cognito-idp:*" • "cognito-idp:userpool"
Amazon Comprehend	• 全部 • 文档分类器 • 实体识别程序	• "comprehend:*" • "comprehend:document-classifier" • "comprehend:entity-recognizer"

服务名称	资源类型	JSON 语法
AWS Config	• 全部 • 聚合授权 • Config 聚合器 • Config 规则	• "config:*" • "config:aggregation-authorization" • "config:config-aggregator" • "config:config-rule"
Amazon CodeGuru Reviewer	• 关联	• "codeguru-reviewer:association"
Amazon CodeGuru 安全	• 扫描	• "codeguru-security:scans"
CodeConnections	• Connection • Host	• "codestar-connections:connection" • "codestar-connections:host"
Amazon Connect	• 接洽流程 • 集成关联 • 队列 • Quick Connect • 路由配置文件 • 用户	• "connect:instance/contact-flow" • "connect:instance/integration-association" • "connect:instance/queue" • "connect:instance/transfer-destination" • "connect:instance/routing-profile" • "connect:instance/agent"
Amazon Connect Wisdom	• Assistant • 关联 • 内容 • 知识库 • 会话	• "wisdom:assistant" • "wisdom:association" • "wisdom:content" • "wisdom:knowledge-base" • "wisdom:session"

服务名称	资源类型	JSON 语法
AWS Database Migration Service	• 全部 • 终端节点 • ES • Rep • Subgrp • 任务	• "dms:*" • "dms:endpoint" • "dms:es" • "dms:rep" • "dms:subgrp" • "dms:task"
Amazon Data Lifecycle Manager	• Policy	• "dlm:policy"
AWS 二极管	• Mapping	• "diode-messaging:mapping"
AWS Direct Connect	• 全部 • Dxcon • Dxlag • Dxvif	• "directconnect:*" • "directconnect:dxcon" • "directconnect:dxlag" • "directconnect:dxvif"
Amazon DynamoDB	• 全部 • 表	• "dynamodb:*" • "dynamodb:table"
Amazon EC2	• 容量预留 • 容量预留车队 • 运营商网关	• "ec2:capacity-reservation" • "ec2:capacity-reservation-fleet" • "ec2:carrier-gateway"
	• Client VPN 端点 • CoIP 池 • 客户网关	• "ec2:client-vpn-endpoint" • "ec2:coip-pool" • "ec2:customer-gateway"
	• 专用主机 • DHCP 选项 • 仅出口 Internet 网关	• "ec2:dedicated-host" • "ec2:dhcp-options" • "ec2:egress-only-internet-gateway"

服务名称	资源类型	JSON 语法
	• 弹性 IP • 活动窗口 • 实例集	• "ec2:elastic-ip" • "ec2:instance-event-window" • "ec2:fleet"
	• FPGA 映像 • 主机预留 • 图像	• "ec2:fpga-image" • "ec2:host-reservation" • "ec2:image"
	• 实例 • 互联网网关 • IP 地址管理器	• "ec2:instance" • "ec2:internet-gateway" • "ec2:ipam"
	• IP 地址管理器池 • IP 地址管理器作用域 • IPv4 池	• "ec2:ipam-pool" • "ec2:ipam-scope" • "ec2:ipv4pool-ec2"
	• 密钥对 • 启动模板 • 本地网关路由表	• "ec2:key-pair" • "ec2:launch-template" • "ec2:local-gateway-route-table"
	• 本地网关路由表虚拟接口组关联 • 本地网关路由表 VPC 关联 • NAT 网关	• "ec2:local-gateway-route-table-virtual-interface-group-association" • "ec2:local-gateway-route-table-vpc-association" • "ec2:natgateway"
	• 网络 ACL • 网络接口 • 网络洞察访问范围	• "ec2:network-acl" • "ec2:network-interface" • "ec2:network-insights-access-scope"

服务名称	资源类型	JSON 语法
	• 网络见解访问范围分析 • 网络洞察分析 • 网络洞察路径	• "ec2:network-insights-access-scope-analysis" • "ec2:network-insights-analysis" • "ec2:network-insights-path"
	• 置放组 • 前缀列表 • 替换根卷任务	• "ec2:placement-group" • "ec2:prefix-list" • "ec2:replace-root-volume-task"
	• 预留实例 • 路由表 • 安全组	• "ec2:reserved-instances" • "ec2:route-table" • "ec2:security-group"
	• 快照 • 竞价型实例请求 • 子网	• "ec2:snapshot" • "ec2:spot-instances-request" • "ec2:subnet"
	• 子网 CIDR 预留 • 流量镜像筛选 • 流量镜像会话	• "ec2:subnet-cidr-reservation" • "ec2:traffic-mirror-filter" • "ec2:traffic-mirror-session"
	• 流量镜像目标 • Transit Gateway • Transit Gatewa	• "ec2:traffic-mirror-target" • "ec2:transit-gateway" • "ec2:transit-gateway-attachment"
	• Transit Gateway Conn • Transit Gateway 多播域 • Transit Gateway政策表	• "ec2:transit-gateway-connect-peer" • "ec2:transit-gateway-multicast-domain" • "ec2:transit-gateway-policy-table"

服务名称	资源类型	JSON 语法
	• 中转网关路由表 • 经过验证的访问端点 • 已验证的访问组	• "ec2:transit-gateway-route-table" • "ec2:verified-access-endpoint" • "ec2:verified-access-group"
	• 已验证的访问实例 • 经过验证的访问信任提供商 • Volume	• "ec2:verified-access-instance" • "ec2:verified-access-trust-provider" • "ec2:volume"
	• VPC 流日志 • VPC • VPC 端点	• "ec2:vpc-flow-log" • "ec2:vpc" • "ec2:vpc-endpoint"
	• VPC 终端节点服务 • VPC 对等连接 • VPN 连接 • VPN 网关	• "ec2:vpc-endpoint-service" • "ec2:vpc-peering-connection" • "ec2:vpn-connection" • "ec2:vpn-gateway"
Amazon EC2 回收站	• 规则	• "rbin:rule"
AWS Elastic Beanstalk	• 应用程序 • 应用程序版本 • 配置模板 • 平台	• "elasticbeanstalk:application" • "elasticbeanstalk:applicationversion" • "elasticbeanstalk:configurationtemplate" • "elasticbeanstalk:platform"
Amazon Elastic Container Registry	• 存储库	• "ecr:repository"

服务名称	资源类型	JSON 语法
Amazon Elastic Container Service	• 容量提供商 • 集群 • 服务 • 任务定义 • 任务集	• "ecs:capacity-provider" • "ecs:cluster" • "ecs:service" • "ecs:task-definition" • "ecs:task-set"
Amazon Elastic File System	• 全部 • 文件系统	• "elasticfilesystem:*" • "elasticfilesystem:file-system"
Amazon Elastic Inference	• Accelerator	• "elastic-inference:elastic-inference-accelerator"
Amazon Elastic Kubernetes Service	• 集群	• "eks:cluster"
Amazon Elastic Search	• 域	• "es:domain"
Amazon EMR	• 集群 • Editor	• "elasticmapreduce:cluster" • "elasticmapreduce:editor"
Amazon EMR Serverless	• 应用程序	• "emr-serverless:applications"
AWS 实体分辨率	• 匹配流程 • 架构映射	• "entityresolution:matchingworkflow" • "entityresolution:schemamapping"
Amazon ElastiCache	• 集群	• "elasticache:cluster"
Amazon EventBridge	• 全部 • 事件总线 • 规则	• "events:*" • "events:event-bus" • "events:rule"

服务名称	资源类型	JSON 语法
亚马逊 Pi EventBridge pes	• 竖线	• "pipes:pipe"
Amazon EventBridge 日程安排	• 计划组	• "scheduler:schedule-group"
Amazon Fraud Detector	• 探测器 • 探测器版本 • 模型 • 规则 • Variable	• "frauddetector:detector" • "frauddetector:detector-version" • "frauddetector:model" • "frauddetector:rule" • "frauddetector:variable"
Amazon Global Accelerator	• Accelerator	• "globalaccelerator:accelerator"
Elastic Load Balancing	• 全部 • Listener • 监听器规则 • 负载均衡器 • 目标组	• "elasticloadbalancing:*" • "elasticloadbalancing:listener" • "elasticloadbalancing:listener-rule" • "elasticloadbalancing:loadbalancer" • "elasticloadbalancing:targetgroup"
Amazon FSx	• 全部 • 备份 • 文件系统	• "fsx:*" • "fsx:backup" • "fsx:file-system"

服务名称	资源类型	JSON 语法
Amazon GuardDuty	• 探测器 • 筛选条件 • IP 集 • 威胁情报集	• "guardduty:detector" • "guardduty:detector/filter" • "guardduty:detector/ipset" • "guardduty:detector/threatintelset"
AWS HealthLake	• 数据存储	• "healthlake:datastore "
AWS HealthOmics	• 注释存储 • 注释存储版本 • 参考存储 • 参考 • 运行 • 运行组 • 序列存储 • 读取集 • 变体存储 • 工作流	• "omics:annotationStore" • "omics:annotationStore/version" • "omics:referenceStore" • "omics:referenceStore/reference" • "omics:run" • "omics:runGroup" • "omics:sequenceStore" • "omics:sequenceStore/readSet" • "omics:variantStore" • "omics:workflow"
Amazon Inspector	• 筛选条件	• "inspector2:filter "
AWS Identity and Access Management	• 实例配置文件 • MFA • OIDC 提供商 • Policy • SAML 提供商 • 服务器证书	• "iam:instance-profile" • "iam:mfa" • "iam:oidc-provider" • "iam:policy" • "iam:saml-provider" • "iam:server-certificate"

服务名称	资源类型	JSON 语法
AWS IoT Analytics	• 全部 • 频道 • 数据集 • 数据存储 • 管道	• "iotanalytics:*" • "iotanalytics:channel" • "iotanalytics:dataset" • "iotanalytics:datastore" • "iotanalytics:pipeline"
AWS IoT Events	• 全部 • 探测器模型 • 输入	• "iotevents:*" • "iotevents:detectorModel" • "iotevents:input"
AWS IoT Fleet Hub	• 应用程序	• "iotfleethub:application"
AWS IoT SiteWise	• 资产 • 资产模型	• "iotsitewise:asset" • "iotsitewise:asset-model "
AWS IoT Greengrass	• 批量部署 • 连接器定义 • 内核定义 • 设备定义 • 功能定义 • 记录器定义 • 资源定义 • 订阅定义	• "greengrass:bulk" • "greengrass:connectorsDefinition" • "greengrass:coresDefinition" • "greengrass:devicesDefinition" • "greengrass:functionsDefinition" • "greengrass:loggersDefinition" • "greengrass:resourcesDefinition" • "greengrass:subscriptionsDefinition"
AWS Key Management Service	• 全部 • 键	• "kms:*" • "kms:key"

服务名称	资源类型	JSON 语法
Amazon Kinesis	• 全部 • 应用程序	• "kinesisanalytics:*" • "kinesisanalytics:application"
Amazon Data Firehose	• 全部 • 传输流	• "firehose:*" • "firehose:deliverystream"
AWS Lambda	• 全部 • 函数	• "lambda:*" • "lambda:function"
Amazon Macie	• 自定义数据标识符	• "macie2:custom-data-identifier"
Amazon MediaStore	• 容器	• "mediastore:container"
Amazon MQ	• 代理 • 配置	• "mq:broker" • "mq:configuration"
Amazon Network Firewall	• 防火墙 • 防火墙策略 • 有状态规则组 • 无状态规则组	• "network-firewall:firewall" • "network-firewall:firewall-policy" • "network-firewall:stateful-rulegroup" • "network-firewall:stateless-rulegroup"
Amazon OpenSearch 无服务器	• 集合	• "aoss:collection"
AWS Organizations	• 账户 • 组织部门 • Policy • 根	• "organizations:account" • "organizations:ou" • "organizations:policy" • "organizations:root"

服务名称	资源类型	JSON 语法
Amazon Pinpoint SMS Voice V2	• 配置集 • 退订列表 • 电话号码 • 池 • 发件人 ID	• "sms-voice:configuration-set" • "sms-voice:opt-out-list" • "sms-voice:phone-number" • "sms-voice:pool" • "sms-voice:sender-id"
Amazon RDS	• 集群参数组 • 集群端点 • 事件订阅 • 数据库选项组 • 数据库参数组 • 数据库代理 • 数据库代理端点 • 预留数据库实例 • 数据库安全组 • DB subnet group（数据库子网组） • 目标组	• "rds:cluster-pg" • "rds:cluster-endpoint" • "rds:es" • "rds:og" • "rds:pg" • "rds:db-proxy" • "rds:db-proxy-endpoint" • "rds:ri" • "rds:secgrp" • "rds:subgrp" • "rds:target-group"

服务名称	资源类型	JSON 语法
Amazon Redshift	• 全部 • 集群 • 数据库组 • 数据库名称 • 数据库用户 • 事件订阅 • HSM 客户端证书 • HSM 配置 • 参数组 • 快照 • 快照复制授权 • 快照计划 • 子网组	• `"redshift:*"` • `"redshift:cluster"` • `"redshift:dbgroup"` • `"redshift:dbname"` • `"redshift:dbuser"` • `"redshift:eventsubscription"` • `"redshift:hsmclientcertificate"` • `"redshift:hsmconfiguration"` • `"redshift:parametergroup"` • `"redshift:snapshot"` • `"redshift:snapshotcopygrant"` • `"redshift:snapshotschedule"` • `"redshift:subnetgroup"`
Amazon Redshift Serverless	• 命名空间 • 工作组	• `"redshift-serverless:namespace"` • `"redshift-serverless:workgroup"`
AWS Resource Access Manager	• 全部 • 资源共享	• `"ram:*"` • `"ram:resource-share"`
AWS Resource Groups	• 全部 • 组	• `"resource-groups:*"` • `"resource-groups:group"`
Amazon Route 53	• 托管区域	• `"route53:hostedzone"`

服务名称	资源类型	JSON 语法
Amazon Route 53 Resolver	• 全部 • 解析程序终端节点 • 解析程序规则	• "route53resolver:*" • "route53resolver:resolver-endpoint" • "route53resolver:resolver-rule"
Amazon S3	• 存储桶 • Storage Lens • 存储镜头组	• "s3:bucket" • "s3:storage-lens" • "s3:storage-lens-group"
Amazon SageMaker	• App Image Config • Artifact • 上下文 • 训练作业 • 处理任务 • 模型包组 • 人工任务 UI • 模型包 • 操作 • 管道 • 试验 • 流定义 • 项目	• "sagemaker:app-image-config" • "sagemaker:artifact" • "sagemaker:context" • "sagemaker:training-job" • "sagemaker:processing-job " • "sagemaker:model-package-group" • "sagemaker:human-task-ui" • "sagemaker:model-package" • "sagemaker:action" • "sagemaker:pipeline" • "sagemaker:experiment" • "sagemaker:flow-definition" • "sagemaker:project"
AWS Secrets Manager	• 全部 • 密钥	• "secretsmanager:*" • "secretsmanager:secret"
AWS 安全湖	• 数据湖 • 订阅者	• "securitylake:data-lake" • "securitylake:subscriber"

服务名称	资源类型	JSON 语法
AWS Service Catalog	• 应用程序 • 属性组 • 产品组合 • 产品	• "servicecatalog:applications" • "servicecatalog:attribute-groups " • "catalog:portfolio " • "catalog:product "
Amazon Simple Notification Service（SNS）	• 主题	• "sns:topic"
Amazon Simple Queue Service (SQS)	• 队列	• "sqs:queue"
Amazon States Language	• 全部 • 活动 • 状态机	• "states:*" • "states:activity " • "states:stateMachine "
AWS Step Functions	• 活动	• "states:activity"
AWS Storage Gateway	• 全部 • Gateway • 共享 • 磁带 • Volume	• "storagegateway:*" • "storagegateway:gateway" • "storagegateway:share" • "storagegateway:tape" • "storagegateway:gateway/volume"

服务名称	资源类型	JSON 语法
AWS Systems Manager	• 关联 • 自动化执行 • 文档 • 维护时段 • 托管实例 • 操作项目 • 补丁基准 • 会话 • 联系人	• "ssm:association" • "ssm:automation-execution" • "ssm:document" • "ssm:maintenancewindow" • "ssm:managed-instance" • "ssm:opsitem" • "ssm:patchbaseline" • "ssm:session" • "ssm-contacts:contact"
Amazon Textract	• 适配器 • 版本	• "textract:adapters" • "textract:adapters/versions"
AWS Transer Family	• Server • 用户 • 工作流	• "transfer:server" • "transfer:user" • "transfer:workflow"
Amazon Well-Arch itected	• 工作负载	• "wellarchitected:workload"
AWS Wickr	• 网络	• "wickr:network"
Amazon WorkSpaces	• 全部 • 连接别名 • 目录 • WorkSpace • WorkSpaces 捆绑包 • WorkSpaces 图片 • WorkSpaces IP 组	• "workspaces:*" • "workspaces:connectionalias" • "workspaces:directory" • "workspaces:workspace" • "workspaces:workspacebundle" • "workspaces:workspaceimage" • "workspaces:workspaceipgroup"
Amazon WorkLink	• 实例集	• "worklink:fleet"

标签策略语法和示例

本页介绍标签策略语法并提供示例。

标签策略语法

标签策略是一个纯文本文件，根据 JSON 的规则设置结构。标签策略的语法遵循管理策略类型的语法。有关该语法的完整讨论，请参阅了解管理策略继承。本主题重点介绍如何将该常规语法应用于标签策略类型的特定要求。

以下标签策略显示了基本标签策略语法：

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "100",
                    "200"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:*"
                ]
            }
        }
    }
}
```

标签策略语法包括以下元素：

- `tags` 字段键名称。标签策略始终以此固定键名开头。它是上面示例策略中的顶行。
- 唯一标识策略语句的策略键。它必须与标签键 的值相匹配，除了大小写处理。与标签键不同（下文将介绍），策略值不区分大小写。

  在此示例中，`costcenter` 是策略键。

- 至少有一个标签键，指定允许的标签键（具有您希望资源遵循的大小写）。如果未定义大小写处理，则标签键的默认大写处理是小写。标签键的值必须与策略键的值匹配。但是，由于策略键值不区分大小写，所以大小写可以不同。

  在此示例中，CostCenter 是标签键。这是符合标签策略要求所需的大小写处理。为此标签键使用其他大小写处理的资源不符合标签策略要求。

  您可以在一个标签策略中定义多个标签键。
- （可选）标签键的一个或多个可接受标签值 的列表。如果标签策略没有为标签键指定标签值，则任何值（包括没有值）都将视为合规。

  在此示例中，CostCenter 标签键的可接受值为 100 和 200。
- （可选）一个 enforced_for 选项，指示是否阻止对指定服务和资源执行任何不合规标记操作。在控制台中，这是用于创建标签策略的可视化编辑器中的 Prevent noncompliant operations for this tag (防止此标签的不合规操作) 选项。此选项的默认设置为空。

  示例标签策略指定所有 AWS Secrets Manager 资源必须具有此标签。

  > **Warning**
  >
  > 只有当您具有使用标签策略经验的情况下，才可以更改默认选项。否则，您可能会阻止组织账户中的用户创建他们所需的资源。

- 运算符指定标记策略如何与组织树中的其他标记策略合并，以创建账户的有效标签策略。在此示例中，@@assign 用于将字符串分配给 tag_key、tag_value 和 enforced_for。有关运算符的更多信息，请参阅继承运算符。
- – 您可以在标签值和 enforced_for 字段中使用 * 通配符：
  - 您仅可以为每个标签值使用一个通配符。例如，允许使用 *@example.com，但不允许使用 *@*.com。
  - 对于 enforced_for，您可以将 <service>:* 与某些服务一起使用，为该服务的所有资源启用强制执行。有关支持 enforced_for 的服务和资源类型的列表，请参阅支持强制执行的服务和资源类型。

    您不能使用通配符指定所有服务或指定所有服务的某个资源。

标签策略示例

下面的示例标签策略 仅供参考。

> **Note**
>
> 尝试在组织中使用这些示例标签策略之前，请注意以下事项：
>
> - 确保您已按照推荐的工作流开始使用标签策略。
> - 您应根据您的独特要求仔细查看和自定义这些标签策略。
> - 标签策略中的所有字符都受到最大大小的约束。本指南中的示例演示了使用额外空白编排格式的标签策略，以提高其可读性。但是，要在策略大小接近最大大小时节省空间，您可以删除任何空白。空白的示例包括引号外部的空格字符和换行符。
> - 未标记的资源不会在结果中显示为不合规。

示例 1：定义组织级的标签键大小写

以下示例显示了一个标签策略，该策略仅定义了两个标签键和您希望组织中的账户标准化所采用的大小写。

策略 A – 组织根标签策略

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

此标签策略定义两个标签键：CostCenter 和 Project。将此标签策略附加到组织根具有以下效果：

- 组织中的所有账户继承此标签策略。

- 组织中的所有账户都必须使用定义的大小写处理以实现合规性。具有 CostCenter 和 Project 标签的资源符合要求。为标签键（例如，costcenter、Costcenter 或 COSTCENTER）使用其他大小写处理的资源不符合要求。
- @@operators_allowed_for_child_policies": ["@@none"] 行锁定标签键。附加在组织树（子策略）下方的标签策略不能使用值设置运算符来更改标签键，包括其大小写处理。
- 对于所有标签策略，不会评估未标记的资源或未在标签策略中定义的标签是否符合标签策略。

AWS 建议您使用此示例作为指南，为要使用的标签键创建类似的标签策略。将其附加到组织根。然后创建类似于下一个示例的标签策略，该策略仅为已定义的标签键定义可接受值。

下一步：定义值

假定您将以前的标签策略附加到组织根。接下来，您可以创建类似于下文的标签策略并将其附加到账户。此策略定义 CostCenter 和 Project 标签键的可接受值。

策略 B – 账户标签策略

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

如果将策略 A 附加到组织根，并将策略 B 附加到账户，则这些策略将合并，以便为该账户创建以下有效标签策略：

策略 A + 策略 B = 账户的有效标签策略

```
{
    "tags": {
        "Project": {
            "tag_value": [
                "A",
                "B"
            ],
            "tag_key": "Project"
        },
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

有关策略继承的更多信息，包括继承运算符的工作方式示例和有效标签策略示例，请参阅[了解管理策略继承](#)。

示例 2：防止使用标签键

要防止使用标签键，您可以将类似以下内容的标签策略附加到组织实体。

此示例策略指定 Color 标签键不接受任何值。它还指定子标签策略中不允许[运算符](#)。因此，受影响账户中的资源上的任何 Color 标签都被视为不符合要求。但是，enforced_for 选项实际上可防止受影响的账户仅使用 Color 标签标记 Amazon DynamoDB 表。

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": [
```

```
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
                "@@assign": [
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

支持的区域

标签策略功能在以下区域中可用：

区域名称	区域参数
美国东部（弗吉尼亚北部）区域[1]	**us-east-1**
美国东部（俄亥俄州）区域	us-east-2
美国西部（北加利福尼亚）区域	us-west-1
美国西部（俄勒冈州）区域	us-west-2
非洲（开普敦）区域[2]	af-south-1
亚太地区（香港）区域[2]	ap-east-1
亚太地区（孟买）区域	ap-south-1
亚太地区（海得拉巴）[2]	ap-south-2
Asia Pacific（Tokyo）Region	ap-northeast-1
亚太地区（首尔）区域	ap-northeast-2
亚太地区（大阪）区域	ap-northeast-3
亚太地区（新加坡）区域	ap-southeast-1

区域名称	区域参数
亚太地区（悉尼）区域	ap-southeast-2
亚太地区（雅加达）区域[2]	ap-southeast-3
亚太地区（墨尔本）[2]	ap-southeast-4
加拿大西部（卡尔加里）[2]	ca-west-1
加拿大（中部）区域	ca-central-1
欧洲地区（法兰克福）区域	eu-central-1
欧洲（苏黎世）地区[2]	eu-central-2
欧洲（米兰）区域[2]	eu-south-1
欧洲（西班牙）[2]	eu-south-2
欧洲地区（爱尔兰）区域	eu-west-1
欧洲地区（伦敦）区域	eu-west-2
欧洲（巴黎）区域	eu-west-3
欧洲地区（斯德哥尔摩）区域	eu-north-1
中东（阿联酋）地区[2]	me-central-1
中东（巴林）区域[2]	me-south-1
南美洲（圣保罗）区域	sa-east-1
以色列（特拉维夫）[2]	il-central-1

[1]调用以下 Organizations 操作时必须指定 **us-east-1** 区域：

- DeletePolicy
- DisablePolicyType

- EnablePolicyType
- 对组织根目录进行的任何其他操作，例如ListRoots。

调用以下作为标签策略功能一部分的 Resource Groups 标记 API 操作时，您也必须指定 **us-east-1** 区域：

- DescribeReportCreation
- GetComplianceSummary
- GetResources
- StartReportCreation

> **Note**
>
> 要评估组织范围的标签策略合规性，您还必须能够访问美国东部（弗吉尼亚北部）区域中的 Amazon S3 存储桶以进行报告存储。有关更多信息，请参阅《标记 AWS 资源用户指南》中的 Amazon S3 存储桶报告存储策略。

[2] 这些区域必须手动启用。要了解有关启用和禁用的更多信息 AWS 区域，请参阅账户管理参考指南中的指定 AWS 区域 您的AWS 账户可以使用。在这些区域中，Resource Groups 控制台不可用。

服务控制策略 (SCP)

服务控制策略 (SCP) 是一种组织策略，可用于管理组织中的权限。SCP 可以集中控制组织中 IAM 用户和 IAM 角色的最大可用权限。SCP 可帮助确保您的账户符合组织的访问控制准则。SCP 仅在启用所有功能的组织中可用。如果您的组织只启用了整合账单功能，则不能使用 SCP。有关启用 SCP 的说明，请参阅启用和禁用策略类型。

SCP 不向组织中的 IAM 用户和 IAM 角色授予权限。SCP 不授予任何权限。SCP 对组织中的 IAM 用户和 IAM 角色可以执行的操作定义权限护栏或设置限制。要授予权限，管理员必须附加策略来控制访问权限，例如附加到 IAM 用户和 IAM 角色的基于身份的策略，以及附加到您账户中资源的基于资源的策略。有效权限是 SCP 允许的权限与基于身份和资源的策略允许的权限之间的逻辑交叉点。

> **Important**
>
> SCP 不会影响管理账户中的用户或角色。它们仅影响组织中的成员账户。

本页面上的主题

测试 SCP 的影响

AWS 强烈建议在未彻底测试策略对账户的影响之前，不要将 SCP 附加到组织的根目录。您可以改为创建一个 OU，并将您的账户一次移入一个，或至少每次以少量移入，以确保您不会无意中阻止用户使用关键服务。确定账户是否使用服务的一种方法是检查 IAM 中服务上次访问的数据。另一种方法是AWS CloudTrail 使用在 API 级别记录服务使用情况。

> **Note**
>
> 除非您修改完整版AWSAccess策略或将其替换为包含允许操作的单独策略，否则成员账户的所有操作都将失败，否则成员账户的所有 AWS 操作都将失败。

SCP 的最大大小

SCP 中的所有字符将计入其最大大小。本指南中的示例演示了使用额外空格编排格式的 SCP，以提高其可读性。但是，在您的策略大小接近最大大小时，可以删除任何空格（例如，引号之外的空格字符和换行符）来节省空间。

> **Tip**
>
> 使用可视化编辑器构建您的 SCP。它会自动删除额外的空格。

将 SCP 附加到组织中的不同级别

有关 SCP 如何工作的详细说明，请参阅 SCP 评估。

SCP 对权限的影响

SCP 与 AWS Identity and Access Management (IAM) 权限策略类似，使用几乎相同的语法。但是，SCP 永远不会授予权限。相反，SCP 是 JSON 策略，用于指定组织中 IAM 用户和 IAM 角色的最大权限。有关更多信息，请参阅《IAM 用户指南》中的策略评估逻辑。

- SCP 只影响 IAM 用户和角色，此类用户和角色由属于组织的账户进行管理。SCP 不会直接影响基于资源的策略，也不会影响组织外的账户的用户或角色。例如，请考虑一个 Amazon S3 存储桶，它由组织中的账户“A”所有。存储桶策略（一种基于资源的策略）会向来自组织外账户 B 的用户授予访问权限。账户 A 附加了一个 SCP。SCP 不适用于账户 B 中的那些外部用户。SCP 仅适用于由该组织内的账户 A 所管理的用户。
- SCP 会限制成员账户中的 IAM 用户和角色的权限，包括成员账户的根用户。任何账户都只有上方的每个 父级允许的那些权限。如果权限在账户上面的任何级别被隐式阻止（通过不包括在 `Allow` 策略语句中）或明确阻止（通过包括在 `Deny` 策略语句中），则受影响账户中的用户或角色不能使用该权限，即使账户管理员将带有 */* 权限的 `AdministratorAccess` IAM policy 附加到用户也是如此。
- SCP 仅影响组织中的成员账户。它们对管理账户中的用户或角色没有任何影响。
- 仍然必须通过适当的 IAM 权限策略将权限授予用户和角色。没有任何 IAM 权限策略的用户没有访问权，即使适用的 SCP 允许所有服务和所有操作也是如此。
- 如果用户或角色具有 IAM 权限策略，而该策略允许访问适用的 SCP 也允许的操作，则用户或角色可以执行该操作。
- 如果用户或角色具有 IAM 权限策略，而该策略允许访问不允许或被相应的 SCP 明确拒绝的操作，则用户或角色不能执行该操作。
- SCP 会影响附加账户中的所有用户和角色，包括根用户。唯一例外在 不受 SCP 限制的任务和实体中介绍。
- SCP 不会 影响任何服务相关角色。服务关联角色使其他 AWS 服务可以与之集成， AWS Organizations 并且不能受到 SCP 的限制。
- 在根目录中禁用 SCP 策略类型时，所有 SCP 将自动与该根目录中的所有 AWS Organizations 实体分离。 AWS Organizations 实体包括组织单位、组织和账户。如果在根中重新启用 SCP，该根将仅恢复为自动附加到根中所有实体的默认 `FullAWSAccess` 策略。在禁用 SCP 之前附加到 AWS Organizations 实体的任何 SCP 都将丢失，并且不能自动恢复，不过您可以手动重新附加它们。

- 如果权限边界（高级 IAM 功能）和 SCP 同时存在，则边界、SCP 以及基于身份的策略必须全部允许操作。

使用访问数据改进 SCP

使用管理账户证书登录后，您可以在 IAM 控制台的AWS Organizations部分中查看 AWS Organizations 实体或策略的上次访问服务数据。您还可以在 IAM 中使用 AWS Command Line Interface (AWS CLI) 或 AWS API 来检索上次访问服务的数据。这些数据包括 AWS Organizations 账户中的 IAM 用户和角色上次尝试访问哪些允许的服务以及何时访问的信息。您可以使用此信息确定不必要的权限，从而优化 SCP 以更好地遵循最小特权原则。

例如，您可能有一个禁止访问三项 AWS 服务的拒绝列表 SCP。SCP 的 Deny 语句中未列出的所有服务均允许访问。IAM 中上次访问的 AWS 服务数据会告诉您 SCP 允许但从未使用过哪些服务。借助该信息，您可以更新 SCP 以拒绝对不需要服务的访问权限。

有关更多信息，请参阅 IAM 用户指南中的以下主题：

- 查看 Organizations 的 Organizations 服务上次的访问数据
- 使用数据来细化组织部门的权限

不受 SCP 限制的任务和实体

您无法使用 SCP 来限制以下任务：

- 管理账户执行的任何操作
- 使用附加到服务相关角色的权限执行的任何操作
- 以根用户身份注册企业支持计划
- 以 root 用户身份更改 AWS 支持级别
- 为 CloudFront 私有内容提供可信签名者功能
- 为 Amazon Lightsail 电子邮件服务器和作为根用户的 Amazon EC2 实例配置反向 DNS
- 一些 AWS相关服务的任务：
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - Amazon Product Marketing API

创建、更新和删除服务控制策略

当登录到您组织的管理账户时，您可以创建和更新服务控制策略（SCP）。您可以通过构建拒绝或允许访问您指定的服务和操作的语句来创建 SCP。

SCP 的默认配置是使用“阻止列表”策略，在该策略中，除了通过创建拒绝访问的语句阻止的操作之外，它会隐式允许所有操作。对于拒绝语句，您可以为该语句指定资源和条件并使用 NotAction 元素。对于允许语句，您只能指定服务和操作。有关拒绝访问和允许访问的语句的更多信息，请参阅 SCP 评估。

> **Tip**
>
> 您可以使用 IAM 中服务上次访问的数据作为更新 SCP 的数据点，以限制仅访问您需要的AWS服务。有关更多信息，请参阅《IAM 用户指南》中的查看 Organizations 的 Organizations 服务上次访问的数据。

本主题内容：

- 为组织启用服务控制策略后，您可以创建策略。
- 当 SCP 要求发生变化时，您可以更新现有策略。
- 当您不再需要策略并将其与所有组织部门（OU）和账户分离后，您可以删除策略。

创建 SCP

> **最小权限**
>
> 要创建 SCP，您需要运行以下操作的权限：
>
> - `organizations:CreatePolicy`

AWS Management Console

创建服务控制策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Service control policies (服务控制策略) 页面上，选择 Create policy (创建策略)。

3. 在 CCreate new service control policy (创建新的服务控制策略) 页面上，输入策略的 Policy name (策略名称) 和可选 Policy description (策略说明)。

4. （可选）添加一个或多个标签，方法是选择 Add tag (添加标签)，然后输入一个键和可选的值。将值留空，设置为空字符串；它并非 null。您最多可以向策略附加 50 个标签。有关更多信息，请参阅为 AWS Organizations 资源添加标签。

   > **Note**
   >
   > 在接下来的大多数步骤中，我们讨论如何使用 JSON 编辑器右侧的控件来逐个元素构建策略。或者，您可以随时在窗口左侧的 JSON 编辑器中输入文本。您可以直接键入，也可以使用复制和粘贴。

5. 为了构建策略，您的后续步骤因您是否要添加拒绝或允许访问的语句而异。有关更多信息，请参阅SCP 评估。如果您使用 Deny 语句，您可以进行额外的控制，因为您可以限制对特定资源的访问，定义 SCP 何时生效的条件并使用 NotAction 元素。有关语法的详细信息，请参阅SCP 语法。

   要添加拒绝 访问的语句，请执行以下操作：

   a. 在编辑器右侧的编辑语句窗格中，在添加操作下选择 AWS 服务。

      当您选择右侧的选项时，JSON 编辑器会更新，以在左侧显示相应的 JSON 策略。

   b. 选择服务后，将打开一个列表，其中包含该服务的可用操作。您可以选择 All actions (所有操作)，或选择要拒绝的一个或多个单独操作。

      左侧的 JSON 将更新，以包含您选择的操作。

      > **Note**
      >
      > 如果您选择一个单独的操作，然后返回并选择 All actions (所有操作)，那么 *servicename*/* 的预期条目会添加到 JSON 中，但您之前选择的单个操作将保留在 JSON 中，而不会被删除。

   c. 如果要添加来自其他服务的操作，您可以选择 Statement (语句) 框顶部的 All services (所有服务)，然后根据需要重复前面两个步骤。

   d. 指定要包含在语句中的资源。

      - 在添加资源旁边，选择添加。

- 在 Add resource (添加资源) 对话框中，从列表中选择要控制其资源的服务。您只能从上一步骤选择的服务中进行选择。
- 在 Resource type (资源类型) 下，选择要控制的资源的类型。
- 最后，在 Resource ARN 中填写 Amazon Resource Name（ARN），以标识您要控制访问权限的特定资源。必须替换由大括号 {} 包围的所有占位符。您可以在资源类型的 ARN 语法允许的地方指定通配符（*）。有关可在何处使用通配符的信息，请参阅特定资源类型的文档。
- 保存您对策略添加的内容，方法是选择 Add resource (添加资源)。JSON 中的 `Resource` 元素反映了您的添加或更改。需要 Resource (资源) 元素。

> **Tip**
>
> 如果要指定选定服务的所有资源，请选择列表中的 All resources (所有资源) 选项，或者直接在 JSON 中编辑 `Resource` 语句以读取 `"Resource":"*"`。

e. （可选）要指定限制策略语句生效时间的条件，请在添加条件旁边选择添加。

- 条件键 – 从列表中，您可以选择任何可用于所有AWS服务（例如 `aws:SourceIp`）的条件键，或仅用于您为此语句选择的其中一个服务的特定于服务的键。
- 限定词 – （可选）如果为条件提供多个值（取决于特定条件键），则可指定限定词来针对值测试请求。
  - 默认值 – 根据策略中的条件键值测试请求中的单个值。如果请求中的值均与策略中的值匹配，则条件返回 true。如果策略指定了多个值，则它们将被视为“or”测试，如果请求值与任何策略值匹配，则条件返回 true。
  - 对于请求中的任何值 – 当请求可以具有多个值时，此选项测试是否有至少一个请求值与策略中的至少一个条件键值匹配。如果请求中的任何一个键值与策略中的任何一个条件值匹配，则条件返回 true。对于没有匹配的键或空数据集，条件返回 false。
  - 对于请求中的所有值 – 当请求可以具有多个值时，此选项测试是否每个请求值都与策略中的条件键值匹配。如果请求中的每个键值均与策略中的至少一个值匹配，则条件返回 true。如果请求中没有键或者键值解析为空数据集（如空字符串），则也会返回 true。
- 运算符 – 运算符指定要进行比较的类型。显示的选项取决于条件键的数据类型。例如，`aws:CurrentTime` 全局条件键允许您从任何日期比较运算符（或 `Null`）中选择，您可以使用它来测试请求中是否存在该值。

对于 Null 测试之外的任何条件运算符，您可以选择 IfExists 选项。

- 值 – (可选) 指定要测试请求的一个或多个值。

选择 Add condition (添加条件)。

有关条件键的更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

f. （可选）要使用 NotAction 元素来拒绝对所有操作（指定操作除外）的访问权限，请将左窗格中的 Action 替换为 NotAction（位于 "Effect": "Deny", 元素后）。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：操作。

6. 要添加允许 访问的语句，请执行以下操作：

a. 在左侧的 JSON 编辑器中，将行 "Effect": "Deny" 改为 "Effect": "Allow"。

当您选择右侧的选项时，JSON 编辑器会更新，以在左侧显示相应的 JSON 策略。

b. 选择服务后，将打开一个列表，其中包含该服务的可用操作。您可以选择 All actions (所有操作)，或选择要允许的一个或多个单独操作。

左侧的 JSON 将更新，以包含您选择的操作。

> **Note**
>
> 如果您选择一个单独的操作，然后返回并选择 All actions (所有操作)，那么 *servicename*/* 的预期条目会添加到 JSON 中，但您之前选择的单个操作将保留在 JSON 中，而不会被删除。

c. 如果要添加来自其他服务的操作，您可以选择 Statement (语句) 框顶部的 All services (所有服务)，然后根据需要重复前面两个步骤。

7. （可选）要向策略添加另一个语句，请选择 Add statement (添加语句) 并使用可视化编辑器构建下一条语句。

8. 添加完语句后，选择 Create policy (创建策略) 以保存已完成的 SCP。

您的新 SCP 会显示在组织的策略列表中。现在，您可以将 SCP 附加到根、OU 或账户。

AWS CLI & AWS SDKs

创建服务控制策略

您可以使用以下命令之一创建 SCP：

- AWS CLI：create-policy

  以下示例假定您有一个名为 Deny-IAM.json 的文件，其中包含 JSON 策略文本。它使用该文件创建新的服务控制策略。

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWS SDK：CreatePolicy

> **Note**
>
> SCP 在管理账户和其他部分情况中不会生效。有关更多信息，请参阅不受 SCP 限制的任务和实体。

更新 SCP

当登录到您组织的管理账户后，您可以重命名或更改策略内容。更改 SCP 的内容会立即影响所有附加账户中的任何用户、组和角色。

最小权限

若要更新 SCP，您需要运行以下操作的权限：

- `organizations:UpdatePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。
- `organizations:DescribePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。

AWS Management Console

更新策略

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在服务控制策略页面上，选择要更新的策略的名称。
3. 在策略的详细信息页面上，选择 Edit policy (编辑策略)。
4. 进行以下任何或全部更改：
   - 您可以通过在 Policy name (策略名称) 中输入新名称来重命名策略。
   - 您可以通过在 Policy description (策略说明) 中输入新文本来更改策略说明。
   - 您可以通过在左窗格中以 JSON 格式编辑策略来编辑策略文本。或者，您可以在右侧的编辑器中选择一个语句，然后使用控件更改其元素。有关每个控件的详细信息，请参阅本主题前面的创建 SCP 过程。
5. 完成后，选择 Save changes (保存更改)。

AWS CLI & AWS SDKs

更新策略

可以使用以下命令之一来更新策略：

- AWS CLI：update-policy

  以下示例重命名策略。

```
$ aws organizations update-policy \
```

```
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

以下示例添加或更改服务控制策略的说明。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

以下示例通过指定包含新 JSON 策略文本的文件来更改 SCP 的策略文档。

```
$ aws organizations update-policy \
```

```
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWS SDK：UpdatePolicy

有关更多信息

有关创建 SCP 的更多信息，请参阅以下主题：

- 服务控制策略示例
- SCP 语法

编辑附加到 SCP 的标签

当您登录到组织的管理账户时，您可以添加或删除附加到 SCP 的标签。有关标记的更多信息，请参阅为 AWS Organizations 资源添加标签。

> **最小权限**
>
> 要编辑附加到AWS组织中 SCP 的标签，您必须拥有以下权限：
>
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
> - `organizations:DescribePolicy` – 仅当使用 Organizations 控制台时才需要
> - `organizations:TagResource`

- `organizations:UntagResource`

AWS Management Console

编辑附加到 SCP 的标签

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Service control policies (服务控制策略) 页面上，选择带有您想要编辑的标签的策略名称。
3. 在策略详细信息页面上，选择 Tags (标签) 选项卡，然后选择 Manage tags (管理标签)。
4. 进行以下任何或全部更改：
   - 更改标签的值，方法是在旧标签上输入新值。您不能直接修改标签键。要更改键，您必须删除带有旧键的标签，然后添加使用新键的标签。
   - 删除任何现有的标签，方法是选择 Remove (删除)。
   - 添加新的标签键和值对。选择 Add tag (添加标签)，然后在提供的框中输入新的键名称和可选值。如果您将 Value (值) 框留空，则值是空字符串；它并非 `null`。
5. 完成后，选择 Save changes (保存更改)。

AWS CLI & AWS SDKs

编辑附加到 SCP 的标签

您可以使用以下命令之一编辑附加到 SCP 的标签：

- AWS CLI：tag-resource 和 untag-resource
- AWS SDK：TagResource 和 UntagResource

删除 SCP

当登录到您组织的管理账户时，您可以删除您的组织中不再需要的策略。

> **注意**
>
> - 必须先将某个策略从所有附加实体中分离，然后才能删除该策略。

- 您无法删除任何AWS托管的 SCP，例如名为 `FullAWSAccess` 的 SCP。

最小权限

若要删除 SCP，您需要运行以下操作的权限：

- `organizations:DeletePolicy`

AWS Management Console

删除 SCP

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Service control policies (服务控制策略) 页面上，选择要删除的 SCP 的名称。
3. 要删除的策略必须先从所有根、OU 和账户分离。选择 Targets (目标) 选项卡，选择显示在 Targets (目标) 列表中的每个根、OU 或账户旁边的单选按钮，然后选择 Detach (分离)。在确认对话框中，选择 Detach (分离)。重复操作，直到删除所有目标。
4. 在页面的顶部，选择 Delete (删除)。
5. 在确认对话框上，输入策略的名称，然后选择 Delete (删除)。

AWS CLI & AWS SDKs

删除 SCP

可以使用以下命令之一删除策略：

- AWS CLI：delete-policy

  以下示例删除指定 SCP。

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  如果成功，此命令不会产生任何输出。
- AWS SDK：DeletePolicy

附加和分离服务控制策略

登录到组织的管理账户时，您可以附加以前创建的服务控制策略（SCP）。您可以将 SCP 附加到组织根、组织部门（OU）或直接附加到账户。要创建 SCP，请完成以下步骤。

> **最小权限**
>
> 要将 SCP 附加到根、OU 或账户，您需要运行以下操作的权限：
>
> - `organizations:AttachPolicy`，且同一条策略语句中有一个 `Resource` 元素包含“*”、指定策略的 Amazon Resource Name（ARN）或是您要附加该策略的根、OU 或账户的 ARN。

AWS Management Console

您可以导航到要附加策略的根、OU 或账户，为其附加 SCP。

通过导航到根、OU 或账户来附加 SCP

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，导航到要将 SCP 附加到的根、OU 或账户，并选择其旁边的复选框。您可能需要展开 OU（选择 ▶ ）以查找所需的 OU 或账户。
3. 在 Policies (策略) 选项卡上的 Service control policies (服务控制策略) 条目中，选择 Attach (附加)。
4. 找到所需的策略，然后选择 Attach policy (附加策略)。

   Policies (策略) 选项卡上的附加的 SCP 列表会更新，以包含新添加的内容。策略更改会立即影响所附加的根或 OU 下方的所附加账户或所有账户中 IAM 用户和角色的权限。

通过导航到策略来附加 SCP

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Service control policies (服务控制策略) 页面上，选择要附加的策略的名称。

3. 在 Targets (目标) 选项卡上，选择 Attach (附加)。
4. 选择要附加策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OU (选择) 以查找所需的 OU 或账户。
5. 选择附加策略。

   Targets (目标) 选项卡上的附加的 SCP 列表会更新，以包含新添加的内容。策略更改会立即影响所附加的根或 OU 下方的所附加账户或所有账户中 IAM 用户和角色的权限。

AWS CLI & AWS SDKs

通过导航到根、OU 或账户来附加 SCP

您可以使用以下命令之一附加 SCP：

- AWS CLI：attach-policy

  以下示例将 SCP 附加到 OU。

  ```
  $ aws organizations attach-policy \
      --policy-id p-i9j8k7l6m5 \
      --target-id ou-a1b2-f6g7h222
  ```

  如果成功，此命令不会产生任何输出。
- AWS 软件开发工具包：AttachPolicy

策略更改会立即影响所附加的根或 OU 下方的所附加账户或所有账户中 IAM 用户和角色的权限。

从组织根、OU 或账户分离 SCP

当您登录到组织的管理账户时，您可以从 SCP 所附加到的组织根、OU 或账户分离 SCP。将 SCP 与实体分离后，该 SCP 将不再适用于受现已分离的实体影响的任何 IAM 用户和 IAM 角色。要分离 SCP，请完成以下步骤。

> **Note**
>
> 您无法从根、OU 或账户分离最后一个 SCP。每个根、OU 和账户必须始终附加有至少一个 SCP。

> **最小权限**
>
> 要从根、OU 或账户分离 SCP，您需要运行以下操作的权限：
>
> - `organizations:DetachPolicy`

AWS Management Console

您可以导航到要从中分离策略的根、OU 或账户，为其分离 SCP。

通过导航到已附加策略的根、OU 或账户来分离 SCP

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面导航到要分离策略的根、OU 或账户。您可能需要展开 OU（选择 ）以查找所需的 OU 或账户。选择根、OU 或账户的名称。
3. 在 Policies (策略) 选项卡上，选择要分离的 SCP 旁边的单选按钮，然后选择 Detach (分离)。
4. 在确认对话框中，选择 Detach policy (分离策略)。

   附加 SCP 的列表更新。分离 SCP 引起的策略更改立即生效。例如，分离 SCP 会立即影响以前附加的账户或以前附加的组织根或 OU 下的账户中 IAM 用户和角色的权限。

通过导航到策略来分离 SCP

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Service control policies (服务控制策略) 页面上，选择要从根、OU 或账户分离的策略的名称。
3. 在 Targets (目标) 选项卡上，选择要分离策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OU（选择

)

以查找所需的 OU 或账户。

4. 选择分离。
5. 在确认对话框中，选择 Detach (分离)。

   附加 SCP 的列表更新。分离 SCP 引起的策略更改立即生效。例如，分离 SCP 会立即影响以前附加的账户或以前附加的组织根或 OU 下的账户中 IAM 用户和角色的权限。

AWS CLI & AWS SDKs

从根、OU 或账户分离 SCP

您可以使用以下命令之一分离 SCP：

- AWS CLI：detach-policy

  以下示例将指定的 SCP 与指定的 OU 分离。

```
$ aws organizations detach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

- AWS 软件开发工具包：DetachPolicy

策略更改会立即影响所附加的根或 OU 下方的所附加账户或所有账户中 IAM 用户和角色的权限

SCP 评估

> **Note**
>
> 此部分中的信息不适用于管理策略类型，包括 AI 服务选择退出策略、备份策略或标签策略。有关更多信息，请参阅了解管理策略继承。

由于您可以在 AWS Organizations 中的不同级别附加多个服务控制策略 (SCP)，因此了解 SCP 的评估方式可以帮助您编写产生正确结果的 SCP。

主题

- SCP 如何与“允许”配合使用
- SCP 如何使用“拒绝”
- 使用 SCP 的策略

SCP 如何与“允许”配合使用

要允许特定账户获得权限，在从根到账户直接路径中的每个 OU（包括目标账户本身），每个级别都必须有显式**Allow**语句。这就是为什么在您启用 SCP 时，AWS Organizations 会附加一个名为 FullAWSAccess 的 AWS 托管 SCP 策略，该策略允许所有服务和操作。如果该策略在组织的任何级别被删除而未被替换，那么该级别下的所有 OU 和账户都将被阻止采取任何行动。

例如，我们来看一下图 1 和图 2 所示的场景。要允许账户 B 获得权限或服务，应将允许该权限或服务的 SCP 附加到根、生产 OU 和账户 B 本身。

SCP 评估遵循“默认拒绝”模式，这意味着 SCP 中未明确允许的任何权限都将被拒绝。如果在任何级别（例如根、生产 OU 或账户 B）的 SCP 中不存在允许语句，则访问将被拒绝。

> **注意**
>
> - SCP 中的 `Allow` 语句允许 `Resource` 元素仅包含一个 `"*"` 条目。
> - SCP 中的 `Allow` 语句完全不能有 `Condition` 元素。

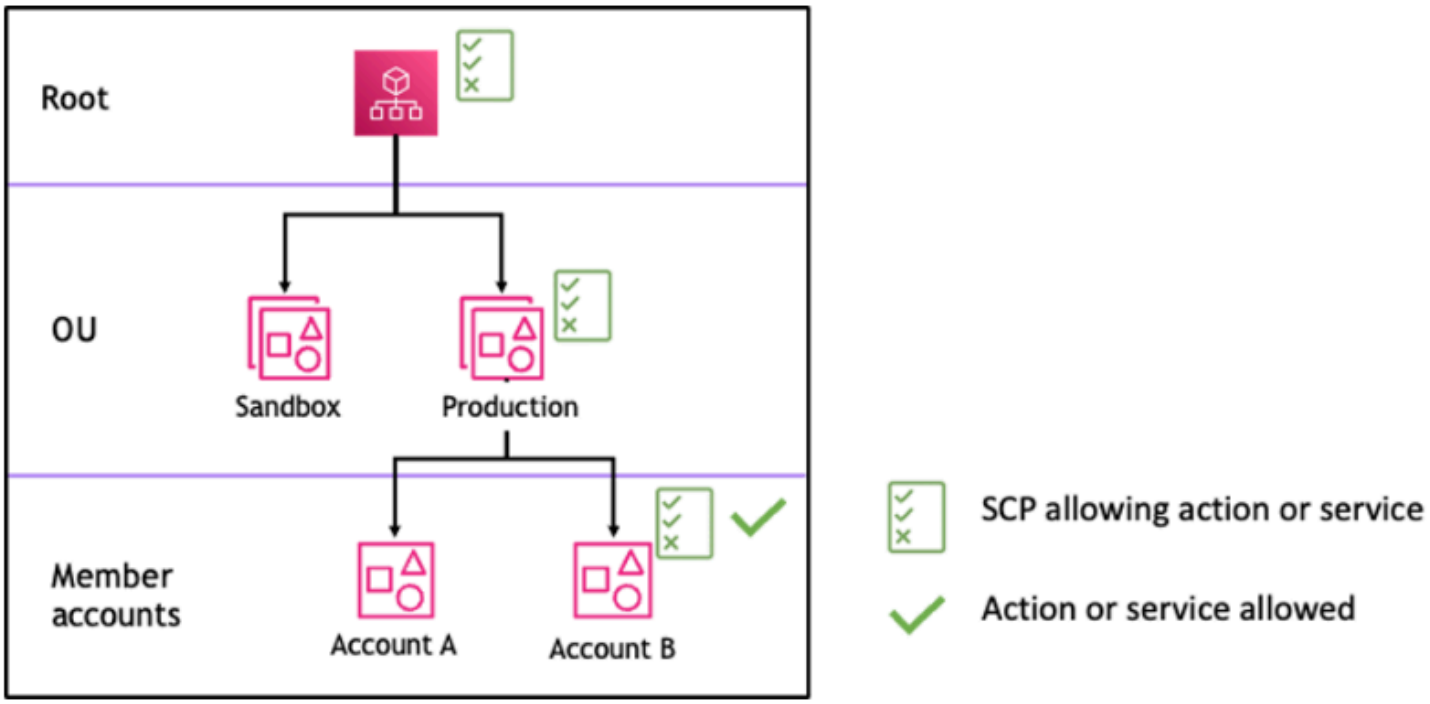


图 1：在根、生产 OU 和账户 B 处附加 *Allow* 语句的组织结构示例

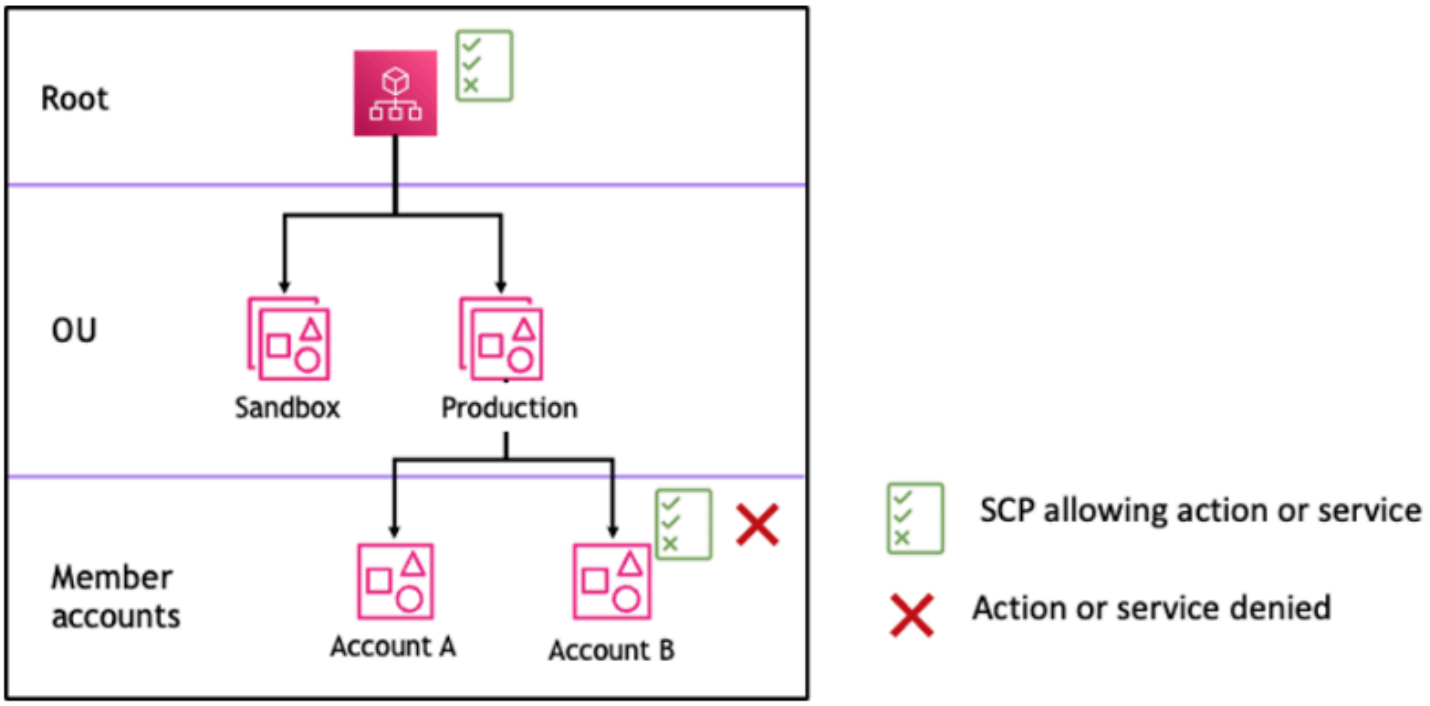


图 2：生产 OU 中缺少 *Allow* 语句的组织结构示例及其对账户 B 的影响

SCP 如何使用“拒绝”

要拒绝特定账户获得权限，在从根到账户直接路径中的每个 OU（包括目标账户本身），任何 SCP 都可以拒绝该权限。

例如，假设有一个 SCP 附加到生产 OU，它为给定服务指定了显式 Deny 语句。碰巧还有另一个 SCP 附加到根和账户 B，它显式允许访问相同的服务，如图 3 所示。因此，账户 A 和账户 B 都将被拒绝访问该服务，因为附加到组织中任何级别的拒绝策略都会针对其下的所有 OU 和成员账户进行评估。

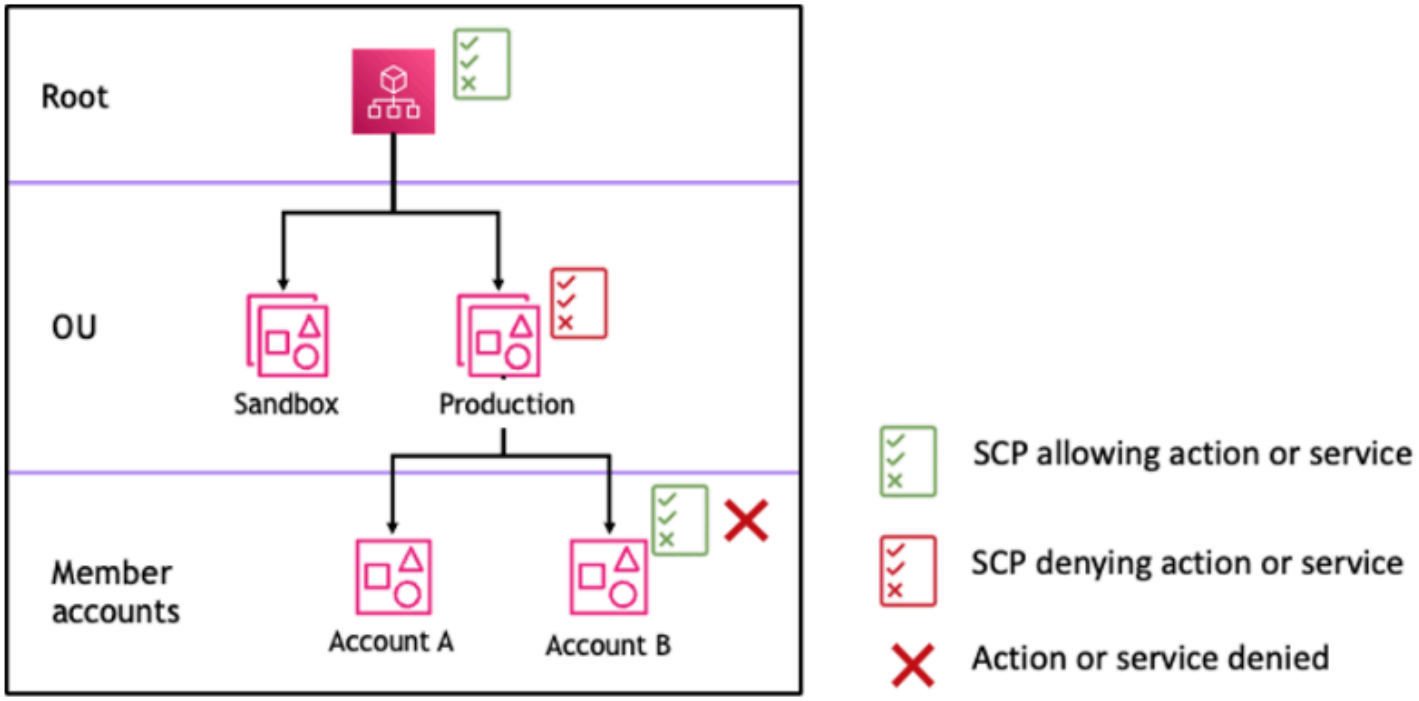


图 3：生产 OU 中附加了 *Deny* 语句的组织结构示例及其对账户 B 的影响

使用 SCP 的策略

在编写 SCP 时，您可以结合使用 `Allow` 和 `Deny` 语句来允许在组织中执行预期操作和服务。`Deny` 语句是实施限制的一种强大方式，应该适用于组织或 OU 更广泛的部分，因为当它们应用于根级或 OU 级别时，会影响其下的所有账户。

例如，您可以使用 [阻止成员账户退出组织] 在根级别实施策略，该策略将对组织中的所有账户有效。拒绝语句还支持条件元素，这有助于创建例外情况。

> **Tip**
>
> 您可以使用 IAM 中服务上次访问的数据来更新您的 SCP，以限制仅访问您需要的AWS服务。有关更多信息，请参阅《IAM 用户指南》中的查看 Organizations 的 Organizations 服务上次访问的数据。

在创建每个根、OU 和账户时，AWS Organizations 会将名为 FullAWSAccess 的 AWS 托管 SCP 附加到该根、OU 和账户。此策略允许所有服务和操作。您可以将 FullAWSAccess 替换为仅允许一组服务的策略，这样除非通过更新 SCP 来显式允许使用新的 AWS 服务，否则不允许使用这些服务。例如，如果您的组织只想允许在您的环境中使用部分服务，则可以使用 `Allow` 语句来仅允许特定服务。

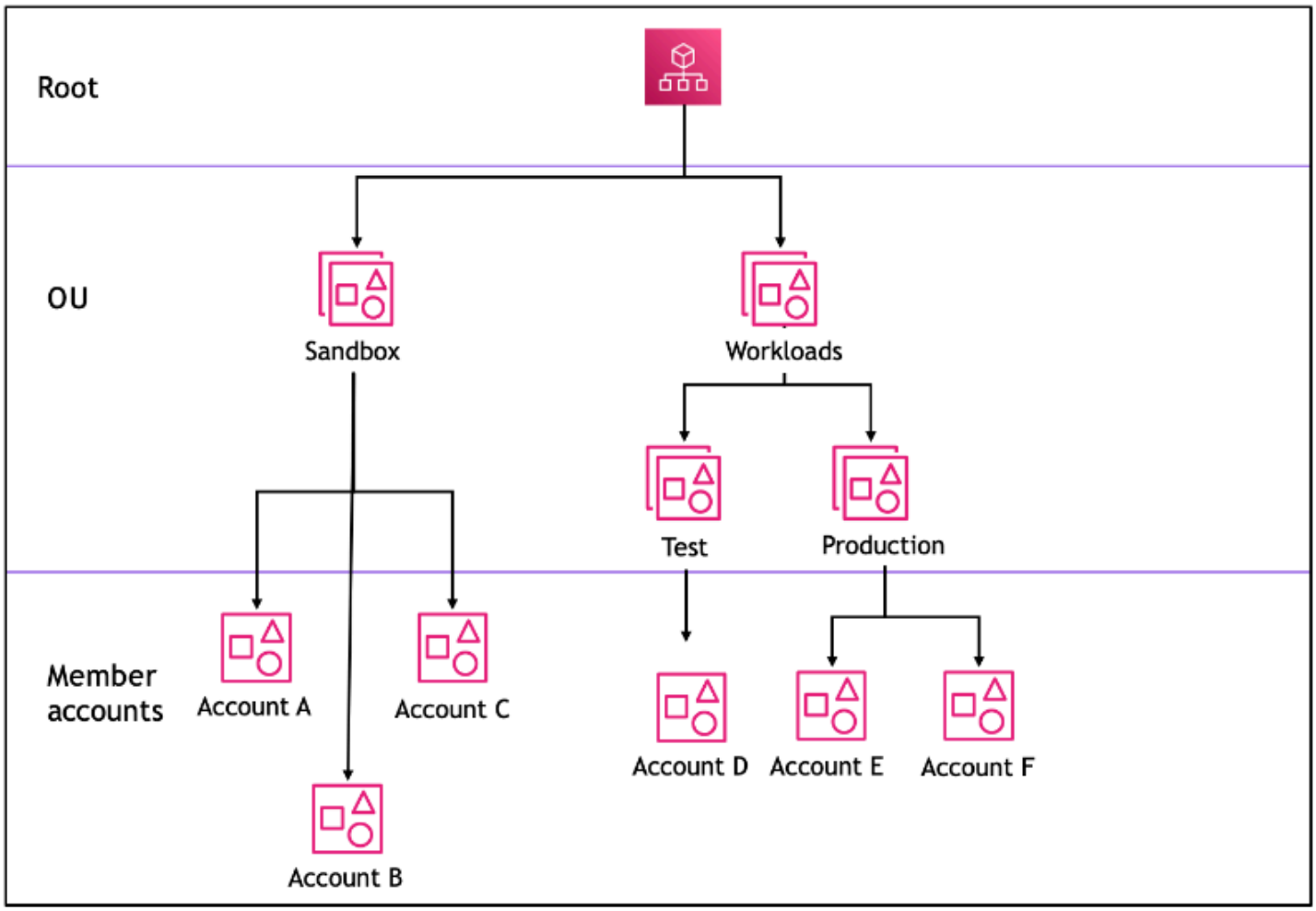
```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

将两个语句组合在一起的策略可能与以下示例类似，它阻止成员账户离开组织并允许使用所需的 AWS 服务。组织管理员可以分离 FullAWSAccess 策略并改为附加此策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

现在，考虑以下示例组织结构，以了解如何在组织的不同级别应用多个 SCP。



下表显示了沙盒 OU 中的有效策略。

情况	根处的 SCP	沙盒 OU 处的 SCP	账户 A 处的 SCP	账户 A 处生成的策略	账户 B 和账户 C 处生成的策略
1	完全 AWS 访问	完全 AWS 访问 + 拒绝 S3 访问	完全 AWS 访问 + 拒绝 EC2 访问	没有 S3，没有 EC2 访问	没有 S3 访问
2	完全 AWS 访问	允许 Amazon Elastic Compute Cloud (Amazon EC2) 访问	允许 EC2 访问	仅允许 EC2 访问	仅允许 EC2 访问
3	拒绝 S3 访问	允许 S3 访问	完全 AWS 访问	无服务访问	无服务访问

下表显示了工作负载 OU 中的有效策略。

情况	根处的 SCP	工作负载 OU 处的 SCP	测试 OU 处的 SCP	账户 D 处生成的策略	生产 OU、账户 E 和账户 F 处生成的策略
1	完全 AWS 访问	完全 AWS 访问	完全 AWS 访问 + 拒绝 EC2 访问	没有 EC2 访问	完全 AWS 访问
2	完全 AWS 访问	完全 AWS 访问	允许 EC2 访问	允许 EC2 访问	完全 AWS 访问
3	拒绝 S3 访问	完全 AWS 访问	允许 S3 访问	无服务访问	无服务访问

SCP 语法

服务控制策略 (SCP) 使用的语法与 (IAM) 权限策略和基于资源的策略 AWS Identity and Access Management （ 如 Amazon S3 存储桶策略 ）使用的语法类似。有关 IAM 策略及其语法的更多信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html中的 IAM 策略概述。

SCP 是一个纯文本文件，根据 JSON 的规则设置结构。它使用本主题中所述的元素。

> **Note**
>
> SCP 中的所有字符将计入其最大大小。本指南中的示例演示了使用额外空格编排格式的 SCP，以提高其可读性。但是，在您的策略大小接近最大大小时，可以删除任何空格（例如，引号之外的空格字符和换行符）来节省空间。

有关 SCP 的一般信息，请参阅服务控制策略 (SCP)。

元素摘要

下表总结了可在 SCP 中使用的策略元素。一些策略元素仅在拒绝操作的 SCP 中可用。Supported effects (支持的效果) 列中列出了可用于 SCP 中的每个策略元素的效果类型。

元素	用途	支持的效果
版本	指定要用于处理策略的语言语法规则。	`Allow, Deny`
Statement	充当策略元素的容器。您可以在 SCP 中拥有多个语句。	`Allow, Deny`

元素	用途	支持的效果
Statement ID (Sid)	（可选）提供语句的友好名称。	`Allow`, `Deny`
效果	定义 SCP 语句是允许还是拒绝账户中的 IAM 用户和角色访问权限。	`Allow`, `Deny`
操作	指定 SCP 允许或拒绝的 AWS 服务和操作。	`Allow`, `Deny`
NotAction	指定免受 SCP 限制的 AWS 服务和操作。用来代替 `Action` 元素。	`Deny`
资源	指定 SCP 适用的 AWS 资源。	`Deny`

元素	用途	支持的效果
Condition	指定语句何时生效的条件。	Deny

以下部分提供了有关如何在 SCP 中使用策略元素的更多信息和示例。

`Version` 元素

每个 SCP 必须包含 `Version` 元素，其值为 `"2012-10-17"`。此版本值与 IAM 权限策略的最新版本相同。

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

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：版本。

`Statement` 元素

一个 SCP 可包含一个或多个 `Statement` 元素。一条策略中只能有一个 `Statement` 关键字，但其值可以是 JSON 语句数组 (使用 [ ] 字符括起)。

以下示例演示包含单个 `Effect`、`Action` 和 `Resource` 元素的语句。

```
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
```

以下示例包括作为一个 `Statement` 元素中的数组列表的两个语句。第一条语句允许所有操作，第二条语句拒绝任何 EC2 操作。结果是账户中的管理员可以委派除了 Amazon Elastic Compute Cloud（Amazon EC2）的权限之外的任意权限。

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
```

```
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
```

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：语句。

Statement ID (`Sid`) 元素

`Sid` 是您针对策略语句提供的可选标识符。您可以为语句数组中的每个语句指定 `Sid` 值。以下示例 SCP 显示了一个示例 `Sid` 语句。

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
}
```

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：ID。

`Effect` 元素

每个语句必须包含一个 `Effect` 元素。该值可以是 `Allow` 或 `Deny`。它会影响在同一个语句中列出的任意操作。

有关更多信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_effect.html中的 IAM JSON 策略元素：效果。

`"Effect": "Allow"`

以下示例演示带有一条语句的 SCP，该语句包含一个 `Effect` 元素，其值为 `Allow`，表示允许账户用户执行 Amazon S3 服务的操作。对于使用允许列表策略（已经分离了所有默认 `FullAWSAccess` 策略使得默认情况下默示拒绝权限）的组织，此示例非常有用。结果是语句允许任何附加账户的 Amazon S3 权限：

```
{
    "Statement": {
```

```
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "*"
    }
}
```

即使它使用与 IAM 权限策略相同的 `Allow` 值关键字，在 SCP 中它也不会实际授予用户执行任何操作的权限。相反，SCP 充当筛选器，用于指定组织中 IAM 用户和 IAM 角色的最大权限。在前面的示例中，即使账户中的用户已经附加了 `AdministratorAccess` 托管式策略，SCP 也会将受影响账户中的所有用户限制为只能执行 Amazon S3 操作。

"Effect": "Deny"

在 `Effect` 元素具有值 `Deny` 的语句中，您还可以限制对特定资源的访问，或者定义 SCP 何时生效的条件。

以下显示了有关如何在拒绝语句中使用条件密钥的示例。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

SCP 中的此语句设置一个防护机制来阻止受影响的账户（其中，SCP 附加到账户本身或包含该账户的组织根或 OU）启动 Amazon EC2 实例（如果 Amazon EC2 实例未设置为 `t2.micro`）。即使将允许此操作的 IAM 策略附加到账户，SCP 所创建的防护机制也会阻止它。

Action 和 NotAction 元素

每个语句必须包含下列项目之一：

- 在允许和拒绝语句中，为 `Action` 元素。
- 仅在拒绝语句中（其中，`Effect` 元素的值为 `Deny`），为 `Action` 或 `NotAction` 语句。

Action或NotAction元素的值是一个字符串列表（JSON 数组），用于标识语句允许或拒绝的 AWS 服务和操作。

所有字符串均包含服务简写（例如“s3”、“ec2”、“iam”或“organizations”），全小写，后跟冒号，然后是该服务的操作。这些操作和通知区分大小写，必须按照各个服务的文档中所示键入。通常，其键入方式为每个单词的开头是大写字母，其余为小写字母。例如："s3:ListAllMyBuckets"。

您也可以在 SCP 中使用星号（*）或问号（？）等通配符：

- 使用星号（*）通配符以匹配名称中包含相同部分的多个操作。值 "s3:*" 表示 Amazon S3 服务中的所有操作。值 "ec2:Describe*" 仅与以“Describe”开头的 EC2 操作匹配。
- 使用问号（？）通配符来匹配单个字符。

> **Note**
>
> 在 SCP 中，Action 或 NotAction 参数中的通配符（*）和（？）只能单独使用或放在字符串结尾处。它不能出现在字符串的开头或中间部分。因此，"servicename:action*" 是有效的，但 "servicename:*action" 和 "servicename:some*action" 在 SCP 中都是无效的。

有关所有服务及其在 AWS Organizations SCP 和 IAM 权限策略中支持的操作的列表，请参阅 IA M 用户指南中的AWS 服务操作、资源和条件密钥。

有关更多信息，请参阅 IAM 用户指南中的 IA M JSON 策略元素： NotAction操作和 IAM JSON 策略元素：

Action 元素的示例

以下示例演示带有一条语句的 SCP，该语句允许账户管理员在账户中委派 EC2 实例的描述、启动、停止和终止权限。这是另一个允许列表示例，这在未附加默认 Allow * 策略时非常有用，因此，在默认情况下，权限将被隐式拒绝。如果默认 Allow * 策略仍附加到以下策略所附加到的根、OU 或账户，则以下策略没有任何效果。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
```

```
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
    }
}
```

以下示例演示如何通过拒绝访问您不希望用于所附加账户中的服务。它假定默认 "Allow *" SCP 仍附加到所有 OU 和根。此示例策略阻止所附加账户中的账户管理员委派 IAM、Amazon EC2 和 Amazon RDS 服务的任何权限。只要没有其他已附加策略拒绝，就可以委派来自其他服务的任何操作。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
}
```

NotAction 元素的示例

以下示例说明如何使用NotAction元素将 AWS 服务排除在策略的影响之外。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
         }
       }
     }
   ]
}
```

使用此声明，除非使用 IAM 操作 AWS 区域，否则受影响的账户只能在指定范围内执行操作。

`Resource` 元素

在 `Effect` 元素具有值 `Allow` 的语句中，您只能在 SCP 的 `Resource` 元素中指定“*”。您不能指定单个资源 Amazon Resource Name（ARN）。

您也可以在 resource 参数中使用星号（*）或问号（？）等通配符：

- 使用星号（*）通配符以匹配名称中包含相同部分的多个操作。
- 使用问号（？）通配符来匹配单个字符。

在 `Effect` 元素具有值 `Deny` 的语句中，您可以 指定单个 ARN，如以下示例所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToAdminRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

此 SCP 阻止受影响账户中的 IAM 用户和角色对在组织的所有账户中创建的常见管理 IAM 角色进行更改。

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：资源。

Condition 元素

您可以在 SCP 中的拒绝语句中指定 Condition 元素。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

此 SCP 拒绝对 eu-central-1 和 eu-west-1 区域之外的任何操作的访问，但列出的服务中的操作除外。

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

不支持的元素

SCP 中不支持以下元素：

- Principal
- NotPrincipal

- `NotResource`

服务控制策略示例

本主题中显示的示例服务控制策略 (SCP) 仅供参考。

> **在使用这些示例之前**
>
> 在组织中使用这些示例 SCP 之前，请执行以下操作：
>
> - 仔细检查并根据您的独特需求定制 SCP。
> - 使用您所用的AWS服务彻底测试您环境中的 SCP。
>
> 本部分中的示例策略演示 SCP 的实施和使用。这些示例策略并不是要完全按照所示实施的官方AWS建议或最佳实践。您有责任仔细测试任何基于拒绝的策略，以确定其是否适合解决环境的业务需求。基于拒绝的服务控制策略可能会无意中限制或阻止您使用AWS服务，除非您在策略中添加了必要的例外情况。有关此类例外情况的示例，请参阅第一个示例，该示例从阻止访问不需要的AWS 区域规则中将全球服务豁免。
> - 请记住，SCP 影响所附加到的每个账户中的每个用户和角色以及根用户。

> **Tip**
>
> 您可以使用 IAM 中服务上次访问的数据来更新您的 SCP，以限制仅访问您需要的AWS服务。有关更多信息，请参阅《IAM 用户指南》中的查看 Organizations 的 Organizations 服务上次访问的数据。

以下每个策略是拒绝列表策略战略的示例。附加拒绝列表策略时还必须附加在受影响账户中允许已批准的操作的其他策略。例如，默认 `FullAWSAccess` 策略允许在账户中使用所有服务。此策略默认附加到根、所有组织部门 (OU) 和所有账户。它实际上不授予权限；SCP 也不授予权限。相反，它使该账户中的管理员能够委派对这些操作的访问权限，方法是将标准 AWS Identity and Access Management（IAM）权限策略附加到账户中的用户、角色或组。然后，其中每个拒绝列表策略通过阻止访问指定服务或操作来覆盖任何策略。

示例

- 一般示例

- 根据请求的AWS 区域拒绝访问AWS
- 阻止 IAM 用户和角色进行某些更改
- 阻止 IAM 用户和角色进行指定的更改，但指定管理员角色除外
- 要求 MFA 执行 API 操作
- 阻止根用户的服务访问
- 阻止成员账户退出组织

- Amazon CloudWatch 的示例 SCP
  - 阻止用户禁用 CloudWatch 或更改其配置
- AWS Config 的示例 SCP
  - 阻止用户禁用 AWS Config 或更改其规则
- Amazon Elastic Compute Cloud（Amazon EC2）的示例 SCP
  - 需要 Amazon EC2 实例以使用特定类型
  - 防止在没有 IMDSv2 的情况下启动 EC2 实例
  - 防止禁用默认 Amazon EBS 加密
- Amazon GuardDuty 的示例 SCP
  - 阻止用户禁用 GuardDuty 或修改其配置
- AWS Resource Access Manager 的示例 SCP
  - 阻止外部共享
  - 允许特定账户仅共享指定的资源类型
  - 阻止与组织或组织部门（OU）共享
  - 仅允许与指定的 IAM 用户和角色共享
- Amazon Route 53 应用程序恢复控制器 SCP 示例
  - 防止用户更新 Route 53 ARC 路由控制状态
- 适用于 Amazon S3 的 SCP 示例
  - 防止上传 Amazon S3 未加密对象
- 标记资源的示例 SCP
  - 需要在指定的已创建资源上使用标签
  - 阻止标记被修改，除非由授权委托人修改
- Amazon Virtual Private Cloud（Amazon VPC）的示例 SCP
  - 阻止用户删除 Amazon VPC 流日志

- 阻止还没有 Internet 访问权的任何 VPC 获取它

一般示例

根据请求的AWS 区域拒绝访问AWS

此 SCP 拒绝对特定区域之外的任何操作的访问。使用您要使用的AWS 区域替换 `eu-central-1` 和 `eu-west-1`。它为已批准的全局服务中的操作提供了豁免。此示例还说明如何豁免由两个指定管理员角色中的任何一个发出的请求。

> **Note**
>
> 要将区域拒绝 SCP 与 AWS Control Tower 一起使用，请参阅 根据请求的AWS 区域拒绝访问AWS。

此策略使用 `Deny` 效果来拒绝访问不是针对两个批准区域（`eu-central-1` 和 `eu-west-1`）之一的操作的所有请求。通过 NotAction 元素，您可以列出其操作（或单个操作）不受此限制约束的服务。由于全球服务具有由 `us-east-1` 区域物理托管的终端节点，因此必须以这种方式豁免它们。借助以这种方式构建的 SCP，如果所请求的服务包含在 `NotAction` 元素中，则允许对 `us-east-1` 区域中的全局服务发出的请求。此示例策略拒绝对 `us-east-1` 区域中的服务的任何其他请求。

> **Note**
>
> 此示例可能未包含所有最新的全局 AWS 服务或操作。将服务和操作列表替换为由组织中的账户使用的全球服务。
>
> > **提示**
> >
> > 您可以在 IAM 控制台中查看服务上次访问的数据，以确定您的组织使用哪些全球服务。IAM 用户、组或角色的详细信息页面上的 Access Advisor (访问顾问) 选项卡显示该实体已使用的AWS服务，并按最近的访问顺序进行排序。

注意事项

- AWS KMS 和 AWS Certificate Manager 支持区域终端节点。但是，如果您想将它们与 Amazon CloudFront 等全球服务一起使用，则必须将它们包含在以下示例 SCP 的全球服务排除列表中。像 Amazon CloudFront 这样的全球服务通常需要访问位于同一区域的 AWS KMS 和 ACM，对于全球服务来说，这是美国东部（弗吉尼亚北部）区域（`us-east-1`）。
- 默认情况下，AWS STS 是全球服务，必须包含在全球服务排除列表中。不过，您可以启用 AWS STS 来使用区域终端节点而不是单个全局终端节点。如果执行此操作，则可以从以下示例 SCP 中的全球服务豁免列表中删除 STS。有关更多信息，请参阅在AWS 区域中管理 AWS STS。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
```

```
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

阻止 IAM 用户和角色进行某些更改

此 SCP 阻止 IAM 用户和角色对在组织的所有账户中创建的特定 IAM 角色进行更改。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}
```

阻止 IAM 用户和角色进行指定的更改，但指定管理员角色除外

此 SCP 基于前面的示例为管理员创建例外。它阻止受影响账户中的 IAM 用户和角色对在组织的所有账户中创建的常见管理 IAM 角色进行更改，但使用指定角色的管理员除外。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessWithException",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
```

```
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

要求 MFA 执行 API 操作

使用如下所示的 SCP，要求先启用多重身份验证（MFA），之后 IAM 用户和角色才能执行操作。在此示例中，操作是停止 Amazon EC2 实例。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

阻止根用户的服务访问

以下策略限制对成员账户中根用户指定操作的所有访问权限。如果要阻止您的账户以特定方式使用根凭证，请将您自己的操作添加到此策略中。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

阻止成员账户退出组织

以下策略阻止使用 LeaveOrganization API 操作，以便成员账户的管理员无法从组织中删除其账户。

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

Amazon CloudWatch 的示例 SCP

此类别中的示例

- 阻止用户禁用 CloudWatch 或更改其配置

阻止用户禁用 CloudWatch 或更改其配置

低级 CloudWatch 操作员需要监控控制面板和警报。但不得删除或更改高级人员可能设置的任何控制面板或警报。此 SCP 阻止任何受影响账户中的用户或角色运行可删除或更改您的控制面板或警报的任何 CloudWatch 命令。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Config 的示例 SCP

此类别中的示例

- 阻止用户禁用 AWS Config 或更改其规则

阻止用户禁用 AWS Config 或更改其规则

此 SCP 阻止任何受影响账户中的用户或角色运行可禁用 AWS Config 或更改其规则或触发器的 AWS Config 操作。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon Elastic Compute Cloud（Amazon EC2）的示例 SCP

此类别中的示例

- 需要 Amazon EC2 实例以使用特定类型
- 防止在没有 IMDSv2 的情况下启动 EC2 实例
- 防止禁用默认 Amazon EBS 加密

需要 Amazon EC2 实例以使用特定类型

借助此 SCP，任何不使用 `t2.micro` 实例类型启动的实例都将被拒绝。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
```

```
    }
  ]
}
```

防止在没有 IMDSv2 的情况下启动 EC2 实例

以下策略限制所有用户在没有 IMDSv2 的情况下启动 EC2 实例。

```
[
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "StringNotEquals":{
            "ec2:MetadataHttpTokens":"required"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "NumericGreaterThan":{
            "ec2:MetadataHttpPutResponseHopLimit":"3"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
```

```
]
```

以下策略限制所有用户在没有 IMDSv2 的情况下启动 EC2 实例，但允许特定 IAM 身份修改实例元数据选项。

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalARN": [
```

```
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
      }
    }
  }
]
```

防止禁用默认 Amazon EBS 加密

以下策略限制所有用户禁用默认 Amazon EBS 加密。

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

Amazon GuardDuty 的示例 SCP

此类别中的示例

- 阻止用户禁用 GuardDuty 或修改其配置

阻止用户禁用 GuardDuty 或修改其配置

此 SCP 阻止任何受影响账户中的用户或角色直接以命令形式或通过控制台禁用 GuardDuty 或更改其配置。它有效地允许对 GuardDuty 信息和资源进行只读访问。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:AcceptInvitation",
                "guardduty:ArchiveFindings",
                "guardduty:CreateDetector",
                "guardduty:CreateFilter",
                "guardduty:CreateIPSet",
                "guardduty:CreateMembers",
                "guardduty:CreatePublishingDestination",
```

```
                "guardduty:CreateSampleFindings",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteDetector",
                "guardduty:DeleteFilter",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeletePublishingDestination",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
                "guardduty:UpdatePublishingDestination",
                "guardduty:UpdateThreatIntelSet"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Resource Access Manager 的示例 SCP

此类别中的示例

- 阻止外部共享
- 允许特定账户仅共享指定的资源类型
- 阻止与组织或组织部门（OU）共享
- 仅允许与指定的 IAM 用户和角色共享

阻止外部共享

以下示例 SCP 阻止用户创建允许与不属于组织的 IAM 用户和角色共享的资源共享。

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

允许特定账户仅共享指定的资源类型

以下 SCP 允许账户 111111111111 和 222222222222 创建共享前缀列表的资源共享，并将前缀列表与现有资源共享相关联。

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

```
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

阻止与组织或组织部门（OU）共享

以下 SCP 阻止用户创建与AWS组织或 OU 共享资源的资源共享。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

仅允许与指定的 IAM 用户和角色共享

以下示例 SCP 允许用户仅与组织 o-12345abcdef、组织部门 ou-98765fedcba 和账户 111111111111 共享资源。

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

```
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
                }
            }
        }
    ]
}
```

Amazon Route 53 应用程序恢复控制器 SCP 示例

此类别中的示例

- 防止用户更新 Route 53 ARC 路由控制状态

防止用户更新 Route 53 ARC 路由控制状态

低级别 Route 53 ARC 操作员需要监控控制面板并查看 Route 53 ARC 信息。但是，操作员不得更新路由控制以将应用程序从一个 AWS 区域 故障转移到另一个，而高级操作员可能允许进行此操作。此 SCP 阻止任何受影响账户中的用户或角色运行可更新 Route 53 ARC 路由控制的 Route 53 ARC 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAll",
            "Effect": "Deny",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

适用于 Amazon S3 的 SCP 示例

此类别中的示例

- 防止上传 Amazon S3 未加密对象

防止上传 Amazon S3 未加密对象

以下策略限制所有用户将未加密的对象上传到 S3 存储桶。

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

以下策略限制所有用户将未加密的对象上传到 S3 存储桶，并且对其存储桶中的对象上传强制执行指定的加密类型（AES256 或 aws:kms）。

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
```

```
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

标记资源的示例 SCP

此类别中的示例

- 需要在指定的已创建资源上使用标签
- 阻止标记被修改，除非由授权委托人修改

需要在指定的已创建资源上使用标签

如果请求不包含指定的标签，以下 SCP 将阻止受影响账户中的 IAM 用户和角色创建特定资源类型。

> **Important**
>
> 请务必使用您在环境中使用的服务测试基于拒绝的策略。以下示例是创建未标记的密钥或运行未标记的 Amazon EC2 实例的简单块，不包括任何例外。
> 以下示例策略与 AWS CloudFormation 不兼容，因为该服务会创建一密钥，然后将其标记为两个单独的步骤。此示例策略有效地阻止 AWS CloudFormation 将密钥作为堆栈的一部分创建，因为这样的操作会导致出现没有按要求被标记的密钥。

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

```
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
```

```
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
  ]
}
```

有关 AWS Organizations SCP 和 IAM 权限策略中均支持的所有服务和操作的列表，请参阅《IAM 用户指南》中的AWS服务的操作、资源和条件键。

阻止标记被修改，除非由授权委托人修改

以下 SCP 显示策略如何仅允许授权委托人修改附加到资源的标签。这是将基于属性的访问控制（ABAC）作为AWS云安全策略的一个重要部分。该策略允许调用者仅修改授权标签（在此示例中为 `access-project`）与附加到发出请求的用户或角色的相同授权标签完全匹配的资源上的标签。该策略还可以阻止授权用户更改用于授权的标签的值。调用委托人必须具有授权标签才能进行任何更改。

此策略仅阻止未经授权的用户更改标签。未被此策略阻止的授权用户必须仍具有单独的 IAM 策略，该策略明确授予相关标记 API 的 `Allow` 权限。例如，如果您的用户具有使用 `Allow */*` 的管理员策略（允许所有服务和所有操作），则组合将导致允许管理员用户仅能更改那些授权标签值与附加到用户委托人的授权标签值匹配的标签。这是因为该策略中的显式 `Deny` 将覆盖管理员策略中的显式 `Allow`。

> **Important**
>
> 这不是一个完整的策略解决方案，不应按如下所示使用。此示例仅用于演示 ABAC 策略的一部分，需要针对生产环境进行定制和测试。
> 有关完整策略及其工作原理的详细分析，请参阅使用 AWS Organizations 中的服务控制策略保护用于授权的资源标签
> 请务必使用您在环境中使用的服务测试基于拒绝的策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
```

```
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "access-project"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
```

```
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

Amazon Virtual Private Cloud（Amazon VPC）的示例 SCP

此类别中的示例

- 阻止用户删除 Amazon VPC 流日志
- 阻止还没有 Internet 访问权的任何 VPC 获取它

阻止用户删除 Amazon VPC 流日志

此 SCP 阻止任何受影响账户中的用户或角色删除 Amazon Elastic Compute Cloud（Amazon EC2）流日志或者 CloudWatch 日志组或日志流。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
```

```
      "Resource": "*"
    }
  ]
 }
```

阻止还没有 Internet 访问权的任何 VPC 获取它

此 SCP 阻止任何受影响账户中的用户或角色更改 Amazon EC2 Virtual Private Cloud（VPC）的配置以允许他们直接访问 Internet。它不会阻止现有直接访问或通过您的本地网络环境路由的任何访问。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
    }
  ]
}
```

管理组织单元

您可以使用组织单元 (OU)，将账户分组到一起，作为一个单元管理。这将极大简化您的账户管理。例如，您可以将基于策略的控制附加到 OU，该 OU 中的所有账户将自动继承策略。您可以在单个组织内创建多个 OU，也可以在其他 OU 中创建 OU。每个 OU 可以包含多个账户，您可以将账户从一个 OU 移动到另一个。但是，OU 名称必须在父 OU 或根内是唯一的。

> **Note**
>
> 组织中有一个根，它 AWS Organizations 会在你第一次建立组织时为你创建。

主题

您还可以查看组织中的所有 OU。有关更多信息，请参阅查看 OU 的详细信息。

浏览根和 OU 层次结构

要在移动账户或附加策略时导航到不同的 OU 或根，可以使用默认“树”视图。

AWS Management Console

以“树”视图形式在组织中导航

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 AWS 账户 页面中 Organization（组织）的顶部，选择 Hierarchy（层次结构）切换按钮[而不是 List（列表）]。

3. 初始状态下，树结构只显示根及子 OU 和账户的第一级。要展开树结构以显示更深的层级，请选择任何父实体旁边的展开图标（ ）。要减少视觉混乱和折叠树结构的分支，请选择展开的父实体旁边的折叠图标（ ）。
4. 选择 OU 或根的名称以查看其详细信息并执行某些操作。或者，您可以选择名称旁的单选按钮，然后在 Actions (操作) 菜单中的实体上执行某些操作。

您还可以使用表格形式查看仅在您组织中的账户列表，而无需先导航到 OU 来找到它们。在此视图中，您无法看到任何 OU，也无法操纵附加到它们的策略。

AWS Management Console

要使用无层次结构的账户平面列表形式查看组织

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，在 “组织” 部分的顶部，选择 “ AWS 账户 仅查看” 开关图标将其打开。 。
3. 显示的账户列表不包含任何层次结构。

创建 OU

登录到组织的管理账户时，您可以在组织的根下创建 OU。OU 最深可嵌套至 5 层。要创建 OU，请完成以下步骤。

Important

如果使用管理此组织 AWS Control Tower，则使用 AWS Control Tower 控制台或 API 创建您的 OU。如果您在 Organizations 中创建 OU，则该组织单位未在其中注册 AWS Control Tower。有关更多信息，请参阅《AWS Control Tower 用户指南》中的引用 AWS Control Tower的外部资源。

最小权限

要在组织的根中创建 OU，您必须拥有以下权限：

- `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
- `organizations:CreateOrganizationalUnit`

AWS Management Console

创建 OU

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 导航到AWS 账户页面。

   控制台会显示根 OU 及其内容。首次访问根时，控制台在该顶级视图中显示所有 AWS 账户 。如果您以前创建了 OU 并将账户移动到其中，则控制台仅显示顶级 OU 以及任何您尚未移动到 OU 中的账户。
3. （可选）如果要在现有 OU 内部创建 OU，请通过选择子 OU 的名称（而不是复选框）或在树视图中选择 OU 旁边的  来导航到该子 OU，在您看到所需内容后，请选择其名称。
4. 在层次结构中选择了正确的父 OU 后，在 Actions (操作) 菜单上的 Organizational Unit (组织部门) 下，选择 Create new (新建)
5. 在 Create organizational unit (创建组织部门) 对话框中，键入要创建的 OU 的名称。
6. （可选）添加一个或多个标签，方法是选择 Add tag (添加标签)，然后输入一个键和可选的值。将值留空，设置为空字符串；它并非 `null`。您最多可以向 OU 附加 50 个标签。
7. 最后，选择 Create organizational unit (创建组织部门)。

您的新 OU 显示在父级内部。现在，您可以将账户移动到此 OU 或者为其附加策略。

AWS CLI & AWS SDKs

创建 OU

您可以使用以下命令之一创建 OU：

- AWS CLI: create-organizational-unit

  要创建 OU，您必须首先找到要作为新 OU 父级的根或 OU 的身份。

要查找根目录的身份，请使用 list-roots 命令。要查找 OU 的身份，请使用 list-children 以导航到所需的 OU。

以下示例说明如何查找根目录的身份，然后在根目录下查找 OU 的身份。最后一个命令显示如何在找到的 OU 中创建新 OU。

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children \
    --parent-id r-a1b2 \
    --child-type ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
$ aws organizations create-organizational-unit \
    --parent-id ou-a1b2-f6g7h111 \
    --name New-Child-OU
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "New-Child-OU"
    }
}
```

- AWS 软件开发工具包：CreateOrganizationalUnit

重命名 OU

登录到组织的管理账户时，您可以重命名 OU。为此，请完成以下步骤。

> **最小权限**
>
> 要重命名 AWS 组织中根目录内的 OU，您必须具有以下权限：
>
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
> - `organizations:UpdateOrganizationalUnit`

AWS Management Console

重命名 OU

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 AWS 账户 页面，导航到要重命名的 OU，然后执行下面的一种步骤：
   - 选择要重命名的 OU 旁边的单选按钮

     然后，在 Actions (操作) 菜单中的 Organizational unit (组织部门) 下，选择 Rename (重命名)。
   - 选择 OU 的名称，以访问 OU 的详细信息页面。然后再页面的顶部选择 Rename (重命名)。
3. 在 Rename organizational unit (重命名组织部门) 对话框中，输入新名称，然后选择 Save changes (保存更改)。

AWS CLI & AWS SDKs

重命名 OU

您可以使用以下命令之一重命名 OU：

- AWS CLI: update-organizational-unit

  以下示例演示了如何重命名 OU。

```
$ aws organizations update-organizational-unit \
```

```
    --organizational-unit-id ou-a1b2-f6g7h222 \
    --name "Renamed-OU"
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "Renamed-OU"
    }
}
```

- AWS 软件开发工具包：UpdateOrganizationalUnit

编辑附加到 OU 的标签

登录到组织的管理账户后，您可以添加或删除附加到 OU 的标签。为此，请完成以下步骤。

> **最小权限**
>
> 要编辑附加到 AWS 组织中根目录内某个 OU 的标签，您必须具有以下权限：
>
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
> - `organizations:DescribeOrganizationalUnit` – 仅当使用 Organizations 控制台时才需要
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

编辑附加到 OU 的标签

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 AWS 账户 页面上，导航到要编辑其标签的 OU 并选择其名称。
3. 在 OU 的详细信息页面上，选择 Tags (标签) 选项卡，然后选择 Manage tags (管理标签)。
4. 您可以在此选项卡上执行以下操作：

- 编辑任何标签的值，方法是在旧标签上输入新值。您不能修改标签键。要更改键，您必须删除带有旧键的标签，然后添加使用新键的标签。
- 删除现有标签，方法是选择要重命名的标签旁边的 Remove (删除)。
- 添加新的标签键和值对。选择 Add tag (添加标签)，然后在提供的框中输入新的键名称和可选值。如果您将 Value (值) 框留空，则值是空字符串；它并非 null。

5. 在完成所有要进行的添加、删除和编辑操作之后，选择 Save changes (保存更改)。

AWS CLI & AWS SDKs

编辑附加到 OU 的标签

您可以使用以下命令之一更改附加到 OU 的标签：

- AWS CLI：tag-resource 和 untag-resource

  以下示例将标签 "Department"="12345" 附加到 OU。注意，Key 和 Value 区分大小写。

```
$ aws organizations tag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tags Key=Department,Value=12345
```

  如果成功，此命令不会产生任何输出。

  以下示例从 OU 中删除 Department 标签。

```
$ aws organizations untag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tag-keys Department
```

  如果成功，此命令不会产生任何输出。

- AWS 软件开发工具包：TagResource和 UntagResource

将账户移动到 OU 或者在根和 OU 之间移动

登录到组织的管理账户时，您可以将组织中的账户从根移动到某个 OU，从一个 OU 移动到另一个，或者从 OU 中移动回根。将账户放入 OU 中可使其遵循附加到该父 OU 及其父链中一直到根的所有 OU

的策略。如果账户未在 OU 中，则该账户仅遵循直接附加到根的策略以及任何直接附加到账户上的策略。要移动账户，请完成以下步骤。

> **最小权限**
>
> 要将账户在 OU 层次结构中移动到新位置，您必须拥有以下权限：
>
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
> - `organizations:MoveAccount`

AWS Management Console

将账户移动到 OU

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，找到要移动的一个或多个账户。您可以导航 OU 层次结构，或启用 View AWS 账户 only (仅限查看亚马逊云科技账户) 来查看没有 OU 结构的账户的平面列表。如果您有很多账户，您可能需要在列表底部选择 Load more accounts in 'ou-name' (加载使用“OU 名称”的更多账户) 以查找要移动的所有账户。
3. 选中要移动的每个账户名称旁的复选框
   ☑ 。
4. 在 Actions (操作) 菜单中的 AWS 账户(亚马逊云科技账户) 下，选择 Move (移动)。
5. 在 Move AWS 账户(移动亚马逊云科技账户) 对话框中，选择并导航到要将账户移动到的 OU 或根，然后选择 Move AWS 账户(移动亚马逊云科技账户)。

AWS CLI & AWS SDKs

将账户移动到 OU

您可以使用以下命令之一移动账户：

- AWS CLI：move-account

  以下示例将 AWS 账户 从根目录移动到 OU。请注意，您必须指定源容器和目标容器的 ID。

```
$ aws organizations move-account \
```

```
    --account-id 111122223333 \
    --source-parent-id r-a1b2 \
    --destination-parent-id ou-a1b2-f6g7h111
```

如果成功，此命令不会产生任何输出。

- AWS 软件开发工具包：MoveAccount

删除 OU

登录到组织的管理账户时，您可以删除不再需要的任何 OU。

您必须先将所有账户移出 OU 和任意子 OU，然后再删除子 OU。

> **最小权限**
>
> 要删除 OU，您必须拥有以下权限：
>
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
> - `organizations:DeleteOrganizationalUnit`

AWS Management Console

删除 OU

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在AWS 账户页面上，找到要删除的 OU，然后选中每个 OU 名称旁边的复选框 ☑ 。
3. 选择 Actions (操作)，然后在 Organizational unit (组织部门) 中，选择 Delete (删除)。
4. 要确认您要删除 OU，请输入 OU 的名称（如果您只选择删除一个）或单词“delete（删除）”（如果您选择删除多个），然后选择 Delete (删除)。

   AWS Organizations 删除 OU 并将其从列表中删除。

AWS CLI & AWS SDKs

删除 OU

您可以使用以下命令之一删除 OU：

- AWS CLI: delete-organizational-unit

  以下示例说明如何删除 OU。

  ```
  $ aws organizations delete-organizational-unit \
      --organizational-unit-id ou-a1b2-f6g7h222
  ```

  如果成功，此命令不会产生任何输出。
- AWS 软件开发工具包：DeleteOrganizationalUnit

为 AWS Organizations 资源添加标签

标签 是自定义的属性标签，您将其添加到 AWS 资源以便更轻松地确定、组织和搜索资源。每个标签具有两个部分：

- 标签键（例如，`CostCenter`、`Environment` 或 `Project`）。标签键最大长度可为 128 个字符，且不区分大小写。
- 标签值（例如，`111122223333` 或 `Production`）。标签值的最大长度可为 256 个字符，与标签键一样区分大小写。可以将标签的值设为空的字符串，但是不能将其设为空值。省略标签值与使用空字符串效果相同。

有关标签键或值中允许使用哪些字符的详细信息，请参阅《Resource Groups 标记 API 参考》中的标签 API 的标签参数。

您可使用标签，按用途、所有者、环境或其他标准对资源进行分类。有关更多信息，请参阅为AWS资源添加标签的最佳实践。

> **Tip**
>
> 使用标签策略帮助在组织账户中跨资源标准化标签实现工作。

当前，在以管理账户登录时，AWS Organizations 支持以下标记操作：

- 您可以向以下组织资源添加标签：
  - AWS 账户
  - 组织部门
  - 组织的根
  - 策略

您可以在以下时间添加标签：

- 在创建资源时 – 在 Organizations 控制台中指定标签，或将 `Tags` 参数和一个 `Create` API 操作一同使用来指定标签。这不适用于组织的根。
- 在创建资源后 – 使用 Organizations 控制台，或调用 `TagResource` 操作。

您可以使用控制台或调用 ListTagsForResource 操作，来查看 AWS Organizations 中任何可标记资源上的标签。

您可以使用控制台指定要删除的键，或者调用 UntagResource 操作，来从资源中删除标签。

使用标签

标签可让您根据对您有用的任何类别对组织内的资源进行分组，从而帮助您整理资源。例如，您可以分配一个跟踪所述部门的“Department”（部门）标签。您可以分配一个“Environment”（环境）标签来跟踪给定资源是否属于 Alpha、Beta、Gamma 或生产环境。

您还可以使用标签执行以下操作：

- 对您的资源强制执行标签标准。
- 控制谁能访问您的资源。

添加、更新和删除标签

当您登录到组织的管理账户时，您可以将标签添加到组织的资源中。

在创建资源时添加标签

> **最小权限**
>
> 要在创建资源时向资源添加标签，您需要以下权限：
>
> - 创建指定类型资源的权限
> - `organizations:TagResource`
> - `organizations:ListTagsForResource` – 仅当使用 Organizations 控制台时才需要

在创建以下资源时，可以添加附加到它们的标签键和值。

- AWS 账户
  - 创建账户
  - 邀请账户
- 组织部门 (OU)

- Policy
  - AI 服务选择退出策略
  - 备份策略
  - 服务控制策略
  - 标签策略

组织根是在您最初创建组织时创建的，因此您只能将标签作为现有资源添加到组织中。

为现有资源添加或更新标签

您还可以添加新标签或更新附加到现有资源的标签值。

> **最小权限**
>
> 要向组织中的资源添加或更新标签，您需要拥有以下权限：
>
> - `organizations:TagResource`
> - `organizations:ListTagsForResource` – 仅当使用 Organizations 控制台时才需要
>
> 要从组织中的资源中删除标签，您需要拥有以下权限：
>
> - `organizations:UntagResource`

AWS Management Console

添加、更新或删除现有资源的标签

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 导航到并选择账户、根、OU 或策略，并点击其名称以打开其详细信息页面。
3. 在标签选项卡上，选择管理标签。
4. 您可以添加新标签、修改现有标签的值或删除标签。

   要添加标签，选择 Add tag (添加标签)，然后输入标签的 Key (键) 和 Value (值)（可选）。

   要删除标签，请选择移除。

标签键和值区分大小写。为希望标准化的标签使用大写字母。您还必须遵守适用的任何标签策略的要求。

5. 根据需要，多次重复执行上一步骤。
6. 选择保存更改。

AWS CLI & AWS SDKs

向现有资源添加或更新标签

您可以使用以下命令之一将标签添加到组织中的可标记资源：

- AWS CLI：tag-resource
- AWS软件开发工具包：TagResource

从组织中的资源中删除标签

您可以使用以下命令之一删除标签：

- AWS CLI：untag-resource
- AWS软件开发工具包：UntagResource

将 AWS Organizations 与其它 AWS 产品结合使用

您可以使用信任访问权限启用您指定的名为信任服务的支持的AWS服务，以在您的组织及其代表您的账户中执行任务。这涉及向可信服务授予权限，但不会以其他方式影响用户或角色的权限。当您允许访问时，信任服务可以在您组织的每个账户中创建一个名为服务相关角色 的 IAM 角色（只要需要该角色）。该角色具有允许可信服务执行该服务文档中所述任务的权限策略。这允许您指定您希望可信服务在代表您的组织账户中保持的设置和配置详细信息。信任服务仅在需要对账户执行管理操作时才会创建服务相关角色，而不一定在组织的所有账户中执行管理操作。

Important

我们强烈建议在相关选项可用时，仅通过可信服务的控制台或其等效 AWS CLI 或 API 操作，来启用和禁用可信访问。这使得信任服务在启用信任访问权限时执行任何必需的初始化，例如在禁用信任访问权限时创建任何必需的资源和任何必需的资源清理。
有关如何使用信任服务启用或禁用对组织的信任服务访问的信息，请参阅AWS 可以与之配合使用的服务 AWS Organizations中了解详情链接下的支持信任访问权限列。
如果您使用 Organizations 控制台、CLI 命令或 API 操作禁用访问，则会导致发生以下操作：

- 服务不能再在您组织的账户中创建服务相关角色。这意味着该服务无法代表您对组织中的任何新账户执行操作。该服务仍然可以在旧账户中执行操作，直到服务完全从 AWS Organizations 中清理。
- 该服务不能再在组织中的成员账户中执行任务，除非附加到您的角色的 IAM policy 明确允许这些操作。这包括从成员账户到管理账户或委托管理员账户（如果相关）的任何数据聚合。
- 有些服务会检测到这一点并清理与集成相关的所有剩余数据或资源，而其他服务则停止访问组织，但会将所有历史数据和配置保留在合适位置，以支持重新启用集成的可能性。

相反，使用其他服务的控制台或命令禁用集成可确保其他服务可以清理仅用于集成的任何资源。服务清除组织账户中的资源的方式取决于该服务。有关更多信息，请参阅有关其他AWS服务的文档。

允许可信访问所需的权限

可信访问需要以下两种服务的权限：AWS Organizations 和可信服务。要允许可信访问，请选择以下场景之一：

- 如果您有在 AWS Organizations 和信任服务中都具有权限的凭证，则通过使用信任服务提供的工具（控制台或 AWS CLI）允许访问。这允许服务代表您在 AWS Organizations 中允许新人访问权限以及创建此服务在您的组织中运行所需的任何资源。

  这些凭证的最低权限如下：

  - `organizations:EnableAWSServiceAccess`。您还可以将 `organizations:ServicePrincipal` 条件键与此操作搭配使用，以将这些操作发出的请求限制为已批准的服务委托人名称列表。有关更多信息，请参阅条件键。
  - `organizations:ListAWSServiceAccessForOrganization` – 在您使用 AWS Organizations 控制台时为必需。
  - 可信服务所需的最低权限取决于此服务。有关更多信息，请参阅可信服务的文档。
- 如果一人拥有在 AWS Organizations 中具有权限的凭证，但其他人拥有在可信服务中具有权限的凭证，请按以下顺序执行这些步骤：

  1. 拥有在 AWS Organizations 中具有权限的凭证的人应使用 AWS Organizations 控制台、AWS CLI 或 AWS 开发工具包允许可信服务的可信访问。这为另一服务授予在执行以下步骤 (步骤 2) 后在组织中执行其所需配置的权限。

     最低 AWS Organizations 权限如下：

     - `organizations:EnableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – 仅在您使用 AWS Organizations 控制台时为必需

     有关在 AWS Organizations 中允许可信访问的步骤，请参阅如何允许或禁止可信访问。
  2. 拥有在可信服务中具有权限的凭证的人可启用此服务以使用 AWS Organizations。这指示此服务执行任何所需初始化 (如，创建可信服务在组织中运行所需的任何资源)。有关信息，请参阅AWS 可以与之配合使用的服务 AWS Organizations处的服务特定说明。

禁止可信访问所需的权限

当您不再需要允许可信服务在您的组织或其账户上运行时，请选择以下场景之一。

> **Important**
>
> 禁止可信服务访问不 会阻止具有相应权限的用户和角色使用该服务。要完全阻止用户和角色访问 AWS 服务，您可以删除授予此访问权限的 IAM 权限，也可以使用 AWS Organizations 中的服务控制策略 (SCP)。

您可以将 SCP 应用于仅成员账户。SCP 不能应用于管理账户。建议您不要在管理账户中运行服务。相反，请在成员账户中运行它们，您可以通过使用 SCP 控制安全性。

- 如果您有在 AWS Organizations 和可信服务中都具有权限的凭证，则可通过使用为可信服务提供的工具（控制台或 AWS CLI）禁止访问。该服务之后将通过删除不再需要的资源并代表您在 AWS Organizations 中禁止此服务的可信访问来清理。

  这些凭证的最低权限如下：

  - `organizations:DisableAWSServiceAccess`。您还可以将 `organizations:ServicePrincipal` 条件键与此操作搭配使用，以将这些操作发出的请求限制为已批准的服务委托人名称列表。有关更多信息，请参阅条件键。
  - `organizations:ListAWSServiceAccessForOrganization` – 在您使用 AWS Organizations 控制台时为必需。
  - 可信服务所需的最低权限取决于此服务。有关更多信息，请参阅可信服务的文档。
- 如果在 AWS Organizations 中具有权限的凭证不是在可信服务中具有权限的凭证，请按以下顺序执行这些步骤：

  1. 在可信服务中具有权限的人首先使用此服务禁止访问。这将指示可信服务通过删除可信服务所需的资源进行清理。有关信息，请参阅AWS 可以与之配合使用的服务 AWS Organizations处的服务特定说明。
  2. 在 AWS Organizations 中具有权限的人之后可使用 AWS Organizations 控制台、AWS CLI 或 AWS 开发工具包禁止可信服务的访问。这将从组织及其账户中删除可信服务的权限。

     最低 AWS Organizations 权限如下：

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – 仅在您使用 AWS Organizations 控制台时为必需

     有关在 AWS Organizations 中禁止可信访问的步骤，请参阅如何允许或禁止可信访问。

如何允许或禁止可信访问

如果您只有 AWS Organizations 的权限并且要代表另一 AWS 服务的管理员允许或禁止对您组织的可信访问，请使用以下过程。

Important

我们强烈建议在相关选项可用时，仅通过可信服务的控制台或其等效 AWS CLI 或 API 操作，来启用和禁用可信访问。这使得信任服务在启用信任访问权限时执行任何必需的初始化，例如在禁用信任访问权限时创建任何必需的资源和任何必需的资源清理。
有关如何使用信任服务启用或禁用对组织的信任服务访问的信息，请参阅AWS 可以与之配合使用的服务 AWS Organizations中了解详情链接下的支持信任访问权限列。
如果您使用 Organizations 控制台、CLI 命令或 API 操作禁用访问，则会导致发生以下操作：

- 服务不能再在您组织的账户中创建服务相关角色。这意味着该服务无法代表您对组织中的任何新账户执行操作。该服务仍然可以在旧账户中执行操作，直到服务完全从 AWS Organizations 中清理。
- 该服务不能再在组织中的成员账户中执行任务，除非附加到您的角色的 IAM policy 明确允许这些操作。这包括从成员账户到管理账户或委托管理员账户（如果相关）的任何数据聚合。
- 有些服务会检测到这一点并清理与集成相关的所有剩余数据或资源，而其他服务则停止访问组织，但会将所有历史数据和配置保留在合适位置，以支持重新启用集成的可能性。

相反，使用其他服务的控制台或命令禁用集成可确保其他服务可以清理仅用于集成的任何资源。服务清除组织账户中的资源的方式取决于该服务。有关更多信息，请参阅有关其他AWS服务的文档。

AWS Management Console

启用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到要启用的服务所在的行，然后选择其名称。
3. 选择 Enable trusted access (启用可信访问)。
4. 在确认对话框中，选中 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
5. 如果您要允许 访问，请告知另一 AWS 服务的管理员，他们现在可以启用另一服务以使用 AWS Organizations。

禁用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到要禁用的服务所在的行，然后选择其名称。
3. 请一直等到其他服务的管理员告知您已禁用此服务且已清理资源。
4. 在确认对话框中输入 **`disable`**，然后选择 Disable trusted access (禁用信任访问权限)。

AWS CLI, AWS API

允许或禁止信任服务访问

您可以使用以下 AWS CLI 命令或 API 操作允许或禁止可信服务访问：

- AWS CLI：AWS organizations enable-aws-service-access
- AWS CLI：AWS organizations disable-aws-service-access
- AWS API：EnableAWSServiceAccess
- AWS API：DisableAWSServiceAccess

AWS Organizations 和服务相关角色

AWS Organizations 使用 IAM 服务相关角色允许信任服务代表您执行在组织的成员账户中执行任务。当您配置可信服务并授权其与您的组织集成时，该服务可请求 AWS Organizations 在其成员账户中创建服务相关角色。可信服务按需异步执行此操作，同时并非所有组织账户都需要。此服务相关角色具有预定义的 IAM 权限，此权限允许信任服务在账户内仅执行特定任务。一般而言，AWS 将管理所有服务相关角色，这意味着，您通常无法更改角色或附加的策略。

为实现上述操作，当您在组织中创建账户或接受邀请以将现有账户加入组织时，AWS Organizations 将使用名为 `AWSServiceRoleForOrganizations` 的服务相关角色预置成员账户。仅 AWS Organizations 服务自身可以代入此角色。此角色具有允许 AWS Organizations 为其他AWS服务创建服务相关角色的权限。此服务相关角色存在于所有组织中。

如果您的组织仅启用了整合账单功能（但我们建议不要这样做），则绝不使用名为 `AWSServiceRoleForOrganizations` 的服务相关角色并且可删除它。如果您之后要在组织中启用所有功能，则此角色是必需的并且您必须还原它。在您开始启用所有功能的流程时，将进行以下检查：

- 对于已受邀加入组织的每个成员账户 – 账户管理员将收到同意启用所有功能的请求。要成功同意此请求，如果服务相关角色 (organizations:AcceptHandshake) 不存在，此管理员必须同时具有 和iam:CreateServiceLinkedRole AWSServiceRoleForOrganizations 权限。如果 AWSServiceRoleForOrganizations 角色已存在，则管理员只需 organizations:AcceptHandshake 权限即可同意该请求。如果此管理员同意此请求，则 AWS Organizations 将创建服务相关角色（如果此角色尚不存在）。
- 对于已在组织中创建的每个成员账户 – 账户管理员将收到重新创建服务相关角色的请求。（成员账户的管理员不会收到启用所有功能的请求，因为管理账户（此前称为“主账户”）的管理员被视为所创建成员账户的所有者。）如果成员账户管理员同意该请求，则 AWS Organizations 将创建服务相关角色。管理员必须同时具有 organizations:AcceptHandshake 和 iam:CreateServiceLinkedRole 权限才能成功接受握手。

在组织中启用所有功能后，您无法再删除任何账户中的 AWSServiceRoleForOrganizations 服务相关角色。

> **Important**
>
> AWS Organizations SCP 决不会影响服务相关角色。这些角色将免受任何 SCP 限制。

AWS 可以与之配合使用的服务 AWS Organizations

借助 AWS Organizations 此功能，您可以 AWS 账户 将多个账户整合到一个组织中，从而大规模执行账户管理活动。合并账户可简化您使用其他 AWS 服务的方式。您可以利用选定服务中 AWS Organizations 提供的多账户管理 AWS 服务，对属于您组织的所有成员账户执行任务。

下表列出了您可以使用的 AWS 服务 AWS Organizations，以及在组织范围内使用每项服务的好处。

可信访问-您可以启用兼容的 AWS 服务，以便在组织 AWS 账户 中的所有部门执行操作。有关更多信息，请参阅 将 AWS Organizations 与其它 AWS 产品结合使用。

AWS 服务的委托管理员-兼容的 AWS 服务可以将组织中的 AWS 成员账户注册为该服务中组织账户的管理员。有关更多信息，请参阅 与 Organizations 配合使用的 AWS 服务的委托管理员。

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Account Management 管理组织所有内容 AWS 账户的详细信息和元数据。	您可以为组织内的所有账户创建、更新和删除备用联系人信息。	 是 了解更多	 是 了解更多	
AWS Application Migration Service AWS Application Migration Service 允许公司 lift-and-shift 访问 AWS 大量物理、虚拟或云服务器，而不会出现兼容性问题、性能中断或转换窗口过长。	您可以管理跨多个账户的大规模迁移任务。	 是 了解更多	 是 了解更多	
AWS Artifact 下载 AWS 安全合规报告，例如 ISO 和 PCI 报告。	您可以代表您组织内的所有账户接受协议。	 是 了解更多	 否	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Audit Manager 自动化持续收集证据，以帮助您审核云服务的使用情况。	持续审计您组织中多个账户的 AWS 使用情况，以简化评估风险和合规性的方式。	 是 了解更多	 是 了解更多	
AWS Backup 管理和监控您组织中的所有账户的备份。	您可以为整个组织或组织部门 (OU) 中的账户组配置和管理备份计划。您可以集中监控所有账户的备份。	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Billing and Cost Management 概述您的 AWS 云财务管理数据，帮助您更快、更明智地做出决策。	允许拆分成本分配数据检索 AWS Organizations 信息（如果适用），并收集您选择使用的分割成本分配数据服务的遥测数据。 有关更多信息，请参阅什么是 AWS Billing and Cost Management？ 在《账单和成本管理》用户指南中。	 是 了解更多	 否	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS CloudFormation Stacksets 通过单个操作跨多个账户和区域创建、更新或删除堆栈。	管理账户或委托管理员账户中的用户可以创建具有服务托管权限的堆栈套，该堆栈套会将堆栈实例部署到您组织中的账户。	 是 了解更多	 是 了解更多	
AWS CloudTrail 允许对您的账户进行监管、合规性检查、操作审核和风险审计。	管理账户或委托管理员账户中的用户可以创建组织跟踪或事件数据存储，记录组织中所有账户的所有事件。	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Compute Optimizer 获取 AWS 计算优化建议。	您可以分析组织账户中的所有资源以获取优化建议。 有关更多信息，请参阅《AWS Compute Optimizer 用户指南》中的 Compute Optimizer 支持的账户。	 是 了解更多	 了解更多	是

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Config 评估、审计和评价您的 AWS 资源的配置。	您可以在组织范围内查看合规性状态。您还可以使用 AWS Config API 操作来管理组织 AWS 账户 中所有部门的 AWS Config 规则和一致性包。 您可以使用委托管理员账户聚合 AWS Organizations中组织所有成员账户中的资源配置和合规性数据。有关更多信息，请	 是 了解更多	 是 了解更多： Config 规则 一致性包 多账户多区域数据聚合	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
	参阅 AWS Config 开发人员指南中的注册委托管理员。			

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Control Tower 设置和管理安全、合规的多账户 AWS 环境。	您可以为所有 AWS 资源设置 landing zone，即多账户环境。该环境包括一个组织和组织实体。您可以使用此环境对所有人强制执行合规性法规 AWS 账户。 有关更多信息，请参阅《AWS Control Tower 用户指南》中的 操作方法 AWS Control Tower和通过 AWS	 是 了解更多	 否	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
	Organizations管理账户。			
AWS 成本优化中心 收集各 AWS 优化产品的成本建议。	您可以轻松识别、筛选和汇总跨 AWS Organizations 成员账户和 AWS 地区 AWS 的成本优化建议。 有关更多信息，请参阅成本优化中心用户指南中的成本优化中心。	 是 了解更多a	 否	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
Amazon Detective 可从日志数据生成可视化，以分析、调查和快速识别安全结果或可疑活动的根本原因。	您可以将 Amazon D AWS Organizations etective 与集成，确保您的侦探行为图能够让您了解所有组织账户的活动。	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
Amazon DevOps Guru 可以分析操作数据以及应用程序指标和事件，以识别偏离正常操作模式的行为。当 DevOps Guru 检测到操作问题或风险时，用户会收到通知。	您可以与集成 AWS Organizations ，以管理整个组织中所有账户的见解。您可以委托一位管理员来查看、排序和筛选来自所有账户的见解，以获取所有受监控的应用程序在组织范围内的运行状况。	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Directory Service 在 AWS 云端设置和运行目录，或者将你的 AWS 资源与现有的本地 Microsoft Active Directory 连接起来。	您可以 AWS Directory Service 与集成，AWS Organizations 以便在一个区域内的多个账户和任何 VPC 之间实现无缝目录共享。	 是 了解更多	 否	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
Amazon EventBridge 实时监控您的 AWS 资源和运行 AWS 的应用程序。	您可以允许在组织中的所有账户之间共享所有亚马逊 CloudWatch 活动（以前称为 Amazon 活动）。EventBridge 有关更多信息，请参阅亚马逊 EventBridge 用户指南 AWS 账户中的在两者之间发送和接收亚马逊 EventBridge 事件。	 否	 否	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Firewall Manager 跨账户和应用程序集中配置和管理 Web 应用程序防火墙规则。	您可以集中配置和管理组织中各个账户的 AWS WAF 规则。	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
Amazon GuardDuty GuardDuty 是一项持续的安全监控服务，用于分析和处理来自各种数据源的信息。它使用威胁情报源和机器学习来标识您 AWS 环境中意外的和未经授权的恶意活动。	您可以指定一个成员账户来查看和管理 GuardDuty 组织中的所有账户。添加成员帐户会自动启用 GuardDuty 所选帐户中的这些帐户 AWS 区域。您还可以自动 GuardDuty 激活添加到组织中的新帐户。 有关更多信息，请参阅亚马逊 GuardDuty 用户	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
	指南中的GuardDut和 Organizations。			
AWS Health 深入了解可能影响资源性能的事件或 AWS 服务可用性问题。	您可以汇总组织中各个账户 AWS Health 的事件。	 是 了解更多	 了解更多	是

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Identity and Access Management 安全地控制对 AWS 资源的访问。	您可以使用 IAM 中服务上次访问的数据，以帮助您更好地了解组织中的 AWS 活动。您可以使用此数据来创建和更新服务控制策略 (SCP)，将访问限制在仅您的组织账户所使用的 AWS 服务。 有关示例，请参阅《IAM 用户指南》中的使用数据来细化	 否	 否	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
	组织部门的权限。			
IAM Access Analyzer 分析您 AWS 环境中基于资源的策略，以确定向信任区域之外的委托人授予访问权限的任何策略。	您可以指定成员账户作为 IAM 访问分析器的管理员。 有关更多信息，请参阅《IAM 用户指南》中的启用访问分析器。	 是 了解更多	 了解更多	是

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
Amazon Inspector 自动扫描您的 AWS 工作负载是否存在漏洞，以发现驻留在 Amazon ECR 中的 Amazon EC2 实例和容器映像，以发现软件漏洞和意外网络泄露。	可以委托一位管理员来启用或禁用对成员账户的扫描、查看从整个组织汇总的结果数据、创建和管理禁止规则。 有关更多信息，请参阅《Amazon Inspector 用户指南》中的使用 AWS Organizations管理多个账户。	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS License Manager 简化将软件许可证迁移到云中的过程。	您可以在整个组织中启用计算资源的跨账户发现。	 是 了解更多	 了解更多	是

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
Amazon Macie 使用机器学习发现您的业务关键型内容并对其进行分类，以帮助您满足数据安全和隐私要求。它会持续评估您存储在 Amazon S3 中的内容，并通知您潜在的问题。	您可以为您组织中的所有账户配置 Amazon Macie，以便从指定的 Macie 管理员账户跨所有账户获取 Amazon S3 中所有数据的统一视图。您可以将 Macie 配置为随着组织壮大而自动保护新账户中的资源。系统会提醒您修正整个组织中的 S3 存储桶中的策	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
	略错误配置。			
AWS Marketplace 一个精挑细选的数字化产品目录，您通过它可以轻松地查找、购买、部署和管理构建解决方案及运营业务所需的第三方软件、数据和服务。	您可以在组织中的各个账户之间共享 AWS Marketplace 订阅和购买的许可证。	 是 了解更多	 否	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Marketplace 私人市场 为您提供广泛的可用产品目录 AWS Marketplace，以及对这些产品的精细控制。	使您能够创建多个私有市场体验，这些体验与您的整个组织、一个或多个 OU 或组织中的一个或多个账户相关联，每个账户都有自己的一套经批准的产品。您的 AWS 管理员还可以通过公司或团队的徽标、消息和配色方案将公司品牌应用于每一次私人市场体验。	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS 网络管理器 使您能够跨 AWS 账户、区域和本地位置集中管理您的 AWS Cloud WAN 核心网络和 T AWS ransit Gateway 网络。	您可以使用组织内的多个 AWS 账户中的传输网关及其关联资源，集中管理和监控您的全球网络。	 是 了解更多	 是 了解更多	
Amazon Q 开发者版 Amazon Q Developer 是一款生成式人工智能 (AI) 驱动的对话助手，可以帮助您理解、构建、扩展和操作 AWS 应用程序。	Amazon Q 开发者的付费订阅版本需要整合 Organizations。	 是 了解更多	 否	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Resource Access Manager 与其他账户共享您拥有的指定 AWS 资源。	您可以在组织内共享资源，而无需交换其他邀请。您可以共享的资源包括 Route 53 Resolver 规则、按需容量预留等。 有关共享容量预留的信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南或适用于 Windows 实例的 Amazon EC2 用户指南。	 是 了解更多	 否	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
	有关可共享资源的列表，请参阅《AWS RAM 用户指南》中的可共享资源。			
AWS 资源探索器 使用类似互联网搜索引擎的体验来探索您的资源。	启用多账户搜索。	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Security Hub 查看您的安全状态， AWS 并根据安全行业标准和最佳实践检查您的环境。	您可以为组织的所有账户（包括添加新账户）自动启用 Security Hub。这扩大了 Security Hub 检查和调查结果的覆盖范围，从而可让您更准确地了解您的整体安全状况。	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
Amazon S3 Storage Lens 存储统计管理工具 通过切实可行的建议，您可以了解 Amazon S3 Storage 使用情况和活动指标。	配置 Amazon S3 Storage Lens，以便了解 Amazon S3 存储使用情况和活动趋势，以及组织中所有成员账户的建议。	 是 了解更多	 了解更多	是
Amazon Security Lake Amazon Security Lake 可将来自云端、本地和自定义源的安全数据，集中到您账户中存储的数据湖中。	创建一个数据湖来收集账户中的日志和事件。	 是 了解更多	 了解更多	是

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Service Catalog 创建和管理获准在 AWS上使用的 IT 服务的目录。	您可以更轻松地跨账户共享产品组合和复制产品，而无需共享产品组合 ID。	 是 了解更多	 了解更多	是
服务限额 从中央位置查看和管理您的服务配额（也称为限制）。	您可以创建一个配额请求模板，以在创建组织账户时自动请求提升配额。	 是 了解更多		否
AWS IAM Identity Center 为您的所有账户和云应用程序提供单一登录访问。	用户可以使用其公司凭据登录 AWS 访问门户，并访问其分配的管理账户或成员账户中的资源。	 是 了解更多	 了解更多	是

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Systems Manager 实现对 AWS 资源的可见性和控制力。	您可以使用 Systems Manager Explorer 同步组织 AWS 账户中所有人的操作数据。 通过使用 Systems Manager Change Manager，您可以从委托管理员账户管理组织中所有成员账户的更改模板、批准和报告。	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
标签策略 在组织账户中跨资源使用标准化标签。	您可以创建标签策略来定义特定资源和资源类型的标记规则，然后将这些策略附加到组织实体和账户，以强制执行这些规则。	 是 了解更多	 否	
AWS Trusted Advisor Trusted Advisor 检查您的 AWS 环境，并在有机会节省资金、提高系统可用性和性能或帮助填补安全漏洞时提出建议。	对组织 AWS 账户 中的所有人进行 Trusted Advisor 检查。	 是 了解更多	 是 了解更多	

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
AWS Well-Architected Tool AWS Well-Architected Tool 可帮助您记录工作负载的状态，并将其与最新的 AWS 架构最佳实践进行比较。	使 Org AWS WA Tool anizations 和 Organizations 的客户都能简化与其组织中其他成员共享 AWS WA Tool 资源的流程。	 是 了解更多		否
Amazon VPC IP 地址管理器（IPAM） IPAM 是一项 VPC 功能，可让您更轻松地规划、跟踪和监控工作负载的 IP 地址。AWS	监控整个组织的 IP 地址使用情况，并在成员账户之间共享 IP 地址池。	 是 了解更多	 了解更多	是

AWS 服务	与一起使用的好处 AWS Organizations	支持可信访问	支持委托管理员	
Amazon VPC Reachability Analyzer Reachability Analyzer 是一种配置分析工具，使您能够在虚拟私有云（VPC）中的源资源和目标资源之间执行连接测试。	跟踪组织中各个账户的路径。	 是 了解更多	 是 了解更多	

AWS Account Management 和 AWS Organizations

AWS Account Management 可帮助您管理组织中所有 AWS 账户的账户信息和元数据。您可以为组织的每个成员账户设置、修改或删除备用联系人信息。有关更多信息，请参阅《AWS Account Management 用户指南》中的在您的组织中使用 AWS Account Management。

以下信息可帮助您将 AWS Account Management 与 AWS Organizations 集成。

启用账户管理可信访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

账户管理功能需要具有 AWS Organizations 的可信访问权限，然后您才能为您的组织将某个成员账户指定为此服务的委托管理员。

您只能使用 Organizations 工具启用信任访问权限。

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS Account Management 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Account Management 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS Account Management 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：EnableAWSServiceAccess

禁用账户管理可信访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 AWS Organizations 管理账户中的管理员可以禁用对 AWS Account Management 的信任访问权限。

您只能使用 Organizations 工具禁用信任访问权限。

您可以使用AWS Organizations控制台，通过运行 Organizations AWS CLI 命令，或者通过调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 AWS Account Management 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **disable**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Account Management 的管理员，他们现在可以使用其控制台或工具禁用该服务，使其无法处理 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS Account Management 作为 Organizations 的信任服务。

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

  如果成功，此命令不会产生任何输出。
- AWS API：DisableAWSServiceAccess

为账户管理功能启用委托管理员账户

当您将某个成员账户指定为组织的委托管理员时，来自指定账户的用户和角色将可以管理组织内其他成员账户的 AWS 账户元数据。如果您没有启用委托管理员账户，则这些任务只能由组织的管理账户执行。这有利于您将组织的管理与您的账户详细信息的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色能够将某个成员账户配置为组织的账户管理委托管理员。

有关如何配置委托策略的一般说明，请参阅 创建或更新基于资源的委托策略。

AWS CLI, AWS API

如果要使用 AWS CLI 或某个 AWS SDK 配置委托管理员账户，您可以使用以下命令：

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

- AWS SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务主体 `account.amazonaws.com` 确定为参数。

AWS Application Migration Service （应用程序迁移服务）和 AWS Organizations

AWS Application Migration Service 简化、加快将应用程序迁移到并降低其成本。 AWS通过 Organizations 集成，您可以使用全局视图功能来管理跨多个账户的大规模迁移。有关更多信息，请参阅应用程序迁移服务用户指南 AWS Organizations中的设置。

使用以下信息来帮助您集 AWS Application Migration Service 成 AWS Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许应用程序迁移服务在组织中的组织账户中执行支持的操作。

只有在应用程序迁移服务与 Organizations 之间禁用可信访问权限或从组织中移除成员帐户后，才能删除或修改此角色。

- `AWSServiceRoleForApplicationMigrationService`

应用程序迁移服务使用的服务主体

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。应用程序迁移服务使用的服务相关角色向以下服务主体授予访问权限：

- mgn.amazonaws.com

使用应用程序迁移服务启用可信访问

通过应用程序迁移服务启用可信访问时，您可以使用全局视图功能，该功能允许您管理跨多个账户的大规模迁移。全局视图提供了可见性，并能够在不同 AWS 账户中的源服务器、应用程序和波浪上执行特定操作。有关更多信息，请参阅AWS Application Migration Service 用户指南中的设置 AWS Organizations。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 AWS Application Migration Service 控制台或控制台启用可信访问。 AWS Organizations

> **Important**
>
> 我们强烈建议您尽可能使用 AWS Application Migration Service 控制台或工具来启用与 Organizations 的集成。这允许 AWS Application Migration Service 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 AWS Application Migration Service提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 AWS Application Migration Service 控制台或工具启用可信访问，则无需完成这些步骤。

您可以使用 AWS Organizations 控制台、运行 AWS CLI 命令或在其中一个 AWS SDK 中调用 API 操作来启用可信访问。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS Application Migration Service 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。

3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您仅是的管理员 AWS Organizations，请告诉管理员他们现在可以使用其控制台启用该服务 AWS Organizations。 AWS Application Migration Service

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来启用可信服务访问：

- AWS CLI: enable-aws-service-access

  您可以运行以下命令以在 Organiz AWS Application Migration Service ations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：启用 AWSServiceAccess

使用应用程序迁移服务禁用可信访问

只有 Organizations 管理帐户中的管理员才能禁用应用程序迁移服务的可信访问权限。

您可以使用 AWS Application Migration Service 或 AWS Organizations 工具禁用可信访问。

> **Important**
>
> 我们强烈建议您尽可能使用 AWS Application Migration Service 控制台或工具来禁用与 Organizations 的集成。这允许 AWS Application Migration Service 执行它需要的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 AWS Application Migration Service 提供的工具禁用集成时，才会使用这些步骤进行处理。
> 如果您使用 AWS Application Migration Service 控制台或工具禁用可信访问，则无需完成这些步骤。

您可以使用 AWS Organizations 控制台、运行 Organizations AWS CLI 命令或在其中一个 AWS 软件开发工具包中调用 Organizations API 操作来禁用可信访问。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 AWS Application Migration Service 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **disable**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您仅是的管理员 AWS Organizations，请告知管理员他们现在可以使用该服务的控制台或工具禁用该服务 AWS Organizations。 AWS Application Migration Service

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来禁用可信服务访问权限：

- AWS CLI: disable-aws-service-access

  您可以运行以下命令在 Organization AWS Application Migration Service s 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。
- AWS API：禁用 AWSServiceAccess

为应用程序迁移服务启用委派管理员帐户

当您将成员帐户指定为组织的委托管理员时，该帐户中的用户和角色可以为应用程序迁移服务执行管理操作，否则这些操作只能由组织管理帐户中的用户或角色执行。这可以帮助您将组织管理与应用程序迁移服务的管理分开。有关更多信息，请参阅应用程序迁移服务用户指南 AWS Organizations中的设置。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色才能将成员账户配置为组织中应用程序迁移服务的委派管理员

AWS CLI, AWS API

如果要使用 AWS CLI 或其中一个 AWS SDK 配置委派管理员帐户，则可以使用以下命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal mgn.amazonaws.com
```

- AWS SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务标识`mgn.amazonaws.com`为参数。

禁用应用程序迁移服务的委派管理员

只有 Organizations 管理账户中的管理员才能移除应用程序迁移服务的委派管理员。您可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作来移除委托管理员。

AWS Artifact 和 AWS Organizations

AWS Artifact 是一项允许您下载 AWS 安全合规性报告（例如 ISO 和 PCI 报告）的服务。使用该功能 AWS Artifact，即使添加了新的报告和帐户，组织管理账户中的用户也可以自动代表组织中的所有成员账户接受协议。成员账户用户可以查看和下载协议。有关更多信息，请参阅《AWS Artifact 用户指南》中的 Arti AWS fact 中管理多个账户的协议。

使用以下信息来帮助您集 AWS Artifact 成 AWS Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色 AWS Artifact 允许在组织中的组织账户中执行支持的操作。

只有在禁用 AWS Artifact 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

尽管您可以在删除组织的成员账户时删除或修改此角色，但我们不建议这样操作。

不鼓励修改角色，因为这可能会导致跨服务混淆代理等安全问题。要了解有关防范混淆代理的更多信息，请参阅AWS Artifact 《用户指南》中的跨服务代理问题防范。

- `AWSServiceRoleForArtifact`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。使用的服务相关角色向以下服务主体 AWS Artifact 授予访问权限：

- `artifact.amazonaws.com`

使用 AWS Artifact启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Organizations 工具启用信任访问权限。

您可以使用 AWS Organizations 控制台、运行 AWS CLI 命令或在其中一个 AWS SDK 中调用 API 操作来启用可信访问。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS Artifact 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您仅是的管理员 AWS Organizations，请告诉管理员他们现在可以使用其控制台启用该服务 AWS Organizations。 AWS Artifact

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来启用可信服务访问：

- AWS CLI: enable-aws-service-access

  您可以运行以下命令以在 Organiz AWS Artifact ations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：启用 AWSServiceAccess

使用 AWS Artifact禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 AWS Organizations 管理账户中的管理员才能使用禁用可信访问权限 AWS Artifact。

您可以仅使用 Organizations 工具禁用信任访问权限。

AWS Artifact 需要使用可信访问权限 AWS Organizations 才能使用组织协议。如果您在使用组织协议 AWS Organizations 时使用禁用可信访问，则它会因为无法访问组织而停止运行。 AWS Artifact 您接受的任何组织协议都将 AWS Artifact 保留，但无法被访问 AWS Artifact。 AWS Artifact 创造的 AWS Artifact 角色仍然存在。如果您之后重新允许可信访问，则 AWS Artifact 将继续像以前一样运行，而无需您重新配置该服务。

从组织中删除的独立账户不再有权访问任何组织协议。

您可以使用 AWS Organizations 控制台、运行 Organizations AWS CLI 命令或在其中一个 AWS 软件开发工具包中调用 Organizations API 操作来禁用可信访问。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 AWS Artifact 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **`disable`**，然后选择 Disable trusted access (禁用信任访问权限)。

5. 如果您仅是的管理员 AWS Organizations，请告知管理员他们现在可以使用该服务的控制台或工具禁用该服务 AWS Organizations。 AWS Artifact

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来禁用可信服务访问权限：

- AWS CLI: disable-aws-service-access

  您可以运行以下命令在 Organization AWS Artifact s 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。
- AWS API：禁用 AWSServiceAccess

AWS Audit Manager 和 AWS Organizations

AWS Audit Manager 可帮助您持续审计您的AWS使用情况，以简化评估风险以及与相关法规和行业标准合规性的方式。Audit Manager 可自动收集证据，以便更轻松地评估您的策略、过程和活动是否有效运行。当需要进行审计时，Audit Manager 可帮助您管理利益攸关方对控件的审核，并帮助您以更少的人工工作量生成可审计的报告。

当您将 Audit Manager 与 AWS Organizations 集成后，您可以从更广泛的来源收集证据，方法是在评估范围内添加组织中的多个AWS 账户。

有关更多信息，请参阅《Audit Manager 用户指南》中的启用 AWS Organizations。

以下信息可帮助您将 AWS Audit Manager 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Audit Manager 在您组织中的组织账户内执行支持的操作。

只有在禁用 Audit Manager 和 Organizations 之间的信任访问，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

有关 Audit Manager 如何使用此角色的详细信息，请参阅《AWS Audit Manager 用户指南》中的使用服务相关角色。

- `AWSServiceRoleForAuditManager`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Audit Manager 使用的服务相关角色为以下服务委托人授予访问权限：

- `auditmanager.amazonaws.com`

使用 Audit Manager 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

在将委托成员账户作为组织的委托管理员之前，Audit Manager 需要对 AWS Organizations 的信任访问权限。

您可以使用 AWS Audit Manager 控制台或 AWS Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 AWS Audit Manager 控制台或工具来实现与 Organizations 的集成。这可让 AWS Audit Manager 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 AWS Audit Manager 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
>
> 如果您使用 AWS Audit Manager 控制台或工具启用信任访问权限，则您无需完成这些步骤。

使用 Audit Manager 控制台启用信任访问权限

有关启用信任访问权限的说明，请参阅《AWS Audit Manager 用户指南》中的设置。

> **Note**
>
> 如果您使用 AWS Audit Manager 控制台配置委托管理员，AWS Audit Manager 会自动为您启用信任访问权限。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来启用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS Audit Manager 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：EnableAWSServiceAccess

使用 Audit Manager 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 AWS Organizations 管理账户中的管理员可以禁用对 AWS Audit Manager 的信任访问权限。

您只能使用 Organizations 工具禁用信任访问权限。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS Audit Manager 作为 Organizations 的信任服务。

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

如果成功，此命令不会产生任何输出。

- AWS API：DisableAWSServiceAccess

为 Audit Manager 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 Audit Manager 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 Audit Manager 的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中具有以下权限的用户或角色才能将成员账户配置为组织中 Audit Manager 的委托管理员：
> `audit-manager:RegisterAccount`

有关为 Audit Manager 启用委托管理员账户的说明，请参阅《AWS Audit Manager 用户指南》中的设置。

如果您使用 AWS Audit Manager 控制台配置委托管理员，Audit Manager 会自动为您启用信任访问权限。

AWS CLI, AWS API

如果要使用 AWS CLI 或某个 AWS SDK 配置委托管理员账户，您可以使用以下命令：

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- AWS SDK：调用 `RegisterAccount` 操作并提供 `delegatedAdminAccount` 作为委托管理员账户的参数。

AWS Backup 和 AWS Organizations

AWS Backup 是一项可用于管理和监控您组织中的 AWS Backup 作业的服务。使用 AWS Backup 时，如果您以组织的管理账户中的用户身份登录，则可以启用组织范围的备份保护和监控。此服务通过

使用备份策略将 AWS Backup 计划集中应用于您组织中所有账户的资源，从而帮助您实现合规性。当您一起使用 AWS Backup 和 AWS Organizations 时，可以获得以下好处：

保护

您可以在组织中启用备份策略类型，然后创建备份策略以附加到组织根、OU 或账户。备份策略将 AWS Backup 计划与该计划自动应用到您账户所需的其他详细信息相结合。直接附加到某账户的策略将与从组织根和任何从父 OU 继承的策略合并，以创建应用于该账户的有效策略。该策略包括 IAM 角色的 ID，该角色有权在您账户中的资源上运行 AWS Backup。AWS Backup 使用 IAM 角色代表您执行备份，如有效策略中的备份计划所指定。

监控

当您在组织中为 AWS Backup 启用可信访问时，您可以使用 AWS Backup 控制台查看有关组织中任何账户的备份、还原和复制作业的详细信息。有关更多信息，请参阅《AWS Backup开发人员指南》中的监控备份任务。

有关 AWS Backup 的更多信息，请参阅 AWS Backup 开发人员指南。

以下信息可帮助您将 AWS Backup 与 AWS Organizations 集成。

使用 AWS Backup 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 AWS Backup 控制台或 AWS Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 AWS Backup 控制台或工具来实现与 Organizations 的集成。这可让 AWS Backup 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 AWS Backup 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 AWS Backup 控制台或工具启用信任访问权限，则您无需完成这些步骤。

要使用 AWS Backup 启用信任访问权限，请参阅《AWS Backup 开发人员指南》中的在多个AWS 账户中启用备份。

使用 AWS Backup 禁用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

AWS Backup 需要对 AWS Organizations 的信任访问权限才能跨您组织的账户监控备份、还原和复制作业。如果禁用对 AWS Backup 的可信访问，您将无法查看当前账户以外的作业。AWS Backup 创建的 AWS Backup 角色将会保留。如果您之后重新启用可信访问，则 AWS Backup 将继续像以前一样运行，而无需您重新配置该服务。

您只能使用 Organizations 工具禁用信任访问权限。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS Backup 作为 Organizations 的信任服务。

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

  如果成功，此命令不会产生任何输出。
- AWS API：DisableAWSServiceAccess

为 AWS Backup 启用委托管理员账户

请参阅《AWS Backup 开发人员指南》中的委托管理员。

AWS Billing and Cost Management 和 AWS Organizations

AWS Billing and Cost Management 提供了一套功能，可帮助您设置账单、检索和支付发票，以及分析、整理、计划和优化成本。当您将Billing and Cost Management与之配合使用时， AWS Organizations 您可以允许分割成本分配数据检索 AWS Organizations 信息（如果适用），并收集您选择使用的分割成本分配数据服务的遥测数据。

使用以下信息来帮助您集 AWS Billing and Cost Management 成 AWS Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Billing and Cost Management 在组织中的账户中执行支持的操作。

只有在禁用 Billing and Billing and Cost Management 和 Organizations 之间的可信访问权限，或者从组织中删除成员账户时，才能删除或修改此角色。

有关更多信息，请参阅《账单和成本管理用户指南》中的 “账单和成本管理” 的服务相关角色权限。

- `AWSServiceRoleForSplitCostAllocationData`

Billing and Cost Management 使用的服务主体

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Billing and Cost Management 使用的服务相关角色向以下服务主体授予访问权限：

Billing and Cost Management 使用 `billing-cost-management.amazonaws.com`服务主体。

通过 Billing and Cost Management 实现可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

通过管理账户启用可信访问权限后，客户可以利用 Billing and Billing and Cost Management 下的拆分成本分配数据功能。当客户使用适用于 Prometheus 的亚马逊托管服务为亚马逊 Elastic Kubernetes Service 启用拆分成本分配数据时，将调用可信访问权限为组织内的所有成员账户创建服务相关角色。这允许拆分成本分配数据从客户的 Amazon Prometheus 托管服务工作空间收集遥测数据，并根据这些指标进行成本分配。

您可以使用 AWS Organizations 控制台、运行 AWS CLI 命令或在其中一个 AWS SDK 中调用 API 操作来启用可信访问。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS Billing and Cost Management 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。

3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您仅是的管理员 AWS Organizations，请告诉管理员他们现在可以使用其控制台启用该服务 AWS Organizations。 AWS Billing and Cost Management

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来启用可信服务访问：

- AWS CLI: enable-aws-service-access

  您可以运行以下命令以在 Organiz AWS Billing and Cost Management ations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：启用 AWSServiceAccess

禁用可信访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您可以仅使用 Organizations 工具禁用信任访问权限。

您可以通过运行 Organizations AWS CLI 命令或在其中一个 AWS 软件开发工具包中调用 Organizations API 操作来禁用可信访问。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来禁用可信服务访问权限：

- AWS CLI: disable-aws-service-access

  您可以运行以下命令在 Organization AWS Billing and Cost Management s 中禁用可信服务。

  ```
  $ aws organizations disable-aws-service-access \
  ```

```
    --service-principal  billing-cost-management.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- AWS API：禁用 AWSServiceAccess

AWS CloudFormation StackSets 和 AWS Organizations

利用 AWS CloudFormation StackSets，您可通过一个操作跨多个AWS 账户和AWS 区域创建、更新或删除堆栈。StackSets 与 AWS Organizations 集成可让您使用每个成员账户中具有相关权限的服务相关角色创建具有服务托管权限的堆栈套。这可将堆栈实例部署到组织中的成员账户。您无需创建必要的 AWS Identity and Access Management 角色；StackSets 代表您在每个成员账户中创建 IAM 角色。

您还可以选择为将来添加到组织的账户启用自动部署。启用自动部署后，关联堆栈集实例的角色和部署将自动添加到将来添加到该 OU 的所有账户中。

启用 StackSets 和 Organizations 之间的信任访问权限后，管理账户有权为您的组织创建和管理堆栈套。管理账户最多可以将五个成员账户注册为委托管理员。启用信任访问权限后，委托管理员还有权为您的组织创建和管理堆栈套。具有服务托管权限的堆栈集是在管理账户中创建的，包括由委托管理员创建的堆栈集。

> **Important**
>
> 委托管理员具有部署到组织中的账户的完全权限。管理账户不能限制委托管理员部署到特定 OU 或执行特定堆栈集操作的权限。

有关将 StackSets 与 Organizations 集成的更多信息，请参阅《AWS CloudFormation 用户指南》中的使用 AWS CloudFormation StackSets。

以下信息可帮助您将 AWS CloudFormation StackSets 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 AWS CloudFormation Stacksets 在您组织中的组织账户内执行支持的操作。

只有在禁用 AWS CloudFormation Stacksets 和 Organizations 之间的信任访问权限，或者从组织中删除成员账户，您才能删除或修改此角色。

- 管理账户：`AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

要为组织中的成员账户创建服务相关角色 `AWSServiceRoleForCloudFormationStackSetsOrgMember`，您需要先在管理账户中创建一个堆栈集。这将会创建一个堆栈集实例，然后该实例会在成员账户中创建相应的角色。

- 成员账户：`AWSServiceRoleForCloudFormationStackSetsOrgMember`

有关创建堆栈集的更多详细信息，请参阅 AWS CloudFormation 用户指南中的使用 AWS CloudFormation StackSets。

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。AWS CloudFormation Stacksets 使用的服务相关角色为以下服务委托人授予访问权限：

- 管理账户：`stacksets.cloudformation.amazonaws.com`

  只有在禁用 Stacksets 和 Organizations 之间的信任访问权限时，您才能修改或删除此角色。
- 成员账户：`member.org.stacksets.cloudformation.amazonaws.com`

  只有在先禁用 Stacksets 和 Organizations 之间的信任访问权限，或者先从目标组织或组织部门（OU）中删除成员账户，您才能删除或修改此角色。

使用 AWS CloudFormation Stacksets 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

只有 Organizations 管理账户的管理员有权启用对其他AWS服务的可信访问权限。您可以使用 AWS CloudFormation 控制台或 Organizations 控制台启用信任访问权限。

您只能使用 AWS CloudFormation StackSets 启用信任访问权限。

要使用 AWS CloudFormation Stacksets 启用信任访问权限，请参阅 AWS CloudFormation 用户指南中的使用 AWS Organizations 启用信任访问权限。

使用 AWS CloudFormation Stacksets 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Organizations 管理账户的管理员有权禁用对其他AWS服务的可信访问权限。您只能使用 Organizations 控制台禁用信任访问权限。如果您在使用 StackSets 时，通过 Organizations 禁用了信任访问权限，则所有之前创建的堆栈实例都将保留。但是，使用服务相关角色的权限部署的堆栈套无法再对 Organizations 管理的账户执行部署。

您可以使用 AWS CloudFormation 控制台或 Organizations 控制台禁用信任访问权限。

> **Important**
>
> 如果您以编程方式禁用信任访问权限（例如使用 AWS CLI 或 API），请注意，这将删除权限。最好使用 AWS CloudFormation 控制台启用信任访问权限。

您可以使用AWS Organizations控制台，通过运行 Organizations AWS CLI 命令，或者通过调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 AWS CloudFormation StackSets 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **`disable`**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您只是 AWS Organizations 的管理员，请告诉 AWS CloudFormation StackSets 的管理员，他们现在可以使用其控制台或工具禁用该服务，使其无法处理 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS CloudFormation StackSets 作为 Organizations 的信任服务。

```
$ aws organizations disable-aws-service-access \
    --service-principal stacksets.cloudformation.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- AWS API：DisableAWSServiceAccess

为 AWS CloudFormation 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 AWS CloudFormation Stacksets 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 AWS CloudFormation Stacksets 的管理分开。

有关如何将成员账户指定为组织中的 AWS CloudFormation Stacksets，请参阅《AWS CloudFormation 用户指南》中的注册委托管理员。

AWS CloudTrail 和 AWS Organizations

AWS CloudTrail 是一项 AWS 服务，可帮助您实现监管、合规以及运营和风险审计 AWS 账户。使用 AWS CloudTrail管理账户中的用户可以创建组织跟踪，记录该组织 AWS 账户 中所有人的所有事件。组织跟踪自动应用到组织中的所有成员账户。成员账户可以查看组织跟踪，但无法修改或删除它。默认情况下，成员账户没有权限访问 Amazon S3 存储桶中组织跟踪的日志文件。这有助于您在组织的账户中统一应用和实施事件日志记录策略。

有关更多信息，请参阅《AWS CloudTrail 用户指南》中的为组织创建跟踪。

使用以下信息来帮助您集 AWS CloudTrail 成 AWS Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色 CloudTrail 允许在组织中的组织账户中执行支持的操作。

只有在禁用 CloudTrail 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForCloudTrail`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。使用的服务相关角色向以下服务主体 CloudTrail 授予访问权限：

- `cloudtrail.amazonaws.com`

使用 CloudTrail 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

如果您通过从 AWS CloudTrail 控制台创建跟踪来启用可信访问，则会自动为您配置可信访问（推荐）。您也可以使用 AWS Organizations 控制台启用可信访问。您必须使用 AWS Organizations 管理账户登录才能创建组织跟踪。

如果您选择使用 AWS CLI 或 AWS API 创建组织跟踪，则必须手动配置可信访问权限。有关更多信息，请参阅《AWS CloudTrail 用户指南》AWS Organizations中的 CloudTrail 作为可信服务启用。

> **Important**
>
> 我们强烈建议您尽可能使用 AWS CloudTrail 控制台或工具来启用与 Organizations 的集成。

您可以通过运行 Organizations AWS CLI 命令或在其中一个 AWS 软件开发工具包中调用 Organizations API 操作来启用可信访问。

AWS CLI, AWS API

使用 Organizations CLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来启用可信服务访问：

- AWS CLI: enable-aws-service-access

  您可以运行以下命令以在 Organiz AWS CloudTrail ations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- AWS API：启用 AWSServiceAccess

使用 CloudTrail 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

AWS CloudTrail 需要使用可信访问权限 AWS Organizations 才能使用组织跟踪和组织事件数据存储。如果您 AWS Organizations 在使用时使用禁用可信访问权限 AWS CloudTrail，则成员账户的所有组织跟踪都将被删除，因为 CloudTrail 无法访问该组织。所有管理账户组织跟踪和组织事件数据存储都将转换为账户级跟踪和事件数据存储。为两者之间的 CloudTrail 集成而创建的`AWSServiceRoleForCloudTrail`角色将 AWS Organizations 保留在账户中。如果您重新启用可信访问权限，则 CloudTrail 不会对现有跟踪和事件数据存储执行操作。管理账户必须更新所有账户级别的跟踪和事件数据存储，才能将其应用于组织。

要将账户级跟踪或事件数据存储转换为组织跟踪或组织事件数据存储，请执行以下操作：

- 在 CloudTrail 控制台中，更新跟踪或事件数据存储，然后选择 “为我的组织中的所有账户启用” 选项。
- 从中 AWS CLI，执行以下操作：
  - 要更新跟踪，请运行update-trail命令并添加`--is-organization-trail`参数。
  - 要更新事件数据存储，请运行update-event-data-store命令并添加`--organization-enabled`参数。

只有 AWS Organizations 管理账户中的管理员才能使用禁用可信访问权限 AWS CloudTrail。您只能使用组织工具禁用可信访问，使用 AWS Organizations 控制台、运行 Organizations AWS CLI 命令或在其中一个 AWS 软件开发工具包中调用 Organizations API 操作。

您可以使用 AWS Organizations 控制台、运行 Organizations AWS CLI 命令或在其中一个 AWS 软件开发工具包中调用 Organizations API 操作来禁用可信访问。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 AWS CloudTrail 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。

4. 在确认对话框中输入 **disable**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您仅是的管理员 AWS Organizations，请告知管理员他们现在可以使用该服务的控制台或工具来禁用该服务 AWS Organizations。 AWS CloudTrail

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来禁用可信服务访问权限：

- AWS CLI: disable-aws-service-access

  您可以运行以下命令在 Organization AWS CloudTrail s 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。
- AWS API：禁用 AWSServiceAccess

为其启用委派管理员账户 CloudTrail

当您 CloudTrail 与 Organizations 一起使用时，您可以注册组织内的任何账户，使其成为 CloudTrail 委托管理员，代表组织管理组织的跟踪和事件数据存储。委派管理员是组织中的成员帐户，可以在中执行与管理帐户 CloudTrail 相同的管理任务。

> **最小权限**
>
> 只有 Organizations 管理账户中的管理员才能为其注册委托管理员 CloudTrail。

您可以使用 CloudTrail 控制台，也可以使用 Organizations `RegisterDelegatedAdministrator` CLI 或 SDK 操作来注册委派管理员帐户。要使用 CloudTrail 控制台注册委派管理员，请参阅添加 CloudTrail 委派管理员。

禁用委派的管理员 CloudTrail

只有 Organizations 管理账户中的管理员才能移除其委派的管理员 CloudTrail。您可以使用 CloudTrail 控制台，也可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作来移

除委派的管理员。有关如何使用 CloudTrail 控制台移除委派管理员的信息，请参阅移除 CloudTrail 委派管理员。

AWS Compute Optimizer 和 AWS Organizations

AWS Compute Optimizer 是一种服务，用于分析 AWS 资源的配置和利用率指标。资源示例包括 Amazon Elastic Compute Cloud（Amazon EC2）实例和 Auto Scaling 组。Compute Optimizer 报告您的资源是否处于最佳状态并生成优化建议，以降低成本并提高工作负载的性能。有关 Compute Optimizer 的更多信息，请参阅 AWS Compute Optimizer 用户指南。

以下信息可帮助您将 AWS Compute Optimizer 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Compute Optimizer 在您组织中的组织账户内执行支持的操作。

只有在禁用 Compute Optimizer 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForComputeOptimizer`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Compute Optimizer 使用的服务相关角色为以下服务委托人授予访问权限：

- `compute-optimizer.amazonaws.com`

使用 Compute Optimizer 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 AWS Compute Optimizer 控制台或 AWS Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 AWS Compute Optimizer 控制台或工具来实现与 Organizations 的集成。这可让 AWS Compute Optimizer 执行所需的任何配置，例如创建服务所需的资源。请仅

在您无法使用 AWS Compute Optimizer 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
如果您使用 AWS Compute Optimizer 控制台或工具启用信任访问权限，则您无需完成这些步骤。

使用 Compute Optimizer 控制台启用信任访问权限

您必须使用组织的管理账户登录 Compute Optimizer 控制台。代表您的组织选择启用，方法是按照《AWS Compute Optimizer 用户指南》中的选择启用账户中的说明操作。

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS Compute Optimizer 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Compute Optimizer 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS Compute Optimizer 作为 Organizations 的信任服务。

```
$ aws organizations enable-aws-service-access \
    --service-principal compute-optimizer.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- AWS API：EnableAWSServiceAccess

使用 Compute Optimizer 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 AWS Organizations 管理账户中的管理员可以禁用对 AWS Compute Optimizer 的信任访问权限。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS Compute Optimizer 作为 Organizations 的信任服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：DisableAWSServiceAccess

为 Compute Optimizer 启用委托管理员账户

当您将某个成员账户指定为组织的委托管理员时，来自指定账户的用户和角色将可以管理组织内其他成员账户的 AWS 账户元数据。如果您没有启用委托管理员账户，则这些任务只能由组织的管理账户执行。这有利于您将组织的管理与您的账户详细信息的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色才能将某个成员账户配置为组织的 Compute Optimizer 委托管理员。

有关为 Compute Optimizer 启用委托管理员账户的说明，请参阅AWS Compute Optimizer 用户指南中的 https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html。

AWS CLI, AWS API

如果要使用 AWS CLI 或某个 AWS SDK 配置委托管理员账户，您可以使用以下命令：

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal compute-optimizer.amazonaws.com
```

- AWS SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务主体 `account.amazonaws.com` 确定为参数。

为 Compute Optimizer 禁用委托管理员账户

只有组织管理账户中的管理员才能为 Compute Optimizer 配置委托管理员。

要使用 Compute Optimizer 控制台禁用委托管理员 Compute Optimizer 账户，请参阅 AWS Compute Optimizer 用户指南中的 https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html。

要使用 AWS AWS CLI 移除委托管理员，请参阅 AWS AWS CLI 命令参考中的 deregister-delegated-administrator。

AWS Config 和 AWS Organizations

AWS Config 中多账户、多区域数据聚合使您能够将多个账户和AWS 区域中的 AWS Config 数据聚合到单个账户中。多账户、多区域数据聚合用于中心 IT 管理员监控企业中多个AWS 账户的合规性。聚合器是 AWS Config 中的一种资源类型，用于从多个源账户和区域收集 AWS Config 数据。在要查看聚合 AWS Config 数据的区域中创建聚合器。创建聚合器时，您可以选择添加独立账户 ID 或您的组织。有关 AWS Config 的更多信息，请参阅 AWS Config 开发人员指南。

您还可以使用 AWS Config API 在组织中跨所有AWS 账户来管理 AWS Config 规则。有关更多信息，请参阅《AWS Config 开发人员指南》中的跨组织中的所有账户启用 AWS Config 规则。

以下信息可帮助您将 AWS Config 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时在组织的账户中创建。此角色允许 AWS Config 在您组织中的账户内执行支持的操作。

- `AWSServiceRoleForConfig`

当您通过创建多账户聚合器在组织中启用 AWS Config 时，会自动创建此角色。AWS Config 要求您选择或创建角色，并为您提供名称。没有自动生成的名称。

只有在禁用 AWS Config 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

使用 AWS Config 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 AWS Config 控制台或 AWS Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 AWS Config 控制台或工具来实现与 Organizations 的集成。这可让 AWS Config 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 AWS Config 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 AWS Config 控制台或工具启用信任访问权限，则您无需完成这些步骤。

使用 AWS Config 控制台启用可信访问权限

要使用 AWS Config 允许对 AWS Organizations 的信任访问权限，请创建多账户聚合器并添加组织。有关如何配置多账户聚合器的信息，请参阅《AWS Config 用户指南》中的使用控制台设置聚合器。

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。

2. 在 Services (服务) 页面上，找到 AWS Config 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Config 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS Config 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：EnableAWSServiceAccess

使用 AWS Config 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用信任访问权限。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

您可以运行以下命令以禁用 AWS Config 作为 Organizations 的信任服务。

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

如果成功，此命令不会产生任何输出。

- AWS API：DisableAWSServiceAccess

AWS 成本优化中心 和 AWS Organizations

AWS 成本优化中心 是一项 B AWS illing and Cost Management 功能，可帮助您整合不同 AWS 账户和 AWS 地区的成本优化建议并确定其优先顺序，从而最大限 AWS 度地利用支出。当您使用成本优化中心时， AWS Organizations 您可以轻松识别、筛选和汇总您的 Organizations 成员账户和 AWS 地区 AWS 的成本优化建议。

有关更多信息，请参阅《AWS Cost Management 用户指南》中的 “成本优化中心”。

使用以下信息来帮助您集 AWS 成本优化中心 成 AWS Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许成本优化中心在组织中的账户中执行支持的操作。

只有在禁用 Cost Optimation Hub 和 Organizations 之间的可信访问权限或从组织中删除成员帐户时，才能删除或修改此角色。

有关更多信息，请参阅《AWS Cost Management 用户指南》中的 “成本优化中心” 的服务相关角色权限。

- `AWSServiceRoleForCostOptimizationHub`

成本优化中心使用的服务主体

成本优化中心使用`cost-optimization-hub.bcm.amazonaws.com`服务主体。

使用成本优化中心实现可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

当您选择使用组织的管理账户并包括组织内的所有成员账户时，您的组织账户中将自动启用成本优化中心的可信访问权限。

您可以使用 AWS Organizations 控制台、运行 AWS CLI 命令或在其中一个 AWS SDK 中调用 API 操作来启用可信访问。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS 成本优化中心 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您仅是的管理员 AWS Organizations，请告诉管理员他们现在可以使用其控制台启用该服务 AWS Organizations。 AWS 成本优化中心

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来启用可信服务访问：

- AWS CLI: enable-aws-service-access

  您可以运行以下命令以在 Organiz AWS 成本优化中心 ations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：启用 AWSServiceAccess

禁用可信访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您可以仅使用 Organizations 工具禁用信任访问权限。

> **Important**
>
> 如果您在选择加入后禁用成本优化中心可信访问权限，则成本优化中心将拒绝访问您组织成员账户的推荐。此外，组织内的成员账户不会选择加入成本优化中心。要了解更多信息，请参阅AWS Cost Management 用户指南中的 “成本优化中心” 和 “Organizations 可信访问”。

您可以通过运行 Organizations AWS CLI 命令或在其中一个 AWS 软件开发工具包中调用 Organizations API 操作来禁用可信访问。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来禁用可信服务访问权限：

- AWS CLI: disable-aws-service-access

  您可以运行以下命令在 Organization AWS 成本优化中心 s 中禁用可信服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：禁用 AWSServiceAccess

AWS Control Tower 和 AWS Organizations

AWS Control Tower 提供了一种简单的方法来设置和管理 AWS 多账户环境，遵循规范的最佳做法。AWS Control Tower 编排扩展了 AWS Organizations 的功能。AWS Control Tower 应用预防性和检测性控制措施（防护机制）来帮助您的组织和账户避免偏离最佳做法（漂移）。

AWS Control Tower 编排扩展了 AWS Organizations 的功能。

有关更多信息，请参阅《AWS Control Tower 用户指南》。

以下信息可帮助您将 AWS Control Tower 与 AWS Organizations 集成。

集成所需的角色

AWSControlTowerExecution 角色必须存在于所有注册的账户中。它允许 AWS Control Tower 管理您的各个账户，并向审核和日志存档账户报告有关这些账户的信息。

要了解有关 AWS Control Tower 使用的角色的更多信息，请参阅 AWS Control Tower 如何与角色一起创建和管理账户和为 AWS Control Tower 使用基于身份的策略 (IAM policy)。

AWS Control Tower 使用的服务主体

AWS Control Tower 使用 controltower.amazonaws.com 服务主体。

使用 AWS Control Tower 启用信任访问权限

AWS Control Tower 使用可信访问来检测偏移以进行预防性控制，并跟踪导致偏移的账户和 OU 更改。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Organizations 工具启用信任访问权限。

要从 Organizations 控制台启用可信访问，请选择 AWS Control Tower 旁边的 **Enable access**。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来启用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS Control Tower 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- AWS API：EnableAWSServiceAccess

使用 AWS Control Tower 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用信任访问权限。

> **Important**
>
> 禁用 AWS Control Tower 的可信访问权限会导致您的 AWS Control Tower 登录区出现偏差。修复偏差的唯一方法是使用 AWS Control Tower 的登录区修复。在 Organizations 中重新启用可信访问权限并不能解决偏差。在《AWS Control Tower 用户指南》中了解有关偏差的更多信息。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS Control Tower 作为 Organizations 的信任服务。

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

  如果成功，此命令不会产生任何输出。
- AWS API：DisableAWSServiceAccess

Amazon Detective 和 AWS Organizations

Amazon Detective 使用日志数据生成可视化图像，使您能够分析、调查和识别安全结果或可疑活动的根本原因。

使用 AWS Organizations 以允许您可以确保通过 Detective 行为图了解所有组织账户的活动。

当您授予对 Detective 的信任访问权限时，Detective 服务可以自动应对组织成员资格的更改。委托管理员可在行为图中启用任何组织账户作为成员账户。Detective 还可以自动启用新组织账户作为成员账户。组织账户无法解除自己与行为图的关联。

有关更多信息，请参阅《Amazon Detective 管理指南》中的在组织中使用 Amazon Detective。

使用以下信息可帮助您将 Amazon Detective 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Detective 在您组织中的组织账户内执行受支持的操作。

只有在禁用 Detective 与 Organizations 之间的信任访问权限后，或是从组织中删除成员账户后，您才能删除或修改此角色。

- `AWSServiceRoleForDetective`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Detective 使用的服务相关角色为以下服务主体授予访问权限：

- `detective.amazonaws.com`

使用 Detective 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

> **Note**
>
> 当您为 Amazon Detective 指定委托管理员时，Detective 会自动为您的组织启用 Detective 信任访问权限。
> Detective 需要具有对 AWS Organizations 的信任访问权限，然后您才能为您的组织将某个成员账户指定为此服务的委托管理员。

您只能使用 Organizations 工具启用信任访问权限。

您可以使用 AWS Organizations 控制台启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务)页面上，找到 Amazon Detective 行，选择该服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 Amazon Detective 的管理员，他们现在可以使用其控制台启用该服务与 AWS Organizations 配合使用。

使用 Detective 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 AWS Organizations 管理账户中的管理员可以使用 Amazon Detective 禁用信任访问权限。

您可以仅使用 Organizations 工具禁用信任访问权限。

您可以使用 AWS Organizations 控制台禁用信任访问权限。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 Amazon Detective 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **`disable`**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您只是 AWS Organizations 的管理员，请告诉 Amazon Detective 的管理员，他们现在可以使用其控制台或工具禁用该服务，使其无法与 AWS Organizations 配合使用。

为 Detective 启用委托管理员账户

Detective 的委托管理员账户是 Detective 行为图的管理员账户。委托管理员决定要启用和禁用该行为图中的哪些组织账户的成员账户状态。委托管理员可将 Detective 配置为在将新组织账户添加到组织时，自动启用这些账户作为成员账户。有关委托管理员如何管理组织账户的信息，请参阅《Amazon Detective 管理指南》中的将组织账户作为成员账户进行管理。

只有组织管理账户中的管理员才能为 Detective 配置委托管理员。

您可以通过 Detective 控制台或 API，或者通过使用 Organizations CLI 或 SDK 操作，来指定委托管理员账户。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色能够将某个成员账户配置为组织的 Detective 委托管理员。

要使用 Detective 控制台或 API 配置委托管理员，请参阅《Amazon Detective 管理指南》中的为组织指定 Detective 管理员账户。

AWS CLI, AWS API

如果要使用 AWS CLI 或某个 AWS SDK 配置委托管理员账户，您可以使用以下命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal detective.amazonaws.com
```

- AWS SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务主体 `account.amazonaws.com` 确定为参数。

为 Detective 禁用委托管理员

您可以使用 Detective 控制台或 API，或者通过使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作，来删除委托管理员。有关如何使用 Detective 控制台或 API 或 Organizations API 删除委托管理员的信息，请参阅《Amazon Detective 管理指南》中的为组织指定 Detective 管理员账户。

Amazon DevOps Guru 和 AWS Organizations

Amazon DevOps Guru 会分析操作数据以及应用程序指标和事件，以识别偏离正常操作模式的行为。当 DevOps Guru 检测到操作问题或风险时，会通知用户。

借助 AWS Organizations 使用 DevOps Guru 启用多账户支持，以便您可以指定成员账户来管理整个组织的见解。此委托管理员随后可以查看、排序和筛选组织内所有账户的见解，以全面了解组织内所有受监控应用程序运行状况，而无需进行任何额外的自定义。

有关更多信息，请参阅《Amazon DevOps Guru 用户指南》中的监控组织中的帐户。

使用以下信息帮助您将 Amazon DevOps Guru 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 DevOps Guru 在您组织中的组织账户内执行受支持的操作。

只有在禁用 DevOps Guru 与 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForDevOpsGuru`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。DevOps Guru 使用的服务相关角色为以下服务委托人授予访问权限：

- `devops-guru.amazonaws.com`

有关更多信息，请参阅《Amazon DevOps Guru 用户指南》中的将服务相关角色用于 DevOps Guru。

使用 DevOps Guru 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

> **Note**
>
> 当您为 Amazon DevOps Guru 指定委托管理员时，DevOps Guru 会自动为您的组织启用 DevOps Guru 信任访问权限。

DevOps Guru 需要拥有对 AWS Organizations 的信任访问权限，然后您才能为您的组织将某个成员账户指定为此服务的委托管理员。

Important

强烈建议您尽可能使用 Amazon DevOps Guru 控制台或工具来实现与 Organizations 的集成。这使 Amazon DevOps Guru 可以任何所需的配置，例如创建服务所需的资源。请仅在您无法使用 Amazon DevOps Guru 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。

您可以使用 AWS Organizations 控制台或 DevOps Guru 控制台启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 Amazon DevOps Guru 行，选择该服务的名称，然后选择 Enable trusted access（启用信任访问权限）。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 Amazon DevOps Guru 的管理员，他们现在可以使用其控制台启用该服务与 AWS Organizations 配合使用。

DevOps Guru console

使用 DevOps Guru 控制台启用信任访问权限

1. 以管理账户中的管理员身份登录并打开 DevOps Guru 控制台：Amazon DevOps Guru 控制台
2. 选择 Enable trusted access (启用可信访问)。

使用 DevOps Guru 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 AWS Organizations 管理账户中的管理员可以使用 Amazon DevOps Guru 禁用信任访问权限。

您可以仅使用 Organizations 工具禁用信任访问权限。

您可以使用 AWS Organizations 控制台禁用信任访问权限。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 Amazon DevOps Guru 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **`disable`**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您只是 AWS Organizations 的管理员，请告诉 Amazon DevOps Guru 的管理员，他们现在可以使用其控制台或工具禁用该服务，使其无法与 AWS Organizations 配合使用。

为 DevOps Guru 启用委托管理员账户

DevOps Guru 的委托管理员账户可以查看从组织中引导到 DevOps Guru 的所有成员账户的见解数据。有关委托管理员如何管理组织账户的信息，请参阅《Amazon DevOps Guru 用户指南》中的监控组织中的账户。

只有组织管理账户中的管理员才能为 DevOps Guru 配置委托管理员。

您可以通过 DevOps Guru 控制台，或者通过使用 Organizations `RegisterDelegatedAdministrator` CLI 或 SDK 操作，来指定委托管理员账户。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色能够将某个成员账户配置为组织中的 DevOps Guru 的委托管理员。

DevOps Guru console

在 DevOps Guru 控制台中配置委托管理员

1. 以管理账户中的管理员身份登录并打开 DevOps Guru 控制台：Amazon DevOps Guru 控制台

2. 选择 Register delegated administrator (注册委派管理员)。您可以选择管理账户或任何成员账户作为委托管理员。

AWS CLI, AWS API

如果要使用 AWS CLI 或某个 AWS SDK 配置委托管理员账户，您可以使用以下命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal devops-guru.amazonaws.com
```

- AWS SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务主体 `account.amazonaws.com` 确定为参数。

为 DevOps Guru 禁用委托管理员

您可以使用 DevOps Guru 控制台，或者通过使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作，来删除委托管理员。有关如何使用 DevOps Guru 控制台删除委托管理员的信息，请参阅《Amazon DevOps Guru 用户指南》中的监控组织中的账户。

AWS Directory Service 和 AWS Organizations

Microsoft Active Directory 版 AWS Directory Service 或 AWS Managed Microsoft AD 可使您以托管服务的形式运行 Microsoft Active Directory（AD）。通过 AWS Directory Service 可轻松在AWS云中设置和运行目录，或将AWS资源与现有的本地 Microsoft Active Directory 相连。AWS Managed Microsoft AD 还可与 AWS Organizations 进行紧密集成，以实现在多个AWS 账户和某一地区内的任意 VPC 内实现目录的无缝分享。有关更多信息，请参阅 AWS Directory Service 管理指南。

以下信息可帮助您将 AWS Directory Service 与 AWS Organizations 集成。

使用 AWS Directory Service 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 AWS Directory Service 控制台或 AWS Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 AWS Directory Service 控制台或工具来实现与 Organizations 的集成。这可让 AWS Directory Service 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 AWS Directory Service 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
>
> 如果您使用 AWS Directory Service 控制台或工具启用信任访问权限，则您无需完成这些步骤。

使用 AWS Directory Service 控制台启用可信访问权限

要共享自动启用信任访问权限的目录，请参阅《AWS Directory Service 管理指南》中的共享您的目录。如需分步说明，请参阅教程：共享AWS托管式 Microsoft AD 目录。

您可以使用 AWS Organizations 控制台启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS Directory Service 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Directory Service 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

使用 AWS Directory Service 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

如果在使用 AWS Directory Service 时禁止使用 AWS Organizations 进行信任访问，所有先前共享的目录会继续正常运行。但是，在重新启用信任访问权限前，您将无法再在组织内共享新目录。

您只能使用 Organizations 工具禁用信任访问权限。

您可以使用 AWS Organizations 控制台禁用信任访问权限。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 AWS Directory Service 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **`disable`**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Directory Service 的管理员，他们现在可以使用其控制台或工具禁用该服务，使其无法处理 AWS Organizations。

AWS Firewall Manager 和 AWS Organizations

AWS Firewall Manager 是一项安全管理服务，您可以使用它集中配置和管理组织中AWS 账户和应用程序的防火墙规则。使用 Firewall Manager，您可以轻松地推行 AWS WAF 规则，创建 AWS Shield Advanced 保护、配置和审计 Amazon Virtual Private Cloud（Amazon VPC）安全组，并部署 AWS Network Firewall。使用 Firewall Manager 一次设置好保护措施，并让它们跨组织中的所有账户和资源自动应用，即使添加新资源和账户时也是如此。有关 AWS Firewall Manager 的更多信息，请参阅 AWS Firewall Manager 开发人员指南。

以下信息可帮助您将 AWS Firewall Manager 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Firewall Manager 在您组织中的组织账户内执行支持的操作。

只有在禁用 Firewall Manager 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForFMS`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Firewall Manager 使用的服务相关角色为以下服务委托人授予访问权限：

- `fms.amazonaws.com`

使用 Firewall Manager 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 AWS Firewall Manager 控制台或 AWS Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 AWS Firewall Manager 控制台或工具来实现与 Organizations 的集成。这可让 AWS Firewall Manager 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 AWS Firewall Manager 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
>
> 如果您使用 AWS Firewall Manager 控制台或工具启用信任访问权限，则您无需完成这些步骤。

您必须使用您的 AWS Organizations 管理账户登录，才能在组织内配置一个账户作为 AWS Firewall Manager 管理员账户。有关更多信息，请参阅《AWS Firewall Manager 开发人员指南》中的设置 AWS Firewall Manager 管理员账户。

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS Firewall Manager 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。

3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Firewall Manager 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS Firewall Manager 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：EnableAWSServiceAccess

使用 Firewall Manager 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您可以使用 AWS Firewall Manager 或者 AWS Organizations 工具禁用信任访问权限。

> **Important**
>
> 强烈建议您尽可能使用 AWS Firewall Manager 控制台或工具来禁用与 Organizations 的集成。这可让 AWS Firewall Manager 执行所需的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 AWS Firewall Manager 提供的工具禁用集成时，才会使用这些步骤进行处理。
> 如果您使用 AWS Firewall Manager 控制台或工具禁用信任访问权限，则您无需完成这些步骤。

使用 Firewall Manager 控制台禁用信任访问权限

您可以按照《AWS Firewall Manager 开发人员指南》中的指定另一个账户作为 AWS Firewall Manager 管理员账户中的说明更改或撤消 AWS Firewall Manager 管理员账户。

如果您撤消此管理员账户，则必须登录 AWS Organizations 管理账户并为 AWS Firewall Manager 设置一个新的管理员账户。

您可以使用AWS Organizations控制台，通过运行 Organizations AWS CLI 命令，或者通过调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 AWS Firewall Manager 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **disable**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Firewall Manager 的管理员，他们现在可以使用其控制台或工具禁用该服务，使其无法处理 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS Firewall Manager 作为 Organizations 的信任服务。

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

  如果成功，此命令不会产生任何输出。

- AWS API：DisableAWSServiceAccess

为 Firewall Manager 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 Firewall Manager 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 Firewall Manager 的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色才能将成员账户配置为组织中 Firewall Manager 的委托管理员。

有关如何将成员账户指定为组织的 Firewall Manager 管理员的说明，请参阅《AWS Firewall Manager 开发人员指南》中的设置 AWS Firewall Manager 管理员账户。

Amazon GuardDuty 和 AWS Organizations

Amazon GuardDuty 是一个持续的安全监控服务，可以通过它分析和处理各种数据源，使用威胁情报源和机器学习来识别AWS环境中的意外的、未经授权的恶意活动。这包括特权升级、使用遭暴露的凭证或者与恶意 IP 地址、URL 或域通信或者您的 Amazon Elastic Compute Cloud 实例和容器工作负载中存在恶意软件等问题。

您可以使用 Organizations 管理组织中所有账户的 GuardDuty，从而帮助简化 GuardDuty 的管理工作。

有关更多信息，请参阅《Amazon GuardDuty 用户指南》中的使用 AWS Organizations 管理 GuardDuty 账户。

使用以下信息可帮助您将 Amazon GuardDuty 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

当您启用可信访问时，将在您组织的管理账户中自动创建以下服务相关角色。这些角色允许 GuardDuty 在您组织中的组织账户内执行支持的操作。只有当在 GuardDuty 和 Organizations 之间禁用可信访问，或者从组织中删除成员账户时，您才能删除角色。

- `AWSServiceRoleForAmazonGuardDuty` 服务相关角色是在已将 GuardDuty 与 Organizations 集成的账户中自动创建的。有关更多信息，请参阅《Amazon GuardDuty 用户指南》中的使用 Organizations 管理 GuardDuty 账户。

- AmazonGuardDutyMalwareProtectionServiceRolePolicy 服务相关角色是在启用了 GuardDuty Malware Protection 的账户中自动创建的。有关更多信息，请参阅《Amazon GuardDuty 用户指南》中的 GuardDuty Malware Protection 的服务相关角色权限

服务相关角色使用的服务委托人

- guardduty.amazonaws.com，由 AWSServiceRoleForAmazonGuardDuty 服务相关角色使用。
- malware-protection.guardduty.amazonaws.com，由 AmazonGuardDutyMalwareProtectionServiceRolePolicy 服务相关角色使用。

使用 GuardDuty 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Amazon GuardDuty 启用信任访问权限。

在将委托成员账户作为组织的 GuardDuty 管理员之前，Amazon GuardDuty 需要对 AWS Organizations 的信任访问权限。如果您使用 GuardDuty 控制台配置委托管理员，GuardDuty 会自动为您启用信任访问权限。

但是，如果要使用 AWS CLI 或某个 AWS SDK 配置委托管理员用户，那么您必须明确调用 EnableAWSServiceAccess 操作并提供服务委托人作为参数。然后，您可以调用 EnableOrganizationAdminAccount 来委托 GuardDuty 管理员账户。

使用 GuardDuty 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用信任访问权限。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 Amazon GuardDuty 作为 Organizations 的信任服务。

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

  如果成功，此命令不会产生任何输出。

- AWS API：DisableAWSServiceAccess

为 GuardDuty 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 GuardDuty 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 GuardDuty 的管理分开。

> **最小权限**
>
> 有关将成员账户指定为委托管理员所需的权限的信息，请参阅《Amazon GuardDuty 用户指南》中的指定委托管理员所需的权限。

指定一个成员账户作为 GuardDuty 的委托管理员

请参阅指定委托管理员并添加成员账户（控制台）和指定委托管理员并添加成员账户（API）

AWS Health 和 AWS Organizations

AWS Health 提供对您的资源性能以及 AWS 服务和账户可用性的持续可见性。 AWS Health 当您的 AWS 资源和服务受到问题影响或将受到即将发生的变更影响时，会发送事件。启用组织视图后，组织管理账户中的用户可以汇总组织中所有账户 AWS Health 的事件。组织视图仅显示启用该功能后交付 AWS Health 的事件，并将其保留 90 天。

您可以使用 AWS Health 控制台、 AWS Command Line Interface (AWS CLI) 或 AWS Health API 启用组织视图。

有关更多信息，请参阅《AWS Health 用户指南》中的聚合 AWS Health 事件。

使用以下信息来帮助您集 AWS Health 成 AWS Organizations。

用于集成的服务关联角色

`AWSServiceRoleForHealth_Organizations`服务相关角色 AWS Health 允许在组织中的组织账户中执行支持的操作。

当您通过调用 EnableHealthServiceAccessForOrganizationAPI 操作启用可信访问时，将在您组织的管理账户中自动创建此角色。否则，请使用 AWS Health 控制台、API 或 CLI 创建角色，如 IAM 用户指南中的创建服务相关角色中所述。

只有在 AWS Health 和 Organizations 之间禁用可信访问权限或从组织中移除成员帐户后，才能删除或修改此角色。

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。使用的服务相关角色向以下服务主体 AWS Health 授予访问权限：

- `health.amazonaws.com`

使用 AWS Health启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

当您启用组织视图功能时 AWS Health，还会自动为您启用可信访问权限。

您可以使用 AWS Health 控制台或控制台启用可信访问。 AWS Organizations

> **Important**
>
> 我们强烈建议您尽可能使用 AWS Health 控制台或工具来启用与 Organizations 的集成。这允许 AWS Health 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 AWS Health提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 AWS Health 控制台或工具启用可信访问，则无需完成这些步骤。

使用 AWS Health 控制台启用可信访问

您可以使用 AWS Health 和以下选项之一来启用可信访问：

- 使用控制 AWS Health 台。有关更多信息，请参阅《AWS Health 用户指南》中的组织视图（控制台）。
- 使用 AWS CLI。有关更多信息，请参阅《AWS Health 用户指南》中的组织视图（CLI）。
- 调用 EnableHealthServiceAccessForOrganization API 操作 。

您可以通过运行 Organizations AWS CLI 命令或在其中一个 AWS 软件开发工具包中调用 Organizations API 操作来启用可信访问。

AWS CLI, AWS API

使用 Organizations CLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来启用可信服务访问：

- AWS CLI: enable-aws-service-access

  您可以运行以下命令以在 Organiz AWS Health ations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：启用 AWSServiceAccess

使用 AWS Health禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

禁用组织视图功能后，将 AWS Health 停止聚合组织中所有其他账户的事件。这也会自动禁用您的信任访问权限。

您可以使用 AWS Health 或 AWS Organizations 工具禁用可信访问。

> **Important**
>
> 我们强烈建议您尽可能使用 AWS Health 控制台或工具来禁用与 Organizations 的集成。这允许 AWS Health 执行它需要的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 AWS Health提供的工具禁用集成时，才会使用这些步骤进行处理。

如果您使用 AWS Health 控制台或工具禁用可信访问，则无需完成这些步骤。

使用 AWS Health 控制台禁用可信访问

您可以使用以下选项之一禁用信任访问权限：

- 使用控制 AWS Health 台。有关更多信息，请参阅《AWS Health 用户指南》中的禁用组织视图（控制台）。
- 使用 AWS CLI。有关更多信息，请参阅《AWS Health 用户指南》中的禁用组织视图（CLI）。
- 调用 DisableHealthServiceAccessForOrganization API 操作 。

您可以通过运行 Organizations AWS CLI 命令或在其中一个 AWS 软件开发工具包中调用 Organizations API 操作来禁用可信访问。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来禁用可信服务访问权限：

- AWS CLI: disable-aws-service-access

  您可以运行以下命令在 Organization AWS Health s 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。
- AWS API：禁用 AWSServiceAccess

为其启用委派管理员账户 AWS Health

将成员账户指定为组织的委托管理员后，该账户中的用户和角色将能够对 AWS Health 执行本来只能由组织管理账户中的用户或角色执行的管理操作。这有利于将组织的管理与 AWS Health的管理分开。

指定一个成员账户作为 AWS Health 的委托管理员

请参阅为您的组织视图注册委派管理员

移除 AWS Health 的委派管理员

请参阅从您的组织视图中移除委派管理员

Amazon Inspector 和 AWS Organizations

Amazon Inspector 是一项自动漏洞管理服务，可持续扫描 Amazon EC2 和容器工作负载中是否存在软件漏洞和意外网络暴露。

使用 Amazon Inspector，您只需为 Amazon Inspector 委托一个管理员账户，即可管理通过 AWS Organizations 关联的多个账户。该委托管理员将为组织管理 Amazon Inspector，并将获得代表您的组织执行诸如以下任务的特殊权限：

- 启用或禁用对成员账户的扫描
- 查看从整个组织汇总的查找结果数据
- 创建和管理禁止规则

有关更多信息，请参阅《Amazon Inspector 用户指南》中的使用 AWS Organizations 管理多个账户。

可以使用以下信息帮助您将 Amazon Inspector 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Amazon Inspector 在您组织中的组织账户内执行受支持的操作。

只有在禁用 Amazon Inspector 与 Organizations 之间的信任访问权限后，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForAmazonInspector2`

有关更多信息，请参阅《Amazon Inspector 用户指南》中的将服务相关角色用于 Amazon Inspector。

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Amazon Inspector 使用的服务相关角色为以下服务委托人授予访问权限：

- `inspector2.amazonaws.com`

使用 Amazon Inspector 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

Amazon Inspector 需要具有对 AWS Organizations 的信任访问权限，然后您才能为您的组织将某个成员账户指定为此服务的委托管理员。

当您为 Amazon Inspector 指定委托管理员时，Amazon Inspector 会自动为您的组织启用 Amazon Inspector 信任访问权限。

但是，如果您要使用 AWS CLI 或某个 AWS SDK 配置委托管理员账户，则您必须明确调用 `EnableAWSServiceAccess` 操作并提供服务主体作为参数。然后您可以调用 `EnableDelegatedAdminAccount` 以委托 Inspector 管理员账户。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来启用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以使用 Organizations 启用 Amazon Inspector 作为信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- AWS API：EnableAWSServiceAccess

> **Note**
>
> 如果您使用 `EnableAWSServiceAccess` API，您还需要调用 `EnableDelegatedAdminAccount` 以委托 Inspector 管理员账户。

使用 Amazon Inspector 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 AWS Organizations 管理账户中的管理员可以使用 Amazon Inspector 禁用信任访问权限。

您只能使用 Organizations 工具禁用信任访问权限。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以使用 Organizations 禁用 Amazon Inspector 作为信任服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：DisableAWSServiceAccess

为 Amazon Inspector 启用委托管理员账户

借助 Amazon Inspector，您可以通过 AWS Organizations 服务使用授权管理员管理组织中的多个账户。

AWS Organizations 管理账户将组织内的某一账户指定为 Amazon Inspector 的委托管理员账户。委托管理员管理组织的 Amazon Inspector，并获得代表您的组织执行诸如以下任务的特殊权限：启用或禁用对成员账户的扫描、查看从整个组织汇总的查找结果数据，以及创建和管理禁止规则

有关委托管理员如何管理组织账户的信息，请参阅《Amazon Inspector 用户指南》中的了解管理员账户与成员账户之间的关系。

只有组织管理账户中的管理员才能为 Amazon Inspector 配置委托管理员。

您可以通过 Amazon Inspector 控制台或 API，或者通过使用 Organizations CLI 或 SDK 操作，来指定委托管理员账户。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色能够将某个成员账户配置为组织中 Amazon Inspector 的委托管理员。

要使用 Amazon Inspector 控制台配置委托管理员，请参阅《Amazon Inspector 用户指南》中的步骤 1：启用 Amazon Inspector - 多账户环境。

> **Note**
>
> 您必须在使用 Amazon Inspector 的每个区域调用 `inspector2:enableDelegatedAdminAccount`。

AWS CLI, AWS API

如果要使用 AWS CLI 或某个 AWS SDK 配置委托管理员账户，您可以使用以下命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- AWS SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务主体 `account.amazonaws.com` 确定为参数。

为 Amazon Inspector 禁用委托管理员

只有 AWS Organizations 管理账户中的管理员才能从组织中删除委托管理员账户。

您可以使用 Amazon Inspector 控制台或 API，或者通过使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作，来删除委托管理员。要使用 Amazon Inspector 控制台删除委托管理员，请参阅《Amazon Inspector 用户指南》中的删除委托管理员。

AWS License Manager 和 AWS Organizations

AWS License Manager 简化了将软件供应商许可证迁移到云的过程。在 AWS 上构建云基础设施时，您可以使用自带许可（BYOL）功能节省成本，即，将现有的许可证清单重新用于云资源。通过基于规则的许可证消耗控制，管理员可以对新的和现有的云部署设置硬限制或软限制，在发生不合规的服务器之前停止使用它。

有关 License Manager 的更多信息，请参阅 License Manager 指南。

通过将 License Manager 链接到 AWS Organizations，您可以：

- 在整个组织中启用计算资源的跨账户发现。
- 查看和管理您拥有并在 AWS 上运行的商用 Linux 订阅。有关更多信息，请参阅 AWS License Manager 中的 Linux 订阅。

以下信息可帮助您将 AWS License Manager 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

当您启用信任访问权限后，您组织的管理账户中会自动创建以下服务相关角色。这些角色允许 License Manager 在您组织中的组织账户内执行支持的操作。

只有在禁用 License Manager 和 Organizations 之间的信任访问权限，或者您从组织中删除成员账户时，您才能删除或修改这些角色。

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

有关更多信息，请参阅 License Manager – 管理账户角色、License Manager – 成员账户角色和 License Manager – Linux 订阅角色。

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。License Manager 使用的服务相关角色为以下服务委托人授予访问权限：

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

使用 License Manager 启用信任访问权限

您只能使用 AWS License Manager 启用信任访问权限。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

使用 License Manager 启用信任访问权限

您必须使用 AWS Organizations 管理账户登录 License Manager，并将其与您的 License Manager 账户相关联。有关更多信息，请参阅 AWS License Manager 中的设置。

使用 License Manager 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用信任访问权限。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS License Manager 作为 Organizations 的信任服务。

```
$ aws organizations disable-aws-service-access \
    --service-principal license-manager.amazonaws.com
```

  如果成功，此命令不会产生任何输出。

  要禁用 Linux 订阅的信任访问权限，请执行以下操作：

```
$  aws organizations disable-aws-service-access \
    --service-principal license-manager-linux-subscriptions.amazonaws.com
```

- AWS API：DisableAWSServiceAccess

为 License Manager 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 License Manager 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 License Manager 的管理分开。

要将成员账户委托为 License Manager 的管理员，请按照《License Manager 用户指南》中注册委托管理员内的步骤操作。

Amazon Macie 和 AWS Organizations

Amazon Macie 是一个完全托管式数据安全和数据隐私服务，它使用机器学习和模式匹配来发现、监控并帮助您保护 Amazon Simple Storage Service（Amazon S3）中的敏感数据。Macie 自动发现敏感数据（例如个人可识别信息（PII）和知识产权），让您更好地了解组织在 Amazon S3 中存储的数据。

有关更多信息，请参阅《Amazon Macie 用户指南》中的使用 AWS Organizations 管理多个 Amazon Macie 账户。

使用以下信息可帮助您将 Amazon Macie 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

在启用可信访问权限时，系统自动在组织的委托 Macie 管理员账户中创建以下服务相关角色。此角色将允许 Macie 为您组织中的账户执行支持的操作。

只有在禁用 Macie 和 Organizations 之间的可信访问权限，或者您将该成员账户从组织中删除时，才能删除此角色。

- `AWSServiceRoleRorAmazonMacie`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Macie 使用的服务相关角色为以下服务委托人授予访问权限：

- `macie.amazonaws.com`

使用 Macie 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 Amazon Macie 控制台或 AWS Organizations 控制台启用信任访问权限。

> **Important**
>
> 强烈建议您尽可能使用 Amazon Macie 控制台或工具来实现与 Organizations 的集成。这可让 Amazon Macie 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon Macie 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 Amazon Macie 控制台或工具启用信任访问权限，则您无需完成这些步骤。

要使用 Macie 控制台启用信任访问权限，请执行以下操作：

在将委托成员账户作为组织的 Macie 管理员之前，Amazon Macie 需要对 AWS Organizations 的信任访问权限。如果您使用 Macie 管理控制台配置委托管理员，Macie 会自动为您启用信任访问权限。

有关更多信息，请参阅《Amazon Macie 用户指南》中的在 Amazon Macie 中集成和配置组织。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来启用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 Amazon Macie 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal macie.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：EnableAWSServiceAccess

为 Macie 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 Macie 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 Macie 的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中具有以下权限的用户或角色才能将成员账户配置为组织中 Macie 的委托管理员：
>
> - `organizations:EnableAWSServiceAccess`
> - `macie:EnableOrganizationAdminAccount`

指定一个成员账户作为 Macie 的委托管理员

在将委托成员账户作为组织的 Macie 管理员之前，Amazon Macie 需要对 AWS Organizations 的信任访问权限。如果您使用 Macie 管理控制台配置委托管理员，Macie 会自动为您启用信任访问权限。

有关更多信息，请参阅 https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin

AWS Marketplace 和 AWS Organizations

AWS Marketplace 是一个精挑细选的数字化产品目录，您通过它可以轻松地查找、购买、部署和管理构建解决方案及运营业务所需的第三方软件、数据和服务。

AWS Marketplace 使用您在 AWS Marketplace 中购买的 AWS License Manager 创建和管理许可证。当您与组织中的其他账户共享（授予访问权限）您的许可证时，AWS Marketplace 创建和管理这些账户的新许可证。

有关更多信息，请参阅《AWS Marketplace 买家指南》中的 AWS Marketplace 的服务相关角色。

以下信息可帮助您将 AWS Marketplace 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 AWS Marketplace 在您组织中的组织账户内执行支持的操作。

只有在禁用 AWS Marketplace 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForMarketplaceLicenseManagement`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。AWS Marketplace 使用的服务相关角色为以下服务委托人授予访问权限：

- `license-management.marketplace.amazonaws.com`

使用 AWS Marketplace 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 AWS Marketplace 控制台或 AWS Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 AWS Marketplace 控制台或工具来实现与 Organizations 的集成。这可让 AWS Marketplace 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 AWS Marketplace 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。如果您使用 AWS Marketplace 控制台或工具启用信任访问权限，则您无需完成这些步骤。

使用 AWS Marketplace 控制台启用可信访问权限

请参阅《AWS Marketplace 买家指南》中的为 AWS Marketplace 创建服务相关角色。

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。

2. 在 Services (服务) 页面上，找到 AWS Marketplace 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Marketplace 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS Marketplace 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：EnableAWSServiceAccess

使用 AWS Marketplace 禁用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Organizations 工具启用信任访问权限。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

您可以运行以下命令以禁用 AWS Marketplace 作为 Organizations 的信任服务。

```
$ aws organizations disable-aws-service-access \
    --service-principal license-management.marketplace.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- AWS API：DisableAWSServiceAccess

AWS Marketplace 私有市场 AWS Organizations

AWS Marketplace 是一个精心策划的数字目录，可用于查找、购买、部署和管理构建解决方案和运营业务所需的第三方软件、数据和服务。私人市场为您提供广泛的可用产品目录 AWS Marketplace，以及对这些产品的精细控制。

AWS Marketplace Private Marketplace 使您能够创建多个私有市场体验，这些体验与您的整个组织、一个或多个 OU 或组织中的一个或多个账户相关联，每个账户都有自己的一套经批准的产品。您的 AWS 管理员还可以通过公司或团队的徽标、消息和配色方案将公司品牌应用于每一次私人市场体验。

有关更多信息，请参阅《AWS Marketplace 买家指南》 AWS Marketplace中的使用角色配置私有市场。

使用以下信息来帮助您将P AWS Marketplace rivate Marketplace与集成 AWS Organizations。

启用集成时，创建了一个服务相关角色

当您使用 P AWS Marketplace rivate Marketplace 控制台启用可信访问时，将在您组织的管理账户中自动创建以下服务相关角色。此角色允许 Private Marketplace 在组织中的账户中执行支持的操作。只有在您禁用 Private Marketplace 和 Organization AWS Marketplace s 之间的可信访问权限并取消组织中所有私有市场体验的关联后，您才能删除或修改此角色。

如果您直接从 Organizations 控制台、CLI 或 SDK 启用可信访问，则不会自动创建服务相关角色。

- `AWSServiceRoleForPrivateMarketplaceAdmin`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Private Marketplace 使用的服务相关角色向以下服务主体授予访问权限：

- `private-marketplace.marketplace.amazonaws.com`

通过 Private Marketplace 启用

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 P AWS Marketplace rivate Marketplace 控制台或控制台启用可信访问。 AWS Organizations

> **Important**
>
> 我们强烈建议您尽可能使用 P AWS Marketplace rivate Marketplace 控制台或工具来启用与 Organizations 的集成。这允许 P AWS Marketplace rivate Marketplace 执行其所需的任何配置，例如创建服务所需的资源。只有当你无法使用P AWS Marketplace rivate Marketplace提供的工具启用集成时，才能继续执行这些步骤。有关更多信息，请参阅此说明。
> 如果您使用 P AWS Marketplace rivate Marketplace 控制台或工具启用可信访问，则无需完成这些步骤。

使用 Private Marketplace 控制台启用可信访问

请参阅《AWS Marketplace 买家指南》中的 Private Marketplace 入门。

您可以使用 AWS Organizations 控制台、运行 AWS CLI 命令或在其中一个 AWS SDK 中调用 API 操作来启用可信访问。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 “服务” 页面上，找到 “P AWS Marketplace rivate Marketplace” 行，选择服务的名称，然后选择 “启用可信访问”。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 Private Marketplace 的管理员 AWS Organizations，请告诉 P AWS Marketplace rivate Marketplace 的管理员，他们现在可以使用其控制台启用该服务 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来启用可信服务访问：

- AWS CLI: enable-aws-service-access

  您可以运行以下命令将 P AWS Marketplace rivate Marketplace 启用为 Organizations 的可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：启用 AWSServiceAccess

使用 Private Marketplace 禁

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以仅使用 Organizations 工具禁用信任访问权限。

您可以通过运行 Organizations AWS CLI 命令或在其中一个 AWS 软件开发工具包中调用 Organizations API 操作来禁用可信访问。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来禁用可信服务访问权限：

- AWS CLI: disable-aws-service-access

  你可以运行以下命令来禁用 AWS Marketplace Private Marketplace 作为 Organizations 的可信服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- AWS API：禁用 AWSServiceAccess

为 Private Marketplace 启用委托管理员账户

管理账户管理员可以将 Private Marketplace 的管理权限委托给被称为委托管理员的指定成员账户。要将账户注册为私有市场的委托管理员，管理账户管理员必须确保启用可信访问权限和服务相关角色，选择注册新管理员，提供 12 位 AWS 账号，然后选择提交。

管理账户和委托管理员账户可以执行 Private Marketplace 管理任务，例如创建体验、更新品牌设置、关联或取消关联受众、添加或删除产品以及批准或拒绝待处理的请求。

要使用 Private Marketplace 控制台配置委托管理员，请参阅《AWS Marketplace 买家指南》中的创建和管理私有市场。

您还可以使用 Organizations `RegisterDelegatedAdministrator` API 配置委托管理员。有关更多信息，请参阅 Organizati ons 命令参考 RegisterDelegatedAdministrator中的。

为私有市场 Private Marketplace

只有组织管理账户中的管理员才能为 Private Marketplace 配置委托管理员。

您可以使用 Private Marketplace 控制台或 API，也可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作来移除委托的管理员。

要使用 Private Marketplace 控制台禁用委托管理员私有市场账户，请参阅《AWS Marketplace 买家指南》中的创建和管理私有市场

AWS 网络管理员和 AWS Organizations

Network Manager 使您能够跨 AWS 账户、区域和本地位置集中管理您的 AWS Cloud WAN 核心网络和 T AWS ransit Gateway 网络。借助多账户支持，您可以为任何账户 AWS 创建单个全球网络，并使用 Network Manager 控制台将多个账户的传输网关注册到全球网络。

在 Network Manager 和 Organizations 之间启用可信访问权限后，注册的委托管理员和管理账户可以利用成员账户中部署的服务相关角色，从而描述附加到该全球网络的资源。在 Network Manager 控制台中，注册的委托管理员和管理账户可以代入成员账户中部署的以下自定义 IAM 角色：`CloudWatch-CrossAccountSharingRole`（用于多账户监控和事件通知）和 `IAMRoleForAWSNetworkManagerCrossAccountResourceAccess`（用于查看和管理多账户资源的控制台切换角色访问权限）

> **Important**
>
> - 我们强烈建议使用 Network Manager 控制台来管理多账户设置（启用/禁用可信访问权限以及注册/取消注册委托管理员）。从控制台管理这些设置时，系统会自动将所有必需的服务相关角色和自定义 IAM 角色部署到多账户访问所需的成员账户，并进行相应的管理。
> - 当您在网络管理器控制台中为网络管理器启用可信访问时，控制台还会启用 AWS CloudFormation StackSets 服务。Network Manager 用于 StackSets 部署多账户管理所需的自定义 IAM 角色。

有关将 Network Manager 与 Organizations 集成的更多信息，请参阅《Amazon VPC 用户指南》中的在 Network Manager 中使用 AWS Organizations管理多个账户。

使用以下信息来帮助您将 AWS 网络管理器与集成 AWS Organizations。

启用集成时，创建了一个服务相关角色

启用可信访问权限时，系统将自动在所列组织账户中创建以下服务相关角色。借助这些角色，Network Manager 将能够在组织中的账户内执行支持的操作。如果禁用可信访问权限，Network Manager 将不会从组织中的账户内删除这些角色。您可以使用 IAM 控制台将其手动删除。

管理账户

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`
- `AWSServiceRoleForCloudWatchCrossAccount`

成员账户

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgMember`

将某个成员账户注册为委托管理员时，系统将在该委托管理员账户中自动创建以下附加角色：

- `AWSServiceRoleForCloudWatchCrossAccount`

服务相关角色使用的服务委托人

服务相关角色只能由为该角色定义的信任关系授权的服务主体代入。

- 对于 AWSServiceRoleForNetworkManager service-linked 角色，唯一拥有访问权限的服务主体是 networkmanager.amazonaws.com。
- 对于 AWSServiceRoleForCloudFormationStackSetsOrgMember 服务相关角色，唯一拥有访问权限的服务主体是 member.org.stacksets.cloudformation.amazonaws.com。
- 对于 AWSServiceRoleForCloudFormationStackSetsOrgAdmin 服务相关角色，唯一拥有访问权限的服务主体是 stacksets.cloudformation.amazonaws.com。
- 对于 AWSServiceRoleForCloudWatchCrossAccount 服务相关角色，唯一拥有访问权限的服务主体是 cloudwatch-crossaccount.amazonaws.com。

如果删除这些角色，则将影响 Network Manager 的多账户功能。

使用 Network Manager 启用可信访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

只有 Organizations 管理账户中的管理员才有权启用对其他 AWS 服务的可信访问。务必要使用 Network Manager 控制台启用可信访问权限，以免出现权限问题。有关更多信息，请参阅《Amazon VPC 用户指南》中的在 Network Manager 中使用 AWS Organizations管理多个账户。

使用 Network Manager 禁用可信访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Organizations 管理账户中的管理员才有权禁用其他 AWS 服务的可信访问权限。

> **Important**
>
> 我们强烈建议您使用 Network Manager 控制台禁用可信访问权限。如果您以任何其他方式（例如使用 AWS CLI API 或 AWS CloudFormation 控制台）禁用可信访问，则可能无法正确清理已部署 AWS CloudFormation StackSets 和自定义 IAM 角色。要禁用可信服务访问权限，请登录 Network Manager 控制台。

为 Network Manager 启用委托管理员账户

将成员账户指定为组织的委托管理员后，该账户中的用户和角色将能够对 Network Manager 执行本来只能由组织管理账户中的用户或角色执行的管理操作。这有利于将组织的管理与 Network Manager 的管理分开。

有关如何将成员账户指定为组织中的 Network Manager 委托管理员的说明，请参阅《Amazon VPC 用户指南》中的注册委托管理员。

亚马逊 Q 开发者（亚马逊 Q）和 AWS Organizations

Amazon Q Developer 是一款生成式人工智能 (AI) 驱动的对话助手，可以帮助您理解、构建、扩展和操作 AWS 应用程序。Amazon Q 的付费订阅版本需要整合 Organizations。有关更多信息，请参阅 Amazon Q 用户指南中的账户、IAM 身份中心和组织设置。

使用以下信息来帮助您集成 Amazon Q Developer AWS Organizations。

服务相关角色

`AWSServiceRoleForAmazonQDeveloper`服务相关角色允许 Amazon Q 在组织中的账户中执行支持的操作。按照 IAM 用户指南中的创建服务相关角色中所述，使用 Amazon Q 控制台、API 或 CLI 创建角色。

只有在禁用 Amazon Q 和 Organizations 之间的可信访问权限或从组织中删除成员账户后，才能删除或修改此角色。

Amazon Q 使用的服务主体

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Amazon Q 使用的服务相关角色向以下服务主体授予访问权限：

- `q.amazonaws.com`

通过 Amazon Q 启用可信访问

Amazon Q 使用可信访问权限与成员账户共享在组织级别所做的设置。例如，Organizations 级别的管理员可以启用功能 X，然后同一组织的所有成员帐户都可以使用功能 X。有关更多信息，请参阅 Amazon Q 开发者用户指南中的设置组织。

您只能使用 Amazon Q Developer 启用可信访问。

要激活 Amazon Q 的可信访问权限，请在 Amazon Q 控制台中按照 Amazon Q 开发者用户指南订阅中的说明进行操作。在步骤 6 中，选择 “与成员帐户共享设置配置文件”。

使用 Amazon Q 禁用可信访问

您只能使用 Amazon Q 开发者工具禁用可信访问。

要停用 Amazon Q 的可信访问权限，请在 Amazon Q 控制台中按照 A mazon Q 开发者用户指南中的订阅中的说明进行操作。在步骤 6 中，取消选择 “与成员帐户共享设置个人资料”。

AWS Resource Access Manager 和 AWS Organizations

AWS Resource Access Manager（AWS RAM）可让您与其他AWS 账户共享您指定的AWS资源。这是一种集中式服务，跨多个账户为共享不同类型的 AWS 资源提供一致的体验。

有关 AWS RAM 的更多信息，请参阅 AWS RAM 用户指南。

以下信息可帮助您将 AWS Resource Access Manager 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 AWS RAM 在您组织中的组织账户内执行支持的操作。

只有在禁用 AWS RAM 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForResourceAccessManager`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。AWS RAM 使用的服务相关角色为以下服务委托人授予访问权限：

- `ram.amazonaws.com`

使用 AWS RAM 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 AWS Resource Access Manager 控制台或 AWS Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 AWS Resource Access Manager 控制台或工具来实现与 Organizations 的集成。这可让 AWS Resource Access Manager 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 AWS Resource Access Manager 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 AWS Resource Access Manager 控制台或工具启用信任访问权限，则您无需完成这些步骤。

使用 AWS RAM 控制台或 CLI 启用信任访问权限

请参阅《AWS RAM 用户指南》中的允许与 AWS Organizations 共享。

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS Resource Access Manager 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Resource Access Manager 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS Resource Access Manager 作为 Organizations 的信任服务。

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

如果成功，此命令不会产生任何输出。

- AWS API：EnableAWSServiceAccess

使用 AWS RAM 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您可以使用 AWS Resource Access Manager 或者 AWS Organizations 工具禁用信任访问权限。

> **Important**
>
> 强烈建议您尽可能使用 AWS Resource Access Manager 控制台或工具来禁用与 Organizations 的集成。这可让 AWS Resource Access Manager 执行所需的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 AWS Resource Access Manager 提供的工具禁用集成时，才会使用这些步骤进行处理。
> 如果您使用 AWS Resource Access Manager 控制台或工具禁用信任访问权限，则您无需完成这些步骤。

使用 AWS Resource Access Manager 控制台或 CLI 禁用信任访问权限

请参阅《AWS RAM 用户指南》中的允许与 AWS Organizations 共享。

您可以使用AWS Organizations控制台，通过运行 Organizations AWS CLI 命令，或者通过调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 AWS Resource Access Manager 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。

4. 在确认对话框中输入 **disable**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Resource Access Manager 的管理员，他们现在可以使用其控制台或工具禁用该服务，使其无法处理 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS Resource Access Manager 作为 Organizations 的信任服务。

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

  如果成功，此命令不会产生任何输出。
- AWS API：DisableAWSServiceAccess

AWS 资源探索器 和 AWS Organizations

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

当您将资源管理器与 AWS Organizations 集成后，可以从更广泛的来源收集证据，方法是在评估范围内添加组织中的多个 AWS 账户。

以下信息可帮助您将 AWS 资源探索器 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许资源管理器在您组织中的组织账户内执行支持的操作。

只有在禁用资源管理器和 Organizations 之间的信任访问权限时，或者如果您从组织中删除成员账户，才能删除或修改此角色。

有关资源管理器如何使用此角色的详细信息，请参阅《AWS 资源探索器 用户指南》中的使用服务相关角色。

- `AWSServiceRoleForResourceExplorer`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。资源管理器使用的服务相关角色将为以下服务主体授予访问权限：

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

使用 AWS 资源探索器 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

在将成员账户委托为组织的委托管理员之前，资源管理器需要对 AWS Organizations 的信任访问权限。

您可以使用资源管理器控制台或 Organizations 控制台启用信任访问权限。强烈建议您尽可能使用资源管理器控制台或工具来实现与 Organizations 的集成。这可让 AWS 资源探索器 执行所需的任何配置，例如创建服务所需的资源。

使用资源管理器控制台启用可信访问权限

有关启用可信访问权限的说明，请参阅《AWS 资源探索器 用户指南》中的使用资源管理器的先决条件。

> **Note**
>
> 如果您使用 AWS 资源探索器 控制台配置委托管理员，AWS 资源探索器 会自动为您启用信任访问权限。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来启用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS 资源探索器 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：EnableAWSServiceAccess

使用资源管理器禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 AWS Organizations 管理账户中的管理员可以禁用对 AWS 资源探索器 的信任访问权限。

您可以使用 AWS 资源探索器 或者 AWS Organizations 工具禁用信任访问权限。

> **Important**
>
> 强烈建议您尽可能使用 AWS 资源探索器 控制台或工具来禁用与 Organizations 的集成。这可让 AWS 资源探索器 执行所需的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 AWS 资源探索器 提供的工具禁用集成时，才会使用这些步骤进行处理。
> 如果您使用 AWS 资源探索器 控制台或工具禁用信任访问权限，则您无需完成这些步骤。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS 资源探索器 作为 Organizations 的信任服务。

```
$ aws organizations disable-aws-service-access \
    --service-principal resource-explorer-2.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- AWS API：DisableAWSServiceAccess

为资源管理器启用委托管理员账户

使用您的委托管理员账户创建多账户资源视图，并将其范围限定为一个组织单位或整个组织。通过创建资源共享，您可以通过 AWS Resource Access Manager 与组织中的任何账户共享多账户视图。

> **最小权限**
>
> 只有 Organizations 管理账户中具有以下权限的用户或角色才能将成员账户配置为组织中资源管理器的委托管理员：
> `resource-explorer:RegisterAccount`

有关为资源管理器启用委托管理员账户的说明，请参阅《AWS 资源探索器 用户指南》中的设置。

如果您使用 AWS 资源探索器 控制台配置委托管理员，资源管理器会自动为您启用信任访问权限。

AWS CLI, AWS API

如果要使用 AWS CLI 或某个 AWS SDK 配置委托管理员账户，您可以使用以下命令：

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务 `resource-explorer-2.amazonaws.com` 确定为参数。

为资源管理器禁用委托管理员

只有 Organizations 管理账户中或资源管理器委托管理员账户中的管理员才能删除资源管理器的委托管理员。您可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作禁用信任访问权限。

AWS Security Hub 和 AWS Organizations

AWS Security Hub 为您提供安全状态的全面视图， AWS 并帮助您根据安全行业标准和最佳实践检查您的环境。

Security Hub 从您的 AWS 账户、您使用的 AWS 服务和支持的第三方合作伙伴产品中收集安全数据。它可以帮助您分析安全趋势并确定最高优先级的安全问题。

当你同时使用 Security Hub 时，你可以自动为所有账户启用 Security Hub，包括在添加新账户时为其启用 Security Hub。 AWS Organizations 这扩大了 Security Hub 检查和调查结果的覆盖范围，从而可让您更全面且准确地了解您的整体安全状况。

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

使用以下信息来帮助您集 AWS Security Hub 成 AWS Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Security Hub 在您组织中的组织账户内执行支持的操作。

只有在禁用 Security Hub 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForSecurityHub`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Security Hub 使用的服务相关角色为以下服务委托人授予访问权限：

- `securityhub.amazonaws.com`

使用 Security Hub 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

当您为 Security Hub 指定委托管理员时，Security Hub 会自动为组织中的 Security Hub 启用信任访问权限。

为 Security Hub 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 Security Hub 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 Security Hub 的管理分开。

想要了解有关信息，请参阅《AWS Security Hub 用户指南》中的指定 Security Hub 管理员账户。

指定一个成员账户作为 Security Hub 的委托管理员

1. 使用您的 Organizations 管理账户登录。
2. 执行下列操作之一：
   - 如果您的管理账户未启用 Security Hub，则在 Security Hub 控制台上，选择 Go to Security Hub (转到 Security Hub)。
   - 如果您的管理账户确实启用了 Security Hub，则在 Security Hub 控制台上，在 “常规” 下选择 “设置”。
3. 在 Delegated Administrator (委托管理员) 中，输入账户 ID。

Amazon S3 Storage Lens 和 AWS Organizations

通过向您的组织授予 Amazon S3 Storage Lens 可信访问权限，即允许其收集和汇总组织 AWS 账户内所有部门的指标。S3 Storage Lens 通过访问属于您组织的账户列表来实现此目的，并收集和分析所有账户的存储和使用情况以及活动指标。

有关更多信息，请参阅《Amazon S3 Storage Lens 用户指南》中的将服务相关角色用于 Amazon S3 Storage Lens。

使用以下信息来帮助您将 Amazon S3 存储镜头与集成 AWS Organizations。

启用集成时，创建了一个服务相关角色

在启用可信访问权限且 Storage Lens 配置已应用到您的企业时，系统自动在您企业的委托管理员账户中创建以下服务相关角色。此角色允许 Amazon S3 Storage Lens 在您组织中的组织账户内执行支持的操作。

只有在禁用 Amazon S3 Storage Lens 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForS3StorageLens`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Amazon S3 Storage Lens 使用的服务相关角色为以下服务委托人授予访问权限：

- `storage-lens.s3.amazonaws.com`

为 Amazon S3 Storage Lens 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 Amazon S3 Storage Lens 控制台或 AWS Organizations 控制台启用信任访问权限。

> **Important**
>
> 强烈建议您尽可能使用 Amazon S3 Storage Lens 控制台或工具来实现与 Organizations 的集成。这可让 Amazon S3 Storage Lens 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon S3 Storage Lens 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
>
> 如果您使用 Amazon S3 Storage Lens 控制台或工具启用信任访问权限，则您无需完成这些步骤。

使用 Amazon S3 控制台启用信任访问权限

请参阅《Amazon 简单存储服务用户指南》中的 “为 S3 存储镜头启用可信访问”。

您可以使用 AWS Organizations 控制台、运行 AWS CLI 命令或在其中一个 AWS SDK 中调用 API 操作来启用可信访问。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 Amazon S3 Storage Lens 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您仅是的管理员 AWS Organizations，请告诉 Amazon S3 Storage Lens 的管理员，他们现在可以使用其控制台启用该服务 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来启用可信服务访问：

- AWS CLI: enable-aws-service-access

  您可以运行以下命令以启用 Amazon S3 Storage Lens 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal storage-lens.s3.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：启用 AWSServiceAccess

为 Amazon S3 Storage Lens 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Amazon S3 Storage Lens 工具来禁用信任访问权限。

您可以使用 Amazon S3 控制台、 AWS CLI 或任何 AWS 软件开发工具包禁用可信访问。

使用 Amazon S3 控制台禁用信任访问权限

请参阅《Amazon 简单存储服务用户指南》中的 “禁用 S3 存储镜头的可信访问”。

为 Amazon S3 Storage Lens 启用委托管理员账户。

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 Amazon S3 Storage Lens 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 Amazon S3 Storage Lens 的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中具有以下权限的用户或角色才能将成员账户配置为组织中 Amazon S3 Storage Lens 存储统计管理工具的委托管理员：
> `organizations:RegisterDelegatedAdministrator`
> `organizations:DeregisterDelegatedAdministrator`

Amazon S3 Storage Lens 在您的组织中最多支持 5 个委托管理员账户。

指定一个成员账户作为 Amazon S3 Storage Lens 的委托管理员

您可以使用 Amazon S3 控制台、 AWS CLI 或任何 AWS 软件开发工具包注册委托管理员。要使用 Amazon S3 控制台将成员账户注册为贵组织的委托管理员账户，请参阅《亚马逊简单存储服务用户指南》中的注册 S3 Storage Lens 的委托管理员。

为 Amazon S3 Storage Lens 取消注册委托管理员

您可以使用 Amazon S3 控制台、 AWS CLI 或任何 AWS 软件开发工具包取消注册委托管理员。要使用 Amazon S3 控制台取消注册委托管理员，请参阅《亚马逊简单存储服务用户指南》中的注销 S3 Storage Lens 的委托管理员。

Amazon Security Lake 和 AWS Organizations

Amazon Security Lake 将来自云端、本地和自定义源的安全数据集中到存储在您的账户的数据湖中。通过与 Organizations 集成，您可以创建一个数据湖来收集账户中的日志和事件。有关更多信息，请参阅《Amazon Security Lake 用户指南》中的使用 AWS Organizations管理多个账户。

使用以下信息来帮助您将 Amazon Security Lake 与集成 AWS Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Amazon Security Lake 在贵组织中的账户中执行支持的操作。

只有在禁用 Amazon Security Lake 和 Organizations 之间的可信访问权限或从组织中删除成员账户后，才能删除或修改此角色。

- `AWSServiceRoleForSecurityLake`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Amazon Security Lake 使用的服务相关角色向以下服务主体授予访问权限：

- `securitylake.amazonaws.com`

通过 Amazon 安全湖启用可信访问

当您授予对安全数据湖的信任访问权限时，安全数据湖可以自动应对组织成员资格的更改。委派的管理员可以在任何组织账户中启用从支持的服务收集 AWS 日志。有关更多信息，请参阅《Amazon Security Lake 用户指南》中的亚马逊安全数据湖的服务相关角色。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Organizations 工具启用信任访问权限。

您可以使用 AWS Organizations 控制台、运行 AWS CLI 命令或在其中一个 AWS SDK 中调用 API 操作来启用可信访问。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 Amazon Security Lake（亚马逊安全数据湖）行，选择该服务的名称，然后选择 Enable trusted access（启用信任访问权限）。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您仅是的管理员 AWS Organizations，请告诉 Amazon Security Lake 的管理员，他们现在可以使用其控制台启用该服务 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来启用可信服务访问：

- AWS CLI: enable-aws-service-access

  您可以运行以下命令以使用 Organizations 启用 Amazon Security Lake 作为信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- AWS API：启用 AWSServiceAccess

使用 Amazon 安全湖禁用可信访问

只有组织管理账户中的管理员才能禁用 Amazon Security Lake 的可信访问权限。

您可以仅使用 Organizations 工具禁用信任访问权限。

您可以使用 AWS Organizations 控制台、运行 Organizations AWS CLI 命令或在其中一个 AWS 软件开发工具包中调用 Organizations API 操作来禁用可信访问。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 Amazon Security Lake（亚马逊安全数据湖）行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **`disable`**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您仅是的管理员 AWS Organizations，请告诉 Amazon Security Lake 的管理员，他们现在可以使用该服务的控制台或工具禁用该服务 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作来禁用可信服务访问权限：

- AWS CLI: disable-aws-service-access

  您可以运行以下命令以使用 Organizations 禁用 Amazon Security Lake 作为信任服务。

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

  如果成功，此命令不会产生任何输出。
- AWS API：禁用 AWSServiceAccess

为 Amazon Security Lake 启用委托管理员账户

Amazon Security Lake 授权管理员将组织中的其他账户添加为成员账户。授权的管理员可以启用亚马逊安全湖并为成员账户配置亚马逊安全湖设置。委派的管理员可以在启用了 Amazon Security Lake 的所有 AWS 区域（无论您当前使用的是哪个区域终端节点）收集整个组织的日志。

您还可以将委托管理员设置为自动将组织中的新帐户添加为成员。Amazon Security Lake 授权的管理员可以访问关联成员账户中的日志和事件。因此，您可以设置 Amazon Security Lake 来收集关联成员账户拥有的数据。您还可以授予订阅用户使用关联成员账户所拥有数据的权限。

有关更多信息，请参阅《Amazon Security Lake 用户指南》中的使用 AWS Organizations管理多个账户。

> 最小权限
>
> 只有 Organizations 管理账户中的管理员才能将成员账户配置为组织中 Amazon Security Lake 的委托管理员

您可以使用 Amazon Security Lake 控制台、Amazon Security Lake `CreateDatalakeDelegatedAdmin` API 操作或 `create-datalake-delegated-admin` CLI 命令来指定委托管理员账户。或者，您也可以使用 Organizations `RegisterDelegatedAdministrator` CLI 或 SDK 操作。有关为 Amazon Security Lake 启用委托管理员账户的说明，请参阅 Amazon Security Lake 用户指南中的指定委派安全湖管理员和添加成员账户。

AWS CLI, AWS API

如果要使用 AWS CLI 或其中一个 AWS SDK 配置委派管理员帐户，则可以使用以下命令：

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \ --service-principal securitylake.amazonaws.com
```

- AWS SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务委托人标识`account.amazonaws.com`为参数。

禁用 Amazon 安全湖的委托管理员

只有 Organizations 管理账户或 Amazon Security Lake 委托管理员账户中的管理员才能从组织中删除委托管理员账户。

您可以使用 Amazon Security `delete-datalake-delegated-admin` Lake `DeleteDatalakeDelegatedAdmin` API 操作、CLI 命令或使用 Organizations CL `DeregisterDelegatedAdministrator` l 或 SDK 操作来删除委派的管理员账户。要使用 Amazon Security Lake 移除委托管理员，请参阅亚马逊安全湖用户指南中的移除亚马逊安全湖委托管理员。

AWS Service Catalog 和 AWS Organizations

借助 Service Catalog，您可以创建和管理获准在 AWS 上使用的 IT 服务的目录。

通过将 Service Catalog 与 AWS Organizations 集成，简化了在整个组织共享产品组合和复制产品的过程。Service Catalog 管理员可以在共享产品组合时引用 AWS Organizations 中现有的组织，并且可以与组织树结构中的任何可信组织部门（OU）共享该产品组合。这样就不再需要共享产品组合，并且在导入产品组合时不再需要接收账户手动引用产品组合 ID。在 Service Catalog 中，通过此机制共享的产品组合将管理员的 Imported Portfolio（导入的产品组合）视图的共享目标账户中列出。

有关 Service Catalog 的更多信息，请参阅 服务目录管理员指南。

以下信息可帮助您将 AWS Service Catalog 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

AWS Service Catalog 不会创建任何服务相关角色作为启用信任访问权限的一部分。

用于授予权限的服务委托人

要启用信任访问权限，您必须指定以下服务委托人：

- `servicecatalog.amazonaws.com`

使用 Service Catalog 启用可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 AWS Service Catalog 控制台或 AWS Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 AWS Service Catalog 控制台或工具来实现与 Organizations 的集成。这可让 AWS Service Catalog 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 AWS Service Catalog 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
>
> 如果您使用 AWS Service Catalog 控制台或工具启用信任访问权限，则您无需完成这些步骤。

使用 Service Catalog CLI 或 AWS SDK 启用可信访问

调用下列命令或操作之一：

- AWS CLI：aws servicecatalog enable-aws-organizations-access
- AWS SDK：AWSServiceCatalog::EnableAWSOrganizationsAccess

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS Service Catalog 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。

3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Service Catalog 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS Service Catalog 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：EnableAWSServiceAccess

使用 Service Catalog 禁用可信访问

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

如果您在使用 Service Catalog 时使用 AWS Organizations 禁用了可信访问，这将不会删除当前的共享，但会阻止您在整个组织中创建新的共享。如果在您调用此操作后当前共享发生更改，则它将不会与您的组织结构同步。

您可以使用 AWS Service Catalog 或者 AWS Organizations 工具禁用信任访问权限。

> **Important**
>
> 强烈建议您尽可能使用 AWS Service Catalog 控制台或工具来禁用与 Organizations 的集成。这可让 AWS Service Catalog 执行所需的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 AWS Service Catalog 提供的工具禁用集成时，才会使用这些步骤进行处理。
>
> 如果您使用 AWS Service Catalog 控制台或工具禁用信任访问权限，则您无需完成这些步骤。

使用 Service Catalog CLI 或 AWS SDK 禁用可信访问

调用下列命令或操作之一：

- AWS CLI：aws servicecatalog disable-aws-organizations-access
- AWS SDK：DisableAWSOrganizationsAccess

您可以使用AWS Organizations控制台，通过运行 Organizations AWS CLI 命令，或者通过调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 AWS Service Catalog 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **disable**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Service Catalog 的管理员，他们现在可以使用其控制台或工具禁用该服务，使其无法处理 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS Service Catalog 作为 Organizations 的信任服务。

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

  如果成功，此命令不会产生任何输出。
- AWS API：DisableAWSServiceAccess

Service Quotas 和 AWS Organizations

Service Quotas 是一项 AWS 服务，可让您从中心位置查看和管理您的配额。配额（也称为限制）是 AWS 账户中资源、操作和项目的最大值。

当 Service Quotas 与 AWS Organizations 关联时，您可以创建一个配额请求模板，以在创建账户时自动请求提升配额。

有关 Service Quotas 的更多信息，请参阅 Service Quotas 用户指南。

以下信息可帮助您将 Service Quotas 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Service Quotas 在您组织中的组织账户内执行支持的操作。

只有在禁用 Service Quotas 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForServiceQuotas`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Service Quotas 使用的服务相关角色为以下服务委托人授予访问权限：

- `servicequotas.amazonaws.com`

启用其他 Service Quotas 服务的信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Service Quotas 启用信任访问权限。

您可以使用服务限额控制台、AWS CLI 或 SDK 启用信任访问权限：

- 使用 Service Quotas 控制台启用信任访问权限

  使用您的 AWS Organizations 管理账户登录，然后在 Service Quotas 控制台上配置模板。有关更多信息，请参阅《Service Quotas 用户指南》中的使用 Service Quotas 模板。

- 使用 Service Quotas AWS CLI 或 SDK 启用信任访问权限

  调用以下命令或操作：

  - AWS CLI：aws service-quotas associate-service-quota-template
  - AWS SDK：AssociateServiceQuotaTemplate

AWS IAM Identity Center 和 AWS Organizations

AWS IAM Identity Center 为您的所有 AWS 账户 和云应用程序提供单一登录访问。它通过 AWS Directory Service 与 Microsoft Active Directory 连接，以允许该目录中的用户使用其现有 Active Directory 用户名和密码登录个性化 AWS 访问门户。从 AWS 访问门户，用户可以访问所有 AWS 账户以及他们拥有权限的云应用程序。

有关 IAM Identity Center 的更多信息，请参阅《AWS IAM Identity Center 用户指南》。

以下信息可帮助您将 AWS IAM Identity Center 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 IAM Identity Center 在您组织中的组织账户内执行支持的操作。

只有当在 IAM Identity Center 和 Organizations 之间禁用可信访问，或者从组织中删除成员账户时，您才能删除角色。

- `AWSServiceRoleForSSO`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。IAM Identity Center 使用的服务相关角色为以下服务主体授予访问权限：

- `sso.amazonaws.com`

对 IAM Identity Center 启用可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 AWS IAM Identity Center 控制台或 AWS Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 AWS IAM Identity Center 控制台或工具来实现与 Organizations 的集成。这可让 AWS IAM Identity Center 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 AWS IAM Identity Center 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 AWS IAM Identity Center 控制台或工具启用信任访问权限，则您无需完成这些步骤。

IAM Identity Center 需要对 AWS Organizations 的可信访问才能正常运行。在设置 IAM Identity Center 时启用可信访问。有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的入门 – 步骤 1：启用 AWS IAM Identity Center。

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS IAM Identity Center 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 AWS IAM Identity Center 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

您可以运行以下命令以启用 AWS IAM Identity Center 作为 Organizations 的信任服务。

```
$ aws organizations enable-aws-service-access \
    --service-principal sso.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- AWS API：EnableAWSServiceAccess

对 IAM Identity Center 禁用可信访问

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

IAM Identity Center 需要对 AWS Organizations 的可信访问才能正常工作。如果您在使用 IAM Identity Center 时使用 AWS Organizations 禁止可信访问，则它将不再正常运行，因为它无法访问组织。用户无法使用 IAM Identity Center 访问账户。IAM Identity Center 创建的所有角色均将保留，但 IAM Identity Center 服务无法访问这些角色。IAM Identity Center 服务相关角色将保留。如果您重新允许可信访问，则 IAM Identity Center 将继续像以前一样运行，而无需您重新配置该服务。

如果您删除组织中的某个账户，则 IAM Identity Center 将自动清除任何元数据和资源（例如，所删除账户的服务相关角色）。从组织中删除的独立账户将无法再与 IAM Identity Center 配合使用。

您可以仅使用 Organizations 工具禁用信任访问权限。

您可以使用AWS Organizations控制台，通过运行 Organizations AWS CLI 命令，或者通过调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 AWS IAM Identity Center 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **`disable`**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您只是 AWS Organizations 的管理员，请告诉 AWS IAM Identity Center 的管理员，他们现在可以使用其控制台或工具禁用该服务，使其无法处理 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS IAM Identity Center 作为 Organizations 的信任服务。

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

  如果成功，此命令不会产生任何输出。
- AWS API：DisableAWSServiceAccess

为 IAM Identity Center 启用委托管理员账户

将成员账户指定为组织的委托管理员后，该账户中的用户和角色将能够对 IAM Identity Center 执行本来只能由组织管理账户中的用户或角色执行的管理操作。这有利于将组织的管理与 IAM Identity Center 的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色能够将某个成员账户配置为组织的 IAM Identity Center 委托管理员。

有关如何为 IAM Identity Center 启用委托管理员账户的说明，请参阅《AWS IAM Identity Center 用户指南》中的委托管理。

AWS Systems Manager 和 AWS Organizations

AWS Systems Manager 是功能的集合，可以实现对 AWS 资源的可见性和控制。以下 Systems Manager 功能可跨您组织中的所有 AWS 账户 与 Organizations 配合工作：

- Systems Manager Explorer 是一个可自定义的操作控制面板，用于报告有关AWS资源的信息。您可以使用 Organizations 和 Systems Manager Explorer，跨组织里的所有AWS 账户同步操作数据。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的 Systems Manager Explorer。

- Systems Manager Change Manager 是一个企业变更管理框架，用于请求、批准、实施和报告应用程序配置和基础架构的操作变更。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的 AWS Systems Manager Change Manager。
- Systems Manager OpsCenter 提供了一个中心位置，运营工程师和 IT 专业人员可以在这里查看、调查和解决与 AWS 资源相关的运营工作项 (OpsItem)。当您将 OpsCenter 与 Organizations 配合使用时，它支持在单个会话期间从管理账户（组织管理账户或 Systems Manager 委托管理员账户）和另一个账户使用 OpsItem。配置后，用户可以执行以下类型的操作：
  - 在另一个账户中创建、查看和更新 OpsiTem。
  - 在另一个账户中查看有关在 OpsiTem 中指定的 AWS 资源的详细信息。
  - 启动 Systems Manager 自动化运行手册以修复其他账户中的 AWS 资源问题。

  有关更多信息，请参阅《AWS Systems Manager 用户指南》中的 AWS Systems Manager OpsCenter。

以下信息可帮助您将 AWS Systems Manager 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Systems Manager 在您组织中的组织账户内执行支持的操作。

只有在禁用 Systems Manager 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Systems Manager 使用的服务相关角色为以下服务委托人授予访问权限：

- `ssm.amazonaws.com`

使用 Systems Manager 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Organizations 工具启用信任访问权限。

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS Systems Manager 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Systems Manager 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS Systems Manager 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- AWS API：EnableAWSServiceAccess

使用 Systems Manager 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

Systems Manager 需要对 AWS Organizations 的信任访问权限才能在组织中跨AWS 账户同步操作数据。如果您禁用信任访问，则 Systems Manager 无法同步操作数据和报告错误。

您可以仅使用 Organizations 工具禁用信任访问权限。

您可以使用AWS Organizations控制台，通过运行 Organizations AWS CLI 命令，或者通过调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services（服务）页面上，找到 AWS Systems Manager 行，然后选择该服务的名称。
3. 选择 Disable trusted access (禁用信任访问权限)。
4. 在确认对话框中输入 **disable**，然后选择 Disable trusted access (禁用信任访问权限)。
5. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Systems Manager 的管理员，他们现在可以使用其控制台或工具禁用该服务，使其无法处理 AWS Organizations。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS Systems Manager 作为 Organizations 的信任服务。

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

  如果成功，此命令不会产生任何输出。

- AWS API：DisableAWSServiceAccess

为 Systems Manager 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 Systems Manager 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 Systems Manager 的管理分开。

如果跨组织使用 Change Manager，则使用委托管理员账户。这是已指定为账户的AWS 账户，用于在 Change Manager 中管理变更模板、变更请求、变更运行手册和审批工作流。委托账户管理整个组织的变更活动。当您设置您的组织以便使用 Change Manager 时，您要指定您的哪个账户在此角色中使用服务。它不必是组织的管理账户。如果您只对单个账户使用 Change Manager，则不需要委托管理员账户。

要将成员帐户指定为委托管理员，请参阅《AWS Systems Manager 用户指南》中的以下主题：

- 有关 Explorer 和 OpsCenter 的信息，请参阅配置委托管理员。
- 有关 Change Manager 的信息，请参阅为 Change Manager 设置组织和委托账户。

标签策略和 AWS Organizations

标签策略是 AWS Organizations 中策略的一种类型，可帮助您在组织账户中跨资源标准化标签。有关标签策略的更多信息，请参阅标签策略。

以下信息可帮助您将标签策略与 AWS Organizations 集成。

服务相关角色使用的服务委托人

Organizations 使用以下服务委托人与附加到资源的标签进行交互。

- `tagpolicies.tag.amazonaws.com`

为标签策略启用信任访问权限

您可以启用信任访问权限，方法是在组织中启用标签策略或使用 AWS Organizations 控制台。

> **Important**
>
> 强烈建议您通过启用标签策略来启用信任访问权限。这使 Organizations 能够执行必需的设置任务。

您可以为标签策略启用信任访问权限，方法是在 AWS Organizations 控制台中启用标签策略类型。有关更多信息，请参阅 启用策略类型。

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 tag policies (标签策略) 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉标签策略的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用标签策略作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal tagpolicies.tag.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：EnableAWSServiceAccess

使用标记策略禁用信任访问权限

您可以为标签策略禁用信任访问权限，方法是在 AWS Organizations 控制台中禁用标签策略类型。有关更多信息，请参阅禁用策略类型。

AWS Trusted Advisor 和 AWS Organizations

AWS Trusted Advisor 可检查您的AWS环境，并在有可能节省开支、提高系统可用性和性能或弥补安全漏洞时为您提供建议。与 Organizations 集成后，您可以接收组织中所有账户的 Trusted Advisor 检查结果，并下载报告以查看检查结果和任何受影响资源的摘要。

有关更多信息，请参阅《AWS Support 用户指南》中的 AWS Trusted Advisor 的组织视图。

以下信息可帮助您将 AWS Trusted Advisor 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Trusted Advisor 在您组织中的组织账户内执行支持的操作。

只有在禁用 Trusted Advisor 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForTrustedAdvisorReporting`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Trusted Advisor 使用的服务相关角色为以下服务委托人授予访问权限：

- `reporting.trustedadvisor.amazonaws.com`

使用 Trusted Advisor 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 AWS Trusted Advisor 启用信任访问权限。

使用 Trusted Advisor 控制台启用可信访问权限

请参阅《AWS Support 用户指南》中的启用组织视图。

使用 Trusted Advisor 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

禁用此功能后，Trusted Advisor 停止记录您组织中所有其他账户的检查信息。您无法查看或下载现有报告或创建新报告。

您可以使用 AWS Trusted Advisor 或者 AWS Organizations 工具禁用信任访问权限。

> **Important**
>
> 强烈建议您尽可能使用 AWS Trusted Advisor 控制台或工具来禁用与 Organizations 的集成。这可让 AWS Trusted Advisor 执行所需的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 AWS Trusted Advisor 提供的工具禁用集成时，才会使用这些步骤进行处理。
>
> 如果您使用 AWS Trusted Advisor 控制台或工具禁用信任访问权限，则您无需完成这些步骤。

使用 Trusted Advisor 控制台禁用信任访问权限

请参阅《AWS Support 用户指南》中的禁用组织视图。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS Trusted Advisor 作为 Organizations 的信任服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- AWS API：DisableAWSServiceAccess

为 Trusted Advisor 启用委托管理员账户

当您将某个成员账户指定为组织的委托管理员时，来自指定账户的用户和角色将可以管理组织内其他成员账户的 AWS 账户元数据。如果您没有启用委托管理员账户，则这些任务只能由组织的管理账户执行。这有利于您将组织的管理与您的账户详细信息的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色才能将某个成员账户配置为组织的 Trusted Advisor 委托管理员。

有关如何为 Trusted Advisor 启用委托管理员账户的说明，请参阅 AWS Support 用户指南中的注册委托管理员。

AWS CLI, AWS API

如果要使用 AWS CLI 或某个 AWS SDK 配置委托管理员账户，您可以使用以下命令：

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

- AWS SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务主体 `account.amazonaws.com` 确定为参数。

为 Trusted Advisor 禁用委托管理员

您可以使用 Trusted Advisor 控制台或者通过使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作来删除委托管理员。有关如何使用 Trusted Advisor 控制台禁用委托管理员 Trusted Advisor 账户的信息，请参阅 AWS Support 用户指南中的取消注册委托管理员。

AWS Well-Architected Tool 和 AWS Organizations

AWS Well-Architected Tool 可帮助您记录工作负载的状态并将其与最新的 AWS 架构最佳做法进行比较。

将 AWS Well-Architected Tool 与 Organizations 结合使用让 AWS Well-Architected Tool 和 Organizations 客户能够简化与组织的其他成员共享 AWS Well-Architected Tool 资源的过程。

有关更多信息，请参阅 AWS Well-Architected Tool 用户指南中的共享您的 AWS Well-Architected Tool 资源。

以下信息可帮助您将 AWS Well-Architected Tool 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 AWS WA Tool 在您组织中的组织账户内执行支持的操作。

只有在禁用 AWS WA Tool 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForWellArchitected`

服务角色策略是 `AWSWellArchitectedOrganizationsServiceRolePolicy`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。AWS WA Tool 使用的服务相关角色为以下服务委托人授予访问权限：

- `wellarchitected.amazonaws.com`

使用 AWS WA Tool 启用信任访问权限

允许更新 AWS WA Tool 以反映组织中的层次变化。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 AWS Well-Architected Tool 控制台或 AWS Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 AWS Well-Architected Tool 控制台或工具来实现与 Organizations 的集成。这可让 AWS Well-Architected Tool 执行所需的任何配置，例如创建服务所需的资源。请

仅在您无法使用 AWS Well-Architected Tool 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
如果您使用 AWS Well-Architected Tool 控制台或工具启用信任访问权限，则您无需完成这些步骤。

使用 AWS WA Tool 控制台启用可信访问权限

请参阅 AWS Well-Architected Tool 用户指南中的共享您的 AWS Well-Architected Tool 资源。

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Services (服务) 页面上，找到 AWS Well-Architected Tool 行，选择服务的名称，然后选择 Enable trusted access (启用信任访问权限)。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **enable**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 AWS Well-Architected Tool 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 AWS Well-Architected Tool 作为 Organizations 的信任服务。

```
$ aws organizations enable-aws-service-access \
    --service-principal wellarchitected.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- AWS API：EnableAWSServiceAccess

使用 AWS WA Tool 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您可以使用 AWS Well-Architected Tool 或者 AWS Organizations 工具禁用信任访问权限。

> **Important**
>
> 强烈建议您尽可能使用 AWS Well-Architected Tool 控制台或工具来禁用与 Organizations 的集成。这可让 AWS Well-Architected Tool 执行所需的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 AWS Well-Architected Tool 提供的工具禁用集成时，才会使用这些步骤进行处理。
> 如果您使用 AWS Well-Architected Tool 控制台或工具禁用信任访问权限，则您无需完成这些步骤。

使用 AWS WA Tool 控制台禁用信任访问权限

请参阅 AWS Well-Architected Tool 用户指南中的共享您的 AWS Well-Architected Tool 资源。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

  您可以运行以下命令以禁用 AWS Well-Architected Tool 作为 Organizations 的信任服务。

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

如果成功，此命令不会产生任何输出。

- AWS API：DisableAWSServiceAccess

Amazon VPC IP 地址管理器 (IPAM) 和 AWS Organizations

Amazon VPC IP 地址管理器 (IPAM) 是一项 VPC 功能，可让您更轻松地计划、跟踪和监控 AWS 工作负载的 IP 地址。

使用 AWS Organizations 可以监控整个组织的 IP 地址使用情况，并在成员账户之间共享 IP 地址池。

有关更多信息，请参阅《Amazon VPC IPAM 用户指南》中的将 IPAM 与 AWS Organizations 集成。

使用以下信息可帮助您将 Amazon VPC IP 地址管理器（IPAM）与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

当您通过 IPAM 控制台或者 IPAM 的 `EnableIpamOrganizationAdminAccount` API 将 IPAM 与 AWS Organizations 集成时，系统会在组织的管理账户和每个成员账户中自动创建以下服务相关角色。

- `AWSServiceRoleForIPAM`

有关更多信息，请参阅《Amazon VPC IPAM 用户指南》中的 IPAM 的服务相关角色。

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。IPAM 使用的服务相关角色将为以下服务主体授予访问权限：

- `ipam.amazonaws.com`

启用 IPAM 可信访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

> **Note**
>
> 当您为 IPAM 指定委托管理员时，它会自动为您的组织启用 IPAM 可信访问权限。

IPAM 需要具有 AWS Organizations 的可信访问权限，然后您才能为您的组织将某个成员账户指定为此服务的委托管理员。

您只能使用 Amazon VPC IP 地址管理器（IPAM）工具启用可信访问权限。

如果您使用 IPAM 控制台或 IPAM `EnableIpamOrganizationAdminAccount` API 将 IPAM 与 AWS Organizations 集成，您将会自动授予对 IPAM 的可信访问权限。授予可信访问权限将会在组织的管理账户和所有成员账户中创建服务相关角色 `AWSServiceRoleForIPAM`。IPAM 使用服务相关角色来监控与组织中的 EC2 联网资源关联的 CIDR，并在 Amazon CloudWatch 中存储与 IPAM 相关的指标。有关更多信息，请参阅《Amazon VPC IPAM 用户指南》中的 IPAM 的服务相关角色。

有关启用可信访问权限的说明，请参阅《Amazon VPC IPAM 用户指南》中的将 IPAM 与 AWS Organizations 集成。

Note

您不能使用 AWS Organizations 控制台或 `EnableAWSServiceAccess` API 通过 IPAM 启用信任访问权限。

禁用 IPAM 可信访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 AWS Organizations 管理账户中的管理员可以使用 AWS Organizations `disable-aws-service-access` API 禁用 IPAM 可信访问权限。

有关禁用 IPAM 账户权限和删除服务相关角色的信息，请参阅《Amazon VPC IPAM 用户指南》中的 IPAM 的服务相关角色。

您可以通过运行 Organizations AWS CLI 命令，或者调用某个 AWS SDK 中的 Organizations API 操作来禁用信任访问权限。

AWS CLI, AWS API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作禁用信任服务访问：

- AWS CLI：disable-aws-service-access

您可以运行以下命令来禁用 Amazon VPC IP 地址管理器（IPAM）作为 Organizations 的可信服务。

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

如果成功，此命令不会产生任何输出。

- AWS API：DisableAWSServiceAccess

为 IPAM 启用委托管理员账户

IPAM 的委托管理员账户负责创建 IPAM 和 IP 地址池、管理和监控组织中的 IP 地址使用情况，以及跨成员账户共享 IP 地址池。有关更多信息，请参阅《Amazon VPC IPAM 用户指南》中的将 IPAM 与 AWS Organizations 集成。

只有组织管理账户中的管理员才能为 IPAM 配置委托管理员。

您可以通过 IPAM 控制台或使用 `enable-ipam-organization-admin-account` API 指定委托管理员账户。有关更多信息，请参阅《AWS AWS CLI 命令参考》中的 enable-ipam-organization-admin-account。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色能够将某个成员账户配置为组织的 IPAM 委托管理员。

要使用 IPAM 控制台配置委托管理员，请参阅《Amazon VPC IPAM 用户指南》中的将 IPAM 与 AWS Organizations 集成。

为 IPAM 禁用委托管理员

只有组织管理账户中的管理员才能为 IPAM 配置委托管理员。

要使用 AWS AWS CLI 删除委托管理员，请参阅《AWS AWS CLI 命令参考》中的 disable-ipam-organization-admin-account。

要使用 IPAM 控制台禁用 IPAM 委托管理员账户，请参阅《Amazon VPC IPAM 用户指南》中的将 IPAM 与 AWS Organizations 集成。

Amazon VPC Reachability Analyzer 和 AWS Organizations

Reachability Analyzer 是一种配置分析工具，使您能够在虚拟私有云（VPC）中的源资源和目标资源之间执行连接测试。

AWS Organizations 与 Reachability Analyzer 一起使用可让您跟踪组织中各个账户的路径。

有关更多信息，请参阅 Reachability Analyzer 用户指南中的 Cross-account analyses for Reachability Analyzer（Reachability Analyzer 的跨账户分析）。

使用以下信息可帮助您将 Reachability Analyzer 与 AWS Organizations 集成。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Reachability Analyzer 在您组织中的组织账户内执行支持的操作。

只有在禁用 Reachability Analyzer 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForReachabilityAnalyzer`

有关更多信息，请参阅 Reachability Analyzer 用户指南中的 Cross-account analyses for Reachability Analyzer（Reachability Analyzer 的跨账户分析）。

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Reachability Analyzer 使用的服务相关角色为以下服务主体授予访问权限：

- `reachabilityanalyzer.networkinsights.amazonaws.com`

启用 Reachability Analyzer 信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

当您为 Reachability Analyzer 指定委托管理员时，它会自动为您的组织启用 Reachability Analyzer 信任访问权限。

Reachability Analyzer 需要具有 AWS Organizations 的信任访问权限，然后您才能为您的组织将某个成员账户指定为此服务的委托管理员。

Important

- 您可以使用 Reachability Analyzer 控制台或 Organizations 控制台启用信任访问权限。但是，强烈建议您使用 Reachability Analyzer 控制台或 `EnableMultiAccountAnalysisForAwsOrganization` API 来实现与 Organizations 的集成。这可让 Reachability Analyzer 执行所需的任何配置，例如创建服务所需的资源。
- 授予可信访问权限将会在组织的管理账户和所有成员账户中创建服务相关角色 `AWSServiceRoleForReachabilityAnalyzer`。Reachability Analyzer 使用服务相关角色来支持管理，并允许委托管理员在组织中的任何资源之间运行连接分析。Reachability Analyzer 能够拍摄组织中账户的网络元素的快照，以回答连接查询。
- 有关更多信息以及有关通过 Reachability Analyzer 启用信任访问权限的说明，请参阅 Reacability Analyzer 用户指南中的 Cross-account analyses for Reachability Analyzer（Reachability Analyzer 的跨账户分析）。

您可以使用AWS Organizations控制台，通过运行 AWS CLI 命令，或者通过调用其中一个 AWS SDK 中的 API 操作来启用信任访问权限。

AWS Management Console

要使用 Organizations 控制台启用信任服务访问权限，请执行以下操作：

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在服务页面上，找到 VPC Reachability Analyzer 行，选择服务的名称，然后选择启用可信访问权限。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 AWS Organizations 的管理员，请告诉 Reachability Analyzer 的管理员，他们现在可以使用其控制台启用该服务来处理 AWS Organizations。

AWS CLI, AWS API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 AWS CLI 命令或 API 操作启用信任服务访问权限：

- AWS CLI：enable-aws-service-access

  您可以运行以下命令以启用 Reachability Analyzer 作为 Organizations 的信任服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal reachabilityanalyzer.networkinsights.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- AWS API：EnableAWSServiceAccess

禁用 Reachability Analyzer 信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您可以使用 Reachability Analyzer 控制台（建议）或 Organizations 控制台禁用信任访问权限。要使用 Reachability Analyzer 控制台禁用信任访问权限，请参阅 Reachability Analyzer 用户指南中的 Reachability Analyzer user guide（Reachability Analyzer 的跨账户分析）。

为 Reachability Analyzer 启用委托管理员账户

委托管理员账户能够对组织中的任何资源运行连接分析。有关更多信息，请参阅《Reachability Analyzer 用户指南》中的 将 Reachability Analyzer 与 AWS Organizations 集成）。

只有组织管理账户中的管理员才能为 Reachability Analyzer 配置委托管理员。

您可以通过 Reachability Analyzer 控制台或使用 `RegisterDelegatedAdministrator` API 指定委托管理员账户。有关更多信息，请参阅 Organizations Command Reference（Organizations 命令参考）中的 RegisterDelegatedAdministrator。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色才能将某个成员账户配置为组织的 Reachability Analyzer 委托管理员

要使用 Reachability Analyzer 控制台配置委托管理员，请参阅《Reachability Analyzer 用户指南》中的将 Reachability Analyzer 与 AWS Organizations 集成。

禁用 Reachability Analyzer 的委托管理员

只有组织管理账户中的管理员才能为 Reachability Analyzer 配置委托管理员。

您可以使用 Reachability Analyzer 控制台或 API，或者通过使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作，来删除委托管理员。

要使用 Reachability Analyzer 控制台禁用 Reachability Analyzer 委托管理员账户，请参阅 Reachability Analyzer 用户指南中的 Cross-account analyses for Reachability Analyzer（Reachability Analyzer 的跨账户分析）。

与 Organizations 配合使用的 AWS 服务的委托管理员

我们建议您将 AWS Organizations 管理账户及其用户和角色仅用于必须由该账户执行的任务。此外，我们还建议您将所有的 AWS 资源存储在组织的其他成员账户中，而非保存在管理账户中。这是因为，Organizations 服务控制策略（SCP）等安全功能不会限制管理账户中的用户或角色。将资源与管理账户分离还可帮助您了解发票上的费用。

许多与 Organizations 集成的 AWS 服务可帮助您减少对管理账户的使用。这些服务允许您将一个或多个成员账户注册为管理员，用来管理该服务中使用的所有组织账户。这些账户被称为该特定服务的委托管理员。通过将成员账户注册为 AWS 服务的委托管理员，您可以使该账户拥有该服务的某些管理权限以及 Organizations 只读操作权限。

在将账户注册为服务的委托管理员之前：

- 确认该服务支持委托管理员。请参阅 AWS 可以与之配合使用的服务 AWS Organizations 中的表格，了解哪些服务支持委托管理员。
- 为该服务启用可信访问。

> **Note**
>
> 要了解如何为某个服务启用委托管理员，请参阅 AWS 可以与之配合使用的服务 AWS Organizations 中的表格，然后在该服务的支持委托管理员列中选择了解详情链接。

授予委托管理员账户的权限

每个特定服务的委托管理员账户都具有该服务授予的权限。要了解更多信息，请参阅 AWS 可以与之配合使用的服务 AWS Organizations 中的表格，然后在该服务的支持委托管理员列中选择了解详情链接。

委托管理员账户还具有以下只读权限：

- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy

借助这些权限，您可以查看但不能更改下列控制台项目：

- 组织结构、所有账户和 OU 以及组织策略
- 成员资格
- 所有账户和 OU。
- 组织策略

安全性 AWS Organizations

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 AWS 云中运行 AWS 服务的基础架构。 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。要了解适用的合规计划 AWS Organizations，请参阅按合规计划划分的范围内的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。

此文档将帮助您了解如何在使用 Organizations 时应用责任共担模型。以下主题说明如何配置 Organizations 以实现您的安全性和合规性目标。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 Organizations 资源。

主题

- AWS PrivateLink 对于 AWS Organizations
- AWS Identity and Access Management 和 AWS Organizations
- AWS Organizations 中的日志记录和监控
- AWS Organizations的合规性验证
- AWS Organizations 中的故障恢复能力
- AWS Organizations 中的基础设施安全性

AWS PrivateLink 对于 AWS Organizations

使用 AWS PrivateLink for AWS Organizations，您无需通过公共互联网即可从虚拟私有云 (VPC) 内访问该 AWS Organizations 服务。

Amazon VPC 允许您在自定义虚拟网络中启动 AWS 资源。可以使用 VPC 控制您的网络设置，例如 IP 地址范围、子网、路由表和网络网关。有关 VPC 的更多信息，请参阅《Amazon VPC 用户指南》。

要将您的 Amazon VPC 连接到 AWS Organizations，您必须先定义接口 VPC 终端节点（接口终端节点）。接口端点由一个或多个弹性网络接口 (ENI) 代表，这些接口是从 VPC 中的子网分配的私有 IP 地址。从您的 VPC 发往 AWS Organizations 接口终端节点的请求将保留在 Amazon 网络上。

有关接口终端节点的一般信息，请参阅 Amazon VPC 用户指南中的使用接口 VPC 终端节点访问 AWS 服务。

主题

- for 的 AWS PrivateLink 限制和限制 AWS Organizations
- 创建 VPC 端点
- 为 AWS Organizations创建 VPC 端点策略

for 的 AWS PrivateLink 限制和限制 AWS Organizations

VPC 限制适用 AWS PrivateLink 于 AWS Organizations。有关更多信息，请参阅 Amazon VPC 用户指南中的使用接口 VPC 终端节点和AWS PrivateLink 配额访问 AWS 服务。此外，以下限制将适用：

- 仅us-east-1在该地区可用
- 不支持传输层安全 (TLS) 1.1

创建 VPC 端点

您可以使用 Amazon VPC 控制台 AWS Command Line Interface （ AWS CLI ）或，在您的 VPC 中创建 AWS Organizations 终端节点 AWS CloudFormation。

有关使用 Amazon VPC 控制台或创建和配置终端节点的信息 AWS CLI，请参阅 Amazon VPC 用户指南中的创建 VPC 终端节点。有关使用创建和配置终端节点的信息 AWS CloudFormation，请参阅用户指南中的 AWS:: EC2:: vpcendPoint 资源。AWS CloudFormation

创建 AWS Organizations 终端节点时，请使用以下内容作为服务名称：

```
com.amazonaws.us-east-1.organizations
```

如果您在访问时需要经过 FIPS 140-2 验证的加密模块 AWS，请使用以下 AWS Organizations FIPS 服务名称：

```
com.amazonaws.us-east-1.organizations-fips
```

为 AWS Organizations创建 VPC 端点策略

您可以将终端节点策略附加到您的 VPC 终端节点，以控制对 Organizations 的访问权限。该策略指定以下信息：

- 可执行操作的主体。
- 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 Amazon VPC 用户指南中的使用终端节点策略控制 VPC 终端节点的访问权限。

示例： AWS Organizations 操作的 VPC 端点策略

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

AWS Identity and Access Management 和 AWS Organizations

访问 AWS Organizations 需要凭证。这些凭证必须有权访问AWS资源，例如 Amazon Simple Storage Service（Amazon S3）存储桶、Amazon Elastic Compute Cloud（Amazon EC2）实例或 AWS Organizations 组织部门（OU）。以下部分提供了有关如何使用 AWS Identity and Access Management（IAM）帮助确保安全访问组织和控制谁可以管理组织的详细信息。

为确定谁能够管理组织的哪些部分，AWS Organizations 使用与其他AWS服务相同的基于 IAM 的权限模型。作为组织的管理账户中的管理员，您可以通过将策略附加到管理账户中的用户、组和角色，授予基于 IAM 的权限以执行 AWS Organizations 任务。这些策略指定这些委托人可执行的操作。您将 IAM 权限策略附加到用户所属的组，或者直接附加到用户或角色。作为最佳实践，我们建议您将策略附加到组而不是用户。您还可以选择向其他人授予完整管理员权限。

对于 AWS Organizations 的大多数管理员操作，您需要将权限附加到管理账户中的用户或组。如果某个成员账户中的用户需要为您的组织执行管理员操作，则您需要将 AWS Organizations 权限授予管理账户中的 IAM 角色，并且在成员账户中启用用户来担任该角色。有关 IAM 权限策略的常规信息，请参阅《IAM 用户指南》中的 IAM 策略概述。

主题

身份验证

您能够以下面任一类型的身份访问 AWS：

- AWS 账户根用户 - 注册AWS时，您需要提供与您的AWS 账户关联的电子邮件地址和密码。这些是您的根凭证，它们提供对您所有 AWS 资源的完全访问权限。

  > **Important**
  >
  > 当您注册 AWS 账户时，系统将会创建一个 AWS 账户根用户。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，请为管理用户分配管理访问权限，并且只使用根用户执行需要根用户访问权限的任务。

- IAM 用户 – IAM 用户就是您的AWS 账户中的一种身份，它具有特定的自定义权限（例如，用于在 Amazon Elastic File System 中创建文件系统的权限）。您可以使用 IAM 用户名和密码登录以保护AWS网页（如AWS Management Console、AWS开发论坛或AWS支持中心）。

  除了用户名和密码之外，您还可以为每个用户生成访问密钥。在通过几个开发工具包之一或使用 AWS Command Line Interface（AWS CLI）以编程方式访问AWS服务时，可以使用这些密钥。SDK 和 AWS CLI 工具使用访问密钥对您的请求进行加密签名。如果您不使用 AWS 工具，则必须自行对请求签名。AWS Organizations 支持签名版本 4，后者是一种用于对入站 API 请求进行身份验证的协议。有关对请求进行身份验证的更多信息，请参阅 I AM 用户指南中的签署 AWS API 请求。

- IAM 角色 – IAM 角色是可在账户中创建的另一种具有特定权限的 IAM 身份。它类似于 IAM 用户，但未与特定人员相关联。利用 IAM 角色，您可以获得可用于访问AWS服务和资源的临时访问密钥。具有临时凭证的 IAM 角色在以下情况下很有用：

  - 联合身份用户访问 – 您可以不创建 IAM 用户，而是使用来自 AWS Directory Service、您的企业用户目录或 Web 身份提供程序的既有用户身份。这些用户被称为联合用户。在通过身份提供商请求访问权限时，AWS将为联合身份用户分配角色。有关联合身份用户的更多信息，请参阅 IAM 用户指南中的联合身份用户和角色。

- 跨账户访问 – 可以使用您账户中的 IAM 角色向另一个AWS 账户授予对您账户的资源的访问权限。有关示例，请参阅《IAM 用户指南》中的教程：使用 IAM 角色委派跨 AWS 账户 的访问权限。
- AWS服务访问 – 可以使用您账户中的 IAM 角色向AWS服务授予对您账户的资源的访问权限。例如，您可以创建一个角色以允许 Amazon Redshift 代表您访问 Amazon S3 存储桶，然后将存储在该存储桶中的数据加载到 Amazon Redshift 集群中。有关更多信息，请参阅 IAM 用户指南中的创建向AWS服务委派权限的角色。
- 在Amazon EC2 上运行的应用程序 – 您不用将访问密钥存储在 EC2 实例中以供实例上运行的应用程序使用并发出 AWS API 请求，而是可以使用 IAM 角色管理这些应用程序的临时凭证。要将AWS角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

访问控制

您可以使用有效的凭证来对自己的请求进行身份验证，但您还必须拥有权限才能管理或访问 AWS Organizations 资源。例如，您必须拥有权限来创建 OU 或者将服务控制策略 (SCP) 附加到账户。

下面几节介绍如何管理 AWS Organizations 的权限。

- 管理您的 AWS 组织的访问权限
- 为 AWS Organizations 使用基于身份的策略（IAM 策略）
- 使用标签和 AWS Organizations 的基于属性的访问控制

管理您的 AWS 组织的访问权限

所有AWS资源（包括组织中的根、OU、账户和策略）都归AWS 账户所有，创建和访问资源的权限由权限策略进行管理。对于一个组织，其管理账户拥有所有资源。账户管理员可通过将权限策略附加到 IAM 身份（用户、组和角色）来控制对 AWS 资源的访问。

> **Note**
>
> 账户管理员 (或管理员用户) 是具有管理员权限的用户。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

在授予权限时，您要决定谁获得权限，获得对哪些资源的权限，以及您允许对这些资源执行的具体操作。

默认情况下，IAM 用户、组和角色没有权限。作为组织管理账户的管理员，您可以执行管理任务或将管理员权限委派给管理账户中的其他 IAM 用户或角色。为此，您可以将 IAM 权限策略附加到 IAM 用户、组或角色。默认情况下，用户没有权限；这有时称为隐式拒绝。该策略将使用显式允许 覆盖隐式拒绝，这将指定用户可以执行哪些操作以及可对哪些资源执行这些操作。如果将权限授予了角色，则组织中其他账户的用户可以代入该角色。

AWS Organizations 资源和操作

此部分讨论如何将 AWS Organizations 概念映射到其 IAM 等效概念。

资源

在 AWS Organizations 中，您可以控制对以下资源的访问：

- 构成组织层次结构的根和 OU
- 组织的成员账户
- 您附加到组织中实体的账户
- 用于更改组织状态的握手

其中，每种资源均有一个与之关联的唯一 Amazon 资源名称 (ARN)。您可以通过在 IAM 权限策略的 `Resource` 元素中指定资源的 ARN 来控制对资源的访问。有关中使用的资源的 ARN 格式的完整列表 AWS Organizations，请参阅《服务授权参考》AWS Organizations中定义的资源类型。

操作

AWS 提供了一组操作来处理组织中的资源。利用这些操作，您可以对资源进行创建、列出、修改、访问其内容以及删除。可在 IAM policy 的 `Action` 元素中引用大多数操作来控制可使用操作的人员。有关可用作 IAM 策略中权限的AWS Organizations操作列表，请参阅《服务授权参考》中的 Organi AWSzations 定义的操作。

在将 `Action` 和 `Resource` 组合到一个权限策略 `Statement` 中后，可以准确控制可对哪些资源执行该组特定操作。

条件键

AWS 提供可供您进行查询以便对某些操作进行更精细控制的条件键。您可以在 IAM policy 的 `Condition` 元素中参考这些条件密钥，以指定将语句视为匹配必须满足的其他条件。

以下条件键专门用 AWS Organizations：

- `aws:PrincipalOrgID` – 简化在基于资源的策略中指定 `Principal` 元素的过程。此全局键提供了列出组织中的所有AWS 账户的所有账户 ID 的替代方法。您可以在 元素中指定组织 IDCondition，而不是列出作为组织成员的所有账户。

  > **Note**
  >
  > 此全局条件也适用于组织的管理账户。

  有关更多信息，请参阅 IAM 用户指南*PrincipalOrgID*中对AWS全局条件上下文密钥的描述。

- `aws:PrincipalOrgPaths` – 使用此条件键可以匹配特定组织根、OU 或其子项的成员。当发出请求的委托人（根用户、IAM 用户或角色）位于指定的组织路径中时，`aws:PrincipalOrgPaths` 条件键返回 true。路径是 AWS Organizations 实体结构的文本表示形式。有关路径的更多信息，请参阅 IAM 用户指南中的了解AWS Organizations实体路径。有关使用此条件键的更多信息，请参阅 IAM 用户指南PrincipalOrgPaths中的 aws:。

  例如，以下条件元素匹配同一组织中两个 OU 之一的成员。

  ```
  "Condition": {
      "ForAnyValue:StringLike": {
          "aws:PrincipalOrgPaths": [
              "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
              "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
          ]
      }
  }
  ```

- `organizations:PolicyType` – 您可以使用此条件键限制与 Organizations 策略相关的 API 操作以仅处理指定类型的 Organizations 策略。您可以将此条件键应用于任何包含与 Organizations 策略交互的操作的策略语句。

  可以将以下值与此条件键结合使用：

  - `AISERVICES_OPT_OUT_POLICY`
  - `BACKUP_POLICY`
  - `SERVICE_CONTROL_POLICY`
  - `TAG_POLICY`

例如，以下示例策略允许用户执行任何 Organizations 操作。但是，如果用户执行采用策略参数的操作，则仅当指定的策略是标记策略时才允许该操作。如果用户指定任何其他类型的策略，则该操作将失败。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
    ]
}
```

- `organizations:ServicePrincipal`— 如果您使用 “启用” 或 “禁用” AWSServiceAccess 操作启用AWSServiceAccess或禁用对其他AWS服务的可信访问，则可用作条件。您可以使用 `organizations:ServicePrincipal` 来将这些操作发出的请求限制为已批准的服务委托人名称列表。

  例如，下面的策略允许用户在启用和禁用对 AWS Organizations 的可信访问时仅指定 AWS Firewall Manager。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

有关可在 IAM 策略中用作权限的所有AWS Organizations特定条件密钥的列表，请参阅《服务授权参考》AWS Organizations中的条件密钥。

了解资源所有权

AWS 账户对在该账户下创建的资源具有所有权，而无论创建资源的人员是谁。具体而言，资源所有者是对资源创建请求进行身份验证的主体实体（即根用户、IAM 用户或 IAM 角色）的 AWS 账户。对于AWS组织，始终为管理账户。您无法从成员账户调用大多数创建或访问组织资源的操作。以下示例说明了它的工作原理：

- 如果您使用管理账户的根账户凭证创建 OU，您的管理账户即为该资源的拥有者。（在 AWS Organizations 中，该资源为 OU。）
- 如果您在管理账户中创建 IAM 用户并向其授予创建 OU 的权限，则该用户可以创建 OU。但是，管理账户（即该用户所属的账户）拥有 OU 资源。
- 如果您在管理账户中创建的 IAM 角色具有创建 OU 的权限，则能够代入该角色的任何人都可以创建 OU。管理账户（即该角色而非代入用户所属的账户）拥有 OU 资源。

管理对资源的访问

权限策略规定谁可以访问哪些内容。下一节介绍创建权限策略时的可用选项。

> **Note**
>
> 本节讨论如何在 AWS Organizations 范围内使用 IAM。这里不提供有关 IAM 服务的详细信息。有关完整的 IAM 文档，请参阅 IAM 用户指南。有关 IAM 策略语法和描述的信息，请参阅 IAM 用户指南中的 IAM JSON 策略参考。

附加到 IAM 身份的策略称作基于身份的策略 (IAM policy)。附加到资源的策略称作基于资源的策略。AWS Organizations 仅支持基于身份的策略 (IAM policy)。

主题

- 基于身份的权限策略 (IAM policy)
- 基于资源的策略

基于身份的权限策略 (IAM policy)

您可以将策略附加到 IAM 身份以允许这些身份对AWS资源执行操作。例如，您可以执行以下操作：

- 将权限策略附加到您的账户中的用户或组 – 要向用户授予创建 AWS Organizations 资源（例如，服务控制策略 (SCP) 或 OU）的权限，您可以将权限策略附加到用户或用户所属的组。用户或组必须位于组织的管理账户中。
- 向角色附加权限策略（授予跨账户权限） – 您可以向 IAM 角色附加基于身份的权限策略以向组织授予跨账户访问权。例如，管理账户中的管理员可以创建一个角色来向成员账户中的用户授予跨账户权限，如下所示：

  1. 管理账户管理员创建一个 IAM 角色，并向该角色附加一个权限策略以授予对组织资源的权限。
  2. 管理账户管理员向将成员账户 ID 标识为能够担任该角色的 `Principal` 的角色附加信任策略。
  3. 随后，成员账户管理员可以委派权限以将角色代入成员账户中的任何用户。通过执行此操作，成员账户中的用户将能够在管理账户和组织中创建和访问资源。如果您需要向 AWS 服务授予代入该角色的权限，则信任策略中的委托人也可以是 AWS 服务委托人。

  有关使用 IAM 委派权限的更多信息，请参阅《IAM 用户指南》中的访问权限管理。

以下是允许用户在您的组织中执行 `CreateAccount` 操作的策略示例。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1OrgPermissions",
         "Effect":"Allow",
         "Action":[
            "organizations:CreateAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

您还可以在策略的 Resource 元素中提供部分 ARN 以指示资源类型。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowCreatingAccountsOnResource",
         "Effect":"Allow",
         "Action":"organizations:CreateAccount",
         "Resource":"arn:aws:organizations::*:account/*"
      }
   ]
}
```

您也可以拒绝创建不包含所创建账户的特定标签的账户。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyCreatingAccountsOnResourceBasedOnTag",
         "Effect":"Deny",
         "Action":"organizations:CreateAccount",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/key":"value"
            }
         }
      }
   ]
}
```

有关用户、群组、角色和权限的更多信息，请参阅 IAM 用户指南中的 IAM 身份（用户、用户组和角色）。

基于资源的策略

一些服务（如 Amazon S3）支持基于资源的权限策略。例如，您可以将策略附加到 Amazon S3 存储桶以管理对该存储桶的访问权限。AWS Organizations 目前不支持基于资源的策略。

指定策略元素：操作、条件、效果和资源

对于每项 AWS Organizations 资源，该服务定义一组 API 操作或可通过某种方式与该资源交互或操作该资源的操作。为授予这些操作的权限，AWS Organizations 定义了一组您可以在策略中指定的操作。例如，对于 OU 资源，AWS Organizations 定义了以下操作：

- `AttachPolicy` 和 `DetachPolicy`
- `CreateOrganizationalUnit` 和 `DeleteOrganizationalUnit`
- `ListOrganizationalUnits` 和 `DescribeOrganizationalUnit`

在有些情况下，执行 API 操作可能需要多个操作的权限，并且可能需要多个资源的权限。

以下是可在 IAM 权限策略中使用的最基本元素：

- Action – 使用此关键字标识要允许或拒绝的操作。例如，根据指定的 `Effect`，`organizations:CreateAccount` 允许或拒绝执行 AWS Organizations `CreateAccount` 操作的用户权限。有关更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素：操作。
- Resource – 使用此关键字指定策略语句适用于的资源的 ARN。有关更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素：资源。
- Condition – 使用此关键字指定要应用策略语句必须满足的条件。`Condition` 通常指定为使策略匹配必须存在的额外情况。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- Effect – 使用此关键字指定策略语句是允许还是拒绝对资源进行的操作。如果没有明确授予 (或允许) 对资源的访问权，则隐式拒绝访问。您也可以明确拒绝对资源的访问权，这样做可确保用户无法对指定资源执行指定操作，即使其他策略授予了访问权也是如此。有关更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素：效果。
- Principal – 在基于身份的策略 (IAM policy) 中，附加了策略的用户会自动成为隐式委托人。对于基于资源的策略，您可以指定要接收权限的用户、账户、服务或其他实体（仅适用于基于资源的策略）。AWS Organizations 目前仅支持基于身份的策略，而不是基于资源的策略。

要了解有关 IAM 策略语法和描述的更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略参考。

为 AWS Organizations 使用基于身份的策略（IAM 策略）

作为组织管理账户的管理员，您可以通过将权限策略附加到组织中的 AWS（IAM）身份（用户、组和角色）来控制对AWS Identity and Access Management资源的访问权。在授予权限时，您要决定谁获

得权限，获得对哪些资源的权限，以及您允许对这些资源执行的具体操作。如果将权限授予了角色，则组织中其他账户的用户可以担任该角色。

默认情况下，用户没有任何类型的权限。所有权限都必须通过策略明确授予。如果未明确授予某个权限，则默示拒绝该权限。如果明确拒绝了某个权限，则其优于任何其他可能允许该权限的策略。换而言之，用户仅具有明确授予和未明确拒绝的权限。

除了本主题中介绍的基本技术之外，您还可以使用应用于组织中资源的标签来控制对组织的访问：组织根、组织部门（OU）、账户和策略。有关更多信息，请参阅 使用标签和 AWS Organizations 的基于属性的访问控制。

将全部管理员权限授予用户

您可以创建一个 IAM 策略，向组织中的 IAM 用户授予完全 AWS Organizations 管理员权限。您可以使用 IAM 控制台中的 JSON 策略编辑器来执行此操作。

使用 JSON 策略编辑器创建策略

1. 登录AWS Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧的导航窗格中，选择策略。

   如果这是您首次选择策略，则会显示欢迎访问托管式策略页面。选择开始使用。
3. 在页面的顶部，选择创建策略。
4. 在策略编辑器部分，选择 JSON 选项。
5. 输入以下 JSON 策略文档：

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

6. 选择下一步。

> **Note**
>
> 您可以随时在可视化和 JSON 编辑器选项卡之间切换。不过，如果您进行更改或在可视化编辑器中选择下一步，IAM 可能会调整策略结构以针对可视化编辑器进行优化。有关更多信息，请参阅《IAM 用户指南》中的调整策略结构。

7. 在查看并创建页面上，为您要创建的策略输入策略名称和描述（可选）。查看此策略中定义的权限以查看策略授予的权限。
8. 选择创建策略可保存新策略。

要了解有关创建 IAM 策略的更多信息，请参阅 IAM 用户指南中的创建 IAM 策略。

按操作授予有限访问权

如果只是授予有限权限而非完全权限，则可以创建一个策略，列出您打算在 IAM 权限策略的 `Action` 元素中允许的各个权限。如以下示例中所示，您可以使用通配符 (*) 字符来仅授予 `Describe*` 和 `List*` 权限，这实际上提供对组织的只读访问权限。

> **Note**
>
> 在服务控制策略 (SCP) 中，`Action` 元素中的通配符 (*) 字符只能由自身使用或用在字符串结尾处。它不能出现在字符串的开头或中间部分。因此，`"servicename:action*"` 是有效的，但 `"servicename:*action"` 和 `"servicename:some*action"` 在 SCP 中都是无效的。

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

有关可在 IAM 策略中分配的所有权限的列表，请参阅《服务授权参考》中的 Organi AWSzations 定义的操作。

授予对特定资源的访问权限

除了限制对特定操作的访问权之外，您还可以限制对组织中特定实体的访问权。前面部分示例中的 `Resource` 元素均指定通配符（“*”），这意味着“操作可以访问的任意资源”。不过，您可以使用希望允许访问的特定实体的 Amazon 资源名称 (ARN) 替换 "*"。

示例：将权限授予单个 OU

以下策略中的第一条语句允许 IAM 用户对整个组织的读取访问权限，但第二条语句允许用户仅在单个指定的组织部门（OU）中执行 AWS Organizations 管理操作。这不会扩展到任何子 OU。未授予账单访问权。请注意，这不会授予您对 OU 中的AWS 账户的管理访问权。它仅授予对指定 OU 中的账户执行 AWS Organizations 操作的权限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "arn:aws:organizations::<masterAccountId>:ou/o-<organizationId>/ou-<organizationalUnitId>"
    }
  ]
}
```

您可以从 AWS Organizations 控制台或调用 `List*` API 来获取 OU 和组织的 ID。您应用到此策略的用户或组可以在指定 OU 中直接包含的任何实体上执行任何操作（`"organizations:*"`）。OU 由 Amazon 资源名称 (ARN) 来标识。

有关各种资源的 ARN 的更多信息，请参阅《服务授权参考》AWS Organizations中定义的资源类型。

向有限服务委托人授予允许可信访问的功能

您可以使用策略语句的 Condition 元素对策略语句匹配的情况做进一步限制。

示例：授予对一个指定服务允许可信访问的权限

以下语句显示如何将允许可信访问的功能局限于您指定的哪些服务。如果用户尝试调用的 API 与用于 AWS IAM Identity Center 的 API 拥有不同的服务委托人，则此策略不匹配并拒绝请求：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

有关各种资源的 ARN 的更多信息，请参阅《服务授权参考》AWS Organizations中定义的资源类型。

使用标签和 AWS Organizations 的基于属性的访问控制

基于属性的访问控制允许您使用管理员管理的属性（例如附加到AWS资源和AWS身份的标签）来控制对这些资源的访问。例如，您可以指定当用户和资源对某个标签具有相同的值时，用户可以访问该资源。

AWS Organizations 可标记的资源包括AWS 账户、组织的根、组织部门（OU）或策略。当您将标签附加到 Organizations 资源时，您可以使用这些标签来控制谁可以访问这些资源。您可以将 Condition 添加元素添加到您的 AWS Identity and Access Management（IAM）权限策略语句，在允许执行操作之前检查某些标签键和值是否存在。这可让您创建一个 IAM 策略，该策略有效地说明“仅允许用户管理那些具有键 X 和值 Y 的标签的 OU”或“仅允许用户管理那些使用与用户附加的标签键 Z 具有相同值的键 Z 标记的 OU”。

您可以根据 IAM 策略中的不同类型的标签引用进行 Condition 测试。

- 检查附加到请求中指定资源的标签
- 检查附加到发出请求的 IAM 用户或角色的标签
- 检查请求中作为参数包含的标签

有关在策略中使用标签进行访问控制的更多信息，请参阅使用资源标签控制对 IAM 用户和角色的访问。有关 IAM 权限策略的完整语法，请参阅 IAM JSON 策略参考

检查附加到请求中指定资源的标签

当您使用AWS Management Console、AWS Command Line Interface（AWS CLI）或其中一个 AWS SDK 发出请求时，您可以指定要通过该请求访问的资源。无论您是试图列出给定类型的可用资源、读取资源还是写入、修改或更新资源，都可以将要访问的资源指定为请求中的参数。此类请求由您附加到用户和角色的 IAM 权限策略控制。在这些策略中，您可以比较附加到请求资源的标签，并根据这些标签的键和值选择允许或拒绝访问。

若要检查附加到资源的标签，请引用 `Condition` 元素中的标签，方法是在标签键名称前面加上以下字符串：`aws:ResourceTag/`

例如，以下示例策略允许用户或角色执行任何 AWS Organizations 操作，除非该资源有一个带有键 `department` 和值 `security` 的标签。如果该键和值存在，则策略明确拒绝 `UntagResource` 操作。

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

        },
        {
            "Effect" : "Deny",
            "Action" : "organizations:UntagResource",
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "aws:ResourceTag/department" : "security"
                }
            }
        }
```

```
    ]
}
```

有关如何使用此元素的更多信息，请参阅《IAM 用户指南》中的控制对资源的访问和 aws:ResourceTag。

检查附加到发出请求的 IAM 用户或角色的标签

您可以根据附加到发出请求的人员（委托人）的 IAM 用户或角色的标签，控制允许该人员执行哪些操作。若要执行此操作，请使用 aws:PrincipalTag/*key-name* 条件键指定必须附加到调用用户或角色的标签和值。

以下示例说明如何仅当指定的标签（cost-center）在调用操作的委托人和操作正在访问的资源上具有相同的值时才允许操作。在此示例中，调用用户只有在实例被标记为与用户相同的 cost-center 时，才能启动或停止 Amazon EC2 实例。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

有关如何使用此元素的更多信息，请参阅《IAM 用户指南》中的控制 IAM 委托人进行的访问和 aws:PrincipalTag。

检查请求中作为参数包含的标签

通过多个操作，您可以将标签指定为请求的一部分。例如，当您创建资源时，您可以指定附加到新资源的标签。您可以指定使用 aws:TagKeys 的 Condition 元素，根据请求中是否包含特定标签键或一组密钥，来允许或拒绝操作。此比较运算符不关心标签包含的值。它只检查是否存在具有指定键的标签。

要检查标签键或键列表，请使用以下语法指定 Condition 元素：

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

您可以使用 ForAllValues: 作为比较运算符的开头，以确保请求中的所有键必须与策略中指定的其中一个键匹配。例如，以下示例策略仅当请求中存在所有三个指定标签键时，才允许任何 Organizations 操作。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
}
```

或者，您可以使用 ForAnyValue: 作为比较运算符的开头，以确保请求中至少有一个键必须与策略中指定的其中一个键匹配。例如，以下策略仅当请求中存在至少一个指定标签键时，才允许 Organizations 操作。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
                    "domain"
                ]
```

```
            }
        }
    }
}
```

通过多个操作，您可以在请求中指定标签。例如，当您创建资源时，您可以指定附加到新资源的标签。您可以将策略中的标签键值对与请求包含的键值对进行比较。若要执行此操作，请引用 Condition 元素中的标签，方法是在标签键名称前面加上以下字符串：aws:RequestTag/*key-name*，然后指定必须存在的标签值。

例如，以下示例策略拒绝用户或角色创建 AWS 账户 的任何请求，其中请求缺少 costcenter 标签，或者为该标签提供了除 1、2，或者 3 以外的值。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

有关如何使用这些元素的更多信息，请参阅《IAM 用户指南》中的 aws:TagKeys 和 aws:RequestTag。

AWS Organizations 中的日志记录和监控

您应对组织进行监控，确保对所做的更改进行记录，这是最佳实践。这有助于确保能够调查任何意外的更改，并回滚不需要的更改。AWS Organizations 目前支持两种 AWS 服务，帮您监控组织和组织内部的活动。

主题

- 使用 AWS Organizations 记录 AWS CloudTrail API 调用
- Amazon EventBridge

使用 AWS Organizations 记录 AWS CloudTrail API 调用

AWS Organizations 与 AWS CloudTrail 集成，后者是在 AWS 中记录用户、角色或 AWS Organizations 服务所执行操作的服务。CloudTrail 将对 AWS Organizations 的所有 API 调用均作为事件捕获，包括来自 AWS Organizations 控制台的调用和对 AWS Organizations API 的代码调用。如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 AWS Organizations 的事件）。如果您不配置跟踪记录，则仍可在 CloudTrail 控制台中的事件历史记录中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向 AWS Organizations 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

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

> **Important**
>
> 您只能在美国东部（弗吉尼亚北部）区域查看 AWS Organizations 的所有 CloudTrail 信息。如果无法在 CloudTrail 控制台中看到您的 AWS Organizations 活动，请使用右上角的菜单将控制台设为美国东部（弗吉尼亚北部）。如果您使用 AWS CLI 或开发工具包工具查询 CloudTrail，请将您的查询引至美国东部（弗吉尼亚北部）终端节点。

CloudTrail 中的 AWS Organizations 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 AWS Organizations 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。

对于AWS 账户中的事件的持续记录（包括 AWS Organizations 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 Amazon S3 桶。在您的AWS 账户中启用了 CloudTrail 日志记录时，对 AWS Organizations 操作的 API 调用在 CloudTrail 日志文件中跟踪，它们随其他AWS服务记录一起写入到这些文件中。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措施。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知

CloudTrail 记录所有 AWS Organizations 操作，AWS Organizations API 参考中介绍了这些操作。例如，对 `CreateAccount`（包括 `CreateAccountResult` 事件）、`ListHandshakesForAccount`、`CreatePolicy` 和 `InviteAccountToOrganization` 的调用将在 CloudTrail 日志文件中生成条目。

每个日志条目都包含有关生成请求的人员的信息。日志条目中的用户身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 IAM 用户凭证发出的
- 请求是使用 IAM 角色还是联合身份用户的临时安全凭证发出的
- 请求是否由其它 AWS 服务发出

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

了解 AWS Organizations 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，因此它们不会按任何特定顺序显示。

示例日志条目：CloseAccount

以下示例显示了示例 `CloseAccount` 调用的 CloudTrail 日志条目，该调用是在调用 API 和关闭账户的工作流开始在后台处理时生成的。

```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2022-03-18T18:17:06Z"
            }
        }
    },
    "eventTime": "2022-03-18T18:17:06Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CloseAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
    "requestParameters": {
        "accountId": "555555555555"
    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


以下示例显示了在后台关闭账户的工作流成功完成后，`CloseAccountResult` 调用的 CloudTrail 日志条目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
   },
   "eventCategory": "Management"
}
```

示例日志条目：CreateAccount

以下示例显示了一个示例 `CreateAccount` 调用的 CloudTrail 日志条目，该调用是在调用 API 和创建账户的工作流开始在后台处理时生成的。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-09-16T21:16:45Z"
            }
        }
    },
    "eventTime": "2018-06-21T22:06:27Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
    "requestParameters": {
        "tags": [],
        "email": "****",
        "accountName": "****"
    },
    "responseElements": {
        "createAccountStatus": {
            "accountName": "****",
            "state": "IN_PROGRESS",
            "id": "car-examplecreateaccountrequestid111",
            "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

以下示例显示了在后台创建账户的工作流成功完成后，CreateAccount 调用的 CloudTrail 日志条目。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}
```

以下示例显示了在 CreateAccount 后台工作流无法创建账户后生成的 CloudTrail 日志条目。

```
  {
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
```

```
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

示例日志条目：CreateOrganizationalUnit

以下示例演示示例 `CreateOrganizationalUnit` 调用的一个 CloudTrail 日志条目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
```

```
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
    },
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

示例日志条目：InviteAccountToOrganization

以下示例演示示例 `InviteAccountToOrganization` 调用的一个 CloudTrail 日志条目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:41:17Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "InviteAccountToOrganization",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "notes": "This is a request for Mary's account to join Diego's organization.",
        "target": {
            "type": "ACCOUNT",
            "id": "111111111111"
```

```
        }
    },
    "responseElements": {
        "handshake": {
            "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
            "state": "OPEN",
            "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
            "id": "h-examplehandshakeid111",
            "parties": [
                {
                    "type": "ORGANIZATION",
                    "id": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "id": "222222222222"
                }
            ],
            "action": "invite",
            "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
            "resources": [
                {
                    "resources": [
                        {
                            "type": "MASTER_EMAIL",
                            "value": "diego@example.com"
                        },
                        {
                            "type": "MASTER_NAME",
                            "value": "Management account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "value": "222222222222"
                },
```

```
                {
                    "type": "NOTES",
                    "value": "This is a request for Mary's account to join Diego's
 organization."
                }
            ]
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

示例日志条目：AttachPolicy

以下示例演示示例 `AttachPolicy` 调用的一个 CloudTrail 日志条目。该响应指示，在请求尝试附加到的根中，由于请求的策略类型未启用，调用失败。

```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
        "policyId": "p-examplepolicyid111",
        "targetId": "ou-examplerootid111-exampleouid111"
    },
```

```
    "responseElements": null,
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Amazon EventBridge

AWS Organizations 可以与 Amazon EventBridge（之前称为 Amazon CloudWatch Events）结合使用，从而在组织中发生管理员指定的操作时生成事件。例如，大多数管理员希望每次在组织中创建新账户时，或成员账户的管理员尝试离开组织时收到提醒，因为这些都是敏感操作。您可以配置 EventBridge 规则来监控这些操作，然后将生成的事件发送到管理员定义的目标。目标可以是 Amazon SNS 主题，向订阅者发送电子邮件或短信。您还可以创建一个 AWS Lambda 函数，记录操作的详细信息以备稍后查看。

有关如何启用 EventBridge 以监控组织中关键活动的教程，请参阅 教程：使用 Amazon EventBridge 监控对您的组织进行的重要更改。

要了解有关 EventBridge 的更多信息，包括如何配置和启用该服务，请参阅《Amazon EventBridge 用户指南》。

AWS Organizations的合规性验证

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

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

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

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

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

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

AWS Organizations 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。

AWS Organizations 中的基础设施安全性

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

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

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

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

如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

AWS Organizations 引用

使用本部分中的主题查找 AWS Organizations 各方面的详细参考信息。

主题

的配额 AWS Organizations

本节指定影响 AWS Organizations的配额。

命名指南

以下是您在中创建的名称的指导原则 AWS Organizations，包括帐户名称、组织单位 (OU)、根和策略：

- 名称必须由 Unicode 字符组成
- 名称的最大字符串长度因对象而异。若要查看各实际限制，请参阅 AWS Organizations API 参考并找到创建对象的 API 操作。查看该操作的 Name 参数的详细信息。例如：账户名称或者 OU 名称。

最大值和最小值

以下是中实体的默认最大值。 AWS Organizations

> **Note**
>
> 您可以使用服务限额控制台请求增加其中一些值。
> Organizations 是一项物理托管在美国东部（弗吉尼亚北部）区域（us-east-1）的全球服务。因此，在使用 us-east-1 Service Quotas 控制台、或 AWS SDK 时，必须使用来访问 Organi AWS CLI zations 配额。

组织 AWS 账户 中的人数	10 – 一个组织中允许的原定设置最大账户数。如果您需要更多，则可以使用服务限额控制台请求增加。

	发送到账户的邀请将计入此限额。如果受邀账户拒绝邀请、管理账户取消邀请或邀请过期，则撤销此计数。 新创建的账户和组织的限额可能会低于默认的 10 个账户。
组织中的根数量	1
组织中的 OU 数量	1000
组织中的每种类型的策略数量	AI 服务选择退出政策：1000 Backup 策略：1000 服务控制策略：2000 标签政策：1000
策略文档的最大大小	AI 服务选择退出策略：2500 个字符 备份策略：10000 个字符 服务控制策略：5120 个字符 标签策略：10000 个字符 注意：如果您使用保存策略 AWS Management Console，则 JSON 元素之间和引号之外的多余空格（例如空格和换行符）将被移除且不计算在内。如果您使用 SDK 操作或保存策略 AWS CLI，则策略将完全按照您提供的方式保存，并且不会自动删除字符。
根中的最大 OU 嵌套数	根下方最深五层 OU。
您可在 24 小时内可以执行的最大邀请尝试次数	您组织中允许的最大账户数或 20 个账户（以较大值为准）。已接受的邀请不计入此配额。一旦某个邀请被接受，您就可以发送另一个同一天的邀请。 如果您的组织中允许的最大账户数少于 20，则如果您尝试邀请超过组织所能容纳的账户数，则会出现“超出账户限制”异常。但是，您可以在一天内取消邀请并发送多次新邀请（最多 20 次尝试）。

您可以同时创建的成员账户数量	5 – 一个创建完成后即可开始另一个，但正在进行中的只能有五个。
您可以在 30 天的周期内关闭的成员账户数量	组织中成员账户的 10%，最多 1000 个。 • < 100 个账户 – 您最多可以关闭 10 个成员账户 • 100-10,000 个账户 — 您可以关闭最多 10% 的会员账户 • > 10,000 个账户 — 您最多可以关闭 1000 个成员账户 例如，如果您有 10,500 个成员账户，则在 30 天内最多可以关闭 1000 个（而不是 1050 个）账户。达到此限额后，您可以通过 AWS Billing 控制台 中关闭额外的账户或等到限额重置后再关闭额外的账户。有关更多信息，请参阅《账户管理指南》中的 “AWS 关闭账户前须知”。
您可以同时关闭的成员账户数量	3 – 同一时间只能处理三个账户关闭。一个账户关闭完成后，您就可以关闭另一个账户。
可以附加到策略的实体数	无限制
您可以附加到根、OU 或账户的标签数	50
基于资源的委托策略的最大大小	40000 个字符

握手的过期时间

以下是中握手的超时时间。 AWS Organizations

邀请加入组织	15 天
请求启用组织中的所有功能	90 天
握手将被删除，不再显示在列表中	握手完成后 30 天

可附加到实体的策略数

最小值和最大值取决于策略类型以及您要将策略附加到的实体。下表显示了各种策略类型以及可将每种类型附加到的实体数。

> **Note**
>
> 这些数字仅适用于那些直接附加到 OU 或账户的策略。通过继承影响 OU 或账户的策略不计入这些限制。

策略类型	附加到实体的数量上限	附加到根的数量上限	每个 OU 附加的数量上限	每个账户附加的数量上限
服务控制策略	1 – 每个实体始终必须至少附加一个 SCP。您无法从实体上删除最后一个 SCP。	5	5	5
AI 服务选择退出策略	0	5	5	5
备份策略	0	10	10	10
标签策略	0	10	10	10

> **Note**
>
> 目前，您的组织中只能有一个根。

节流限制

下表按管理类别列出了 AWS Organizations API，并显示了它们在账户和组织层面各自的限制率。

AWS Organizations API	每个账户的限额（速率、突发量）	每个组织的限制（速率、突发）
账户管理		
CloseAccount	.05、1	
CreateAccount, CreateGovCloudAccount	0.1、3	
DescribeAccount	20、30	24、36
DescribeCreateAccountStatus	2、2	2、3
LeaveOrganization	1、1	
ListCreateAccountStatus	5、8	6、10
握手管理		
AcceptHandshake, DescribeHandshake	1、1	
CancelHandshake	2、3	
DeclineHandshake	1、3	
InviteAccountToOrganization	3、5	
ListHandshakesForAccount, ListHandshakesForOrganization	5、8	6、10
组织管理		
CreateOrganization, DeleteOrganization, EnableFullControl	1、1	
CreateOrganizationalUnit, DescribeOrganization	1、2	

AWS Organizations API	每个账户的限额（速率、突发量）	每个组织的限制（速率、突发）
MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit	2、3	
DescribeOrganizationalUnit	2、2	2、3
ListAccounts	8、12	9、15
ListChildren	6、10	7、12
ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent	5、8	6、10
ListRoots	1、2	1、3
ListTagsForResource	10、15	12、18
RemoveAccountFromOrganization	2、2	
TagResource, UntagResource	4、6	
策略管理		
CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy	2、3	
DescribePolicy	2、2	2、3
DisablePolicyType, EnablePolicyType	1、1	
ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy	5、8	6、10
UpdatePolicy	2、3	

AWS Organizations API	每个账户的限额（速率、突发量）	每个组织的限制（速率、突发）
服务管理		
启用AWSServiceAccess、禁用 AWSServiceAccess	1、2	
清单AWSServiceAccess ForOrganization， ListDeleg atedServicesForAccount	1、3	1、4
ListDelegatedAdministrators	5、8	6、10
RegisterDelegatedAdministra tor, DeregisterDelegate dAdministrator	1、2	

可用于 AWS Organizations 的 AWS 托管式策略

此部分介绍向您提供的、可用于管理您的组织的AWS托管式策略。您无法修改或删除 AWS 托管策略，但可以根据需要将其附加到组织中的实体或从这些实体上分离。

可用于 AWS Identity and Access Management（IAM）的 AWS Organizations 托管式策略

IAM 托管式策略由AWS提供和维护。托管式策略为常见任务提供权限，您可以通过将托管式策略附加到相应的 IAM 用户或角色对象来为其分配权限。您无需自己编写该策略，当AWS根据需要更新策略以支持新服务时，您将自动并且立即获得策略更新带来的好处。您可以在 IAM 控制台的 Policies (策略) 页面中查看AWS托管式策略的列表。使用 Filter policies (筛选策略) 下拉菜单，选择 AWS managed (亚马逊云科技托管)。

您可以使用以下托管式策略向组织中的用户授予权限。

策略名称	描述	ARN
AWSOrganizationsFullAccess	提供创建和完全管理组织所需的所有权限。下面的代码段显示了此策略声明的内容： `{ "Version": "2012-10-17", "Statement": [{ "Sid": "AWSOrganizationsFullAccess", "Effect": "Allow", "Action": "organizations:*", "Resource": "*" }, { "Sid": "AWSOrganizationsFullAccessAccount", "Effect": "Allow", "Action": ["account:PutAlternateContact", "account:DeleteAlternateContact", "account:GetAlternateContact", "account:GetContactInformation", "account:PutContactInformation", "account:ListRegions", "account:EnableRegion", "account:DisableRegion"], "Resource": "*" },`	arn: aws: iam:: aws: policy/AWSOrganizationsFullAccess

策略名称	描述	ARN

	{
	"Sid": "AWSOrganizationsFullAccessCreateSLR",
	"Effect": "Allow",
	"Action": "iam:CreateServiceLinkedRole",
	"Resource": "*",
	"Condition": {
	"StringEquals": {
	"iam:AWSServiceName": "organizations.amazonaws.com"
	}
	}
	}
	]
	}	

策略名称	描述	ARN

AWSOrganizationsReadOnlyAccess	提供对组织信息的只读访问权限。它不允许用户进行任何更改。下面的代码段显示了此策略声明的内容：
	
	{
	"Version":"2012-10-17",
	"Statement":[
	{
	"Sid": "AWSOrganizationsReadOnly",
	"Effect":"Allow",
	"Action":[
	"organizations:Describe*",
	"organizations:List*"
	],
	"Resource": "*"
	},
	{
	"Sid": "AWSOrganizationsReadOnlyAccount",
	"Effect":"Allow",
	"Action":[
	"account:GetAlternateContact",
	"account:GetContactInformation",
	"account:ListRegions"
	],
	"Resource": "*"
	}
	]
	}
		arn: aws: iam:: aws: policy/AWSOrganizationsReadOnlyAccess

更新 Organizations AWS托管式策略

下表显示了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）。有关此页面更改的提示，请订阅 AWS Organizations 文档历史记录页面上的 RSS 源。

更改	描述	日期
AWSOrganizationsFullAccess— 更新为包括描述政策声明的Sid元素。	Organizations 为AWSOrganizationsFullAccess 托管策略添加了Sid元素。	2024年2月6日
AWSOrganizationsReadOnlyAccess— 更新为包括描述政策声明的Sid元素。	Organizations 为AWSOrganizationsReadOnlyAccess 托管策略添加了Sid元素。	2024年2月6日
AWSOrganizationsFullAccess— 更新为允许AWS 区域通过 Organizations 控制台启用或禁用所需的账户 API 权限。	Organizations 添加了针对策略的 account:ListRegions 、account:EnableRegion 和 account:DisableRegion 操作，以启用写入访问权限，来启用或禁用账户的区域。	2022 年 12 月 22 日
AWSOrganizationsReadOnlyAccess— 更新为允许AWS 区域通过 Organizations 控制台发布所需的账户 API 权限。	Organizations 添加了针对策略的 account:ListRegions 操作，以启用查看账户区域的访问权限。	2022 年 12 月 22 日
AWSOrganizationsFullAccess— 更新为允许通过 Organizations 控制台添加或编辑账户联系人所需的账户 API 权限。	Organizations 添加了针对策略的 account:GetContactInformation 和 account:PutContactInformation 操作，以启用用于修改账户联系人的写入访问权限。	2022 年 10 月 21 日
AWSOrganizationsReadOnlyAccess— 更新为允许通过 Organizations 控制台查看账户联系人所需的账户 API 权限。	Organizations 添加了针对策略的 account:GetContactInformation 操作，以启用用于查看账户联系人的访问权限。	2022 年 10 月 21 日

更改	描述	日期
AWSOrganizationsFullAccess— 更新为允许创建组织。	Organizations 为策略添加了 `CreateServiceLinkedRole` 权限，以启用创建组织所需的服务相关角色创建权限。权限仅限于创建一个角色，该角色只能由 `organizations.amazonaws.com` 服务使用。	2022 年 8 月 24 日
AWSOrganizationsFullAccess— 更新为允许通过Organizations控制台添加、编辑或删除账户备用联系人所需的账户 API 权限。	Organizations 添加了针对策略的 `account:GetAlternateContact` 、`account:DeleteAlternateContact` 、`account:PutAlternateContact` 操作，以启用用于修改账户备用联系人的写访问权限。	2022 年 2 月 7 日
AWSOrganizationsReadOnlyAccess— 更新为允许通过 Organizations 控制台查看账户备用联系人所需的账户 API 权限。	Organizations 添加了针对策略的 `account:GetAlternateContact` 操作，以启用用于查看账户备用联系人的访问权限。	2022 年 2 月 7 日

AWS Organizations 托管服务控制策略

服务控制策略（SCP）类似于 IAM 权限策略，但它是 AWS Organizations 而非 IAM 的功能。可以使用 SCP 来指定受影响的实体的最大权限数。您可以将 SCP 附加到组织的根、组织单位 (OU) 或账户。您可以创建自己的策略，也可以使用 IAM 定义的策略。您可以在 Organizations 控制台的 Policies (策略) 页面上查看组织中的策略列表。

> **Important**
>
> 每个根、OU 和账户必须始终附加有至少一个 SCP。

策略名称	描述	ARN
已满 AWSAccess	提供 AWS Organizations 管理账户对成员账户的访问权。	arn: aws: organizations:: aws: policy/service_control_ AWSAccess

AWS Organizations 故障排除

如果您在使用 AWS Organizations 时遇到问题，请查询本部分中的相关主题。

主题

排查一般问题

使用此处的信息可帮助您诊断并修复在使用 AWS Organizations 时可能遇到的拒绝访问或其他常见问题。

主题

当我向 AWS Organizations 发出请求时，收到了“access denied”(访问被拒绝) 消息

- 验证您是否具有调用您请求的操作和资源的许可。管理员必须通过将 IAM policy 附加到您的用户、组或角色来授予权限。如果授予这些权限的策略语句包含任何条件 (例如，当日时间或 IP 地址限制)，则您还必须在发送请求时满足这些要求。有关查看或修改适用于用户、组或角色的策略的信息，请参阅《IAM 用户指南》中的使用策略。
- 如果您手动签署 API 请求（不使用 AWS 开发工具包），请验证您已正确签署请求。

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

- 请确认您用于发出请求的 用户或角色具有正确的权限。临时安全凭证权限派生自 用户或角色，因此权限范围仅限于相应 用户或角色的权限。有关临时安全凭证权限的确定方式的更多信息，请参阅《IAM 用户指南》中的控制临时安全凭证的权限。
- 验证您的请求是否采用了正确的签名和适当的格式。有关详细信息，请参阅所选软件开发工具包的工具包文档或《IAM 用户指南》中的使用临时安全凭证以请求对AWS资源的访问权限。
- 验证您的临时安全凭证没有过期。有关更多信息，请参阅《IAM 用户指南》中的请求临时安全凭证。

当我尝试以成员账户身份离开组织或以管理账户身份删除成员账户时，收到“access denied”（拒绝访问）消息

- 要删除成员账户，必须先在此成员账户中启用 IAM 用户访问账单的权限。有关更多信息，请参阅《AWS Billing 用户指南》中的激活对账单和成本管理控制台的访问权。
- 仅当账户拥有作为独立账户运行所需的信息时，才能从组织中删除此账户。当您使用 AWS Organizations 控制台、API 或 AWS CLI 命令在组织中创建账户时，系统不会自动收集此类信息。对于您想用作独立账户的账户，您必须接受 AWS 客户协议，选择支持计划，提供和验证所需联系信息，并提供当前的付款方式。AWS 将使用该付款方式向账户未绑定到组织期间发生的任何可结算（非 AWS 免费套餐）AWS 活动收费。有关更多信息，请参阅成员账户离开组织。

尝试向组织中添加账户时，我收到“quota exceeded (超出限额)”消息

组织存在最大账户数限制。已删除或已关闭的账户会继续计入此配额。

加入邀请也计入组织的最大账户数中。如果受邀账户拒绝邀请、管理账户取消邀请或邀请过期，则撤销此计数。

- 关闭或删除AWS 账户前，请从组织中删除它，以免其继续占用您的配额。
- 有关如何请求增加配额的更多信息，请参阅最大值和最小值。

我在添加或删除账户时收到了一条“此操作需要一段等待期”消息

某些操作需要一段等待期。例如，您无法立即删除新创建的账户。过几天再尝试此操作。如果您在添加和删除账户时遇到有关账户配额的问题，请参阅最大值和最小值来了解有关如何请求提高配额的信息。

尝试向组织中添加账户时，我收到“organization is still initializing”消息

如果您收到此类错误，而且距您创建组织已过了一个多小时，请联系 AWS Support。

当我尝试将账户邀请到我的组织时，收到“Invitations are disabled (邀请被禁用)”消息。

当您启用组织中的所有功能时，会发生这种情况。此操作可能需要一些时间才能完成，并且需要所有成员账户进行响应。在操作完成之前，您无法邀请新账户加入组织。

我所做的更改不总是立即可见

作为全球数据中心的计算机要访问的服务，AWS Organizations 使用称为最终一致性的分布式计算模型。您在 AWS Organizations 中所做的任何更改需要一些时间才会在相关终端节点中可见。它在服务器与服务器之间或复制区域与复制区域之间发送数据需要时间，这会造成一定的延迟。AWS Organizations 也使用缓存来提高性能，但在某些情况下，这可能会增加时间。在之前缓存的数据超时之前，更改可能不可见。

在设计全球应用程序时，需要考虑这些可能的延迟，即使在一个位置所做的更改对另一个位置不是立即可见，也要确保按预期工作。

有关其他某些 AWS 服务如何受此影响的更多信息，请参阅以下资源：

- 《Amazon Redshift 数据库开发人员指南》中的管理数据一致性
- Amazon Simple Storage Service 用户指南中的 Amazon S3 数据一致性模型
- AWS大数据博客中的 Ensuring Consistency When Using Amazon S3 and Amazon Elastic MapReduce for ETL Workflows
- 《Amazon EC2 API 参考》中的 EC2 最终一致性。

排查 AWS Organizations 策略问题

使用此处的信息可帮助您诊断和修复在 AWS Organizations 策略中找到的常见错误。

服务控制策略

AWS Organizations 中的服务控制策略（SCP）与 IAM 策略类似并有共用的语法。此语法以 JavaScript 对象表示法 (JSON) 的规则开头。JSON 描述对象 以及组成对象的名称和值对。IAM 策略语法通过定义有意义的名称和值进行构建，使用策略授予权限的AWS服务可以理解这些名称和值。

AWS Organizations 使用部分 IAM 句法和语法。有关详细信息，请参阅 SCP 语法。

常见策略错误

- 多个策略对象
- 多个 Statement 元素
- 策略文档超出最大大小

多个策略对象

一个 SCP 必须包含一个并且只能包含一个 JSON 对象。可通过在两旁放置 { } 括号来表示对象。虽然您可以通过在外部对中嵌入额外 { } 括号在 JSON 对象中嵌套其他对象，但是一个策略只能包含一个最外层的 { } 括号对。以下示例不正确，因为它在顶层包含两个对象 (以##标示)：

```
{
  "Version": "2012-10-17",
  "Statement":
  {
     "Effect":"Allow",
     "Action":"ec2:Describe*",
     "Resource":"*"
  }
}
{
  "Statement": {
     "Effect": "Deny",
     "Action": "s3:*",
     "Resource": "*"
  }
}
```

不过，您可以使用正确的策略语法来实现上面示例的意图。可以将两个数据块合并到单个 Statement 元素中，而不是包含两个完整的策略对象 (每个都有自己的 Statement 元素)。Statement 元素将两个对象组成的数组作为其值，如以下示例所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
```

```
      "Resource":" *"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

无法将此示例进一步压缩到带一个元素的 Statement 中，因为两个元素具有不同的作用。通常，您只能在每个语句中的 Effect 和 Resource 元素相同时组合语句。

多个 Statement 元素

此错误乍一看似乎是由上一部分中的错误变化而来的。但是，它在句法上是不同类型的错误。在以下示例中，顶层只有一个策略对象，由单个 { } 括号对表示。但是，该对象包含两个 Statement 元素。

一个 SCP 策略只能包含一个 Statement 元素，名称 (Statement) 在冒号左侧，它的值在冒号右侧。Statement 元素的值必须是对象，以 { } 括号表示，其中包含一个 Effect 元素、一个 Action 元素和一个 Resource 元素。以下示例不正确，因为它在策略对象中包含两个 Statement 元素：

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

因为值对象可以是多个值对象组成的数组，所以您可以通过将两个 Statement 元素合并为一个对象数组元素来解决此问题，如以下示例所示：

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

```
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
 ]
}
```

Statement 元素的值是对象数组。此示例中的数组包含两个对象，每个对象是 Statement 元素的正确值。数组中的每个对象之间用逗号隔开。

策略文档超出最大大小

SCP 文档的最大大小为 5,120 个字符。此最大大小包括所有字符，含空格。要减小 SCP 的大小，您可以删除引号之外的所有空格字符（如空格和换行符）。

通过提出 HTTP 查询请求来调用 API

本部分包含有关使用适用于 AWS Organizations 的查询 API 的常规信息。有关 API 操作和错误的详细信息，请参阅 AWS Organizations API 参考。

> **Note**
>
> 您可以使用 AWS 开发工具包之一，代替对 AWS Organizations 查询 API 进行直接调用。AWS 开发工具包中包含适用于各种编程语言和平台（Java、Ruby、.NET、iOS、Android 等）的库和示例代码。开发工具包提供便捷的方式来创建对 AWS Organizations 和 AWS 的编程访问。例如，软件开发工具包执行以下类似任务：加密签署请求、管理错误以及自动重试请求。有关 AWS 开发工具包的信息（包括如何下载及安装），请参阅适用于 Amazon Web Services 的工具。

使用适用于 AWS Organizations 的查询 API 可以调用服务操作。查询 API 请求是 HTTPS 请求，必须包含 `Action` 参数，以指示要执行的操作。AWS Organizations 支持所有操作的 GET 和 POST 请求。也就是说，API 不要求您使用某些操作的 GET 请求和其他操作的 POST 请求。然而，GET 请求受 URL 的大小限制。尽管此限制与浏览器相关，不过通常为 2048 字节。因此，对于要求更高的查询 API 请求，您必须使用 POST 请求。

响应是 XML 文档。有关响应的详细信息，请参阅 AWS Organizations API 参考中的各个操作页面。

主题

端点

AWS Organizations 有一个在美国东部（弗吉尼亚北部）区域托管的全局 API 终端节点。

有关所有服务的AWS终端节点和区域的更多信息，请参阅中的区域终端节点AWS 一般参考。

必须使用 HTTPS

由于查询 API 返回安全凭证等敏感信息，必须使用 HTTPS 对所有 API 请求加密。

签署 AWS Organizations API 请求

必须使用访问密钥 ID 和秘密访问密钥签署请求。我们强烈建议您不要使用 AWS 账户根用户 凭证处理日常的 AWS Organizations 工作。您可以使用用户或角色的凭证。

要对您的 API 请求进行签名，您必须使用 AWS 签名版本 4。有关 Signature Version 4 的信息，请参阅《IAM 用户指南》中的签署 AWS API 请求。

AWS Organizations 不支持早期版本，例如签名版本 2。

有关更多信息，请参阅下列内容：

- AWS 安全凭证：提供有关可用于访问 AWS 的凭证类型的一般信息。
- IAM 中的安全最佳实践：提供有关使用 IAM 服务的建议，以帮助您保护您的 AWS 资源，包括 AWS Organizations 中的资源。
- IAM 中的临时安全凭证：说明如何创建和使用临时安全凭证。

AWS Organizations 的文档历史记录

下表介绍了 AWS Organizations 的主要文档更新。

- API 版本：2016-11-28

变更	说明	日期
更新的政策声明	为AWS Organizations托管策略声明添加了新Sid元素。	2024年2月6日
新的结算管理账户主题	添加了指向注意事项和详细步骤的链接，这些步骤介绍了如何关闭管理账户。	2024年2月1日
更新了最佳实践	在最佳实践部分增加了新信息，以帮助确保与 IAM 最佳实践保持一致。	2023 年 6 月 12 日
更新了 AWSOrganizationsFullAccess 和 AWSOrganizationsReadOnlyAccess托管策略	两个托管策略均已更新，以启用对账户联系人的写入或读取访问。	2022 年 10 月 21 日
更新了 AWSOrganizationsFullAccess 托管策略	更新了托管式策略，以允许通过添加创建新组织需要的服务相关角色时所需的权限来创建组织。	2022 年 8 月 24 日
Organizations 从 AWS Organizations 控制台关闭账户功能	管理账户中的主体可以从 AWS Organizations 控制台关闭成员账户，并使用 IAM 策略保护成员账户免遭意外关闭。	2022 年 3 月 29 日
将公告更新为可以使用 AWS Organizations 控制台更新备用联系人	Organizations 现在可以通过 AWS Organizations控制台为组织内的账户更新备用联系人。	2022 年 2 月 8 日

	宣布账户管理参考中的新功能和要点以供说明。	
Organizations 托管策略更新 - 对现有策略的更新	更新了 AWSOrganizationsFullAccess 和 AWSOrganizationsReadOnlyAccess 托管政策，允许通过AWS Organizations控制台更新或查看账户备用联系人所需的账户 API 权限。	2022 年 2 月 7 日
组织与 Amazon DevOps Guru 集成	您可以将 Amazon DevOps Guru AWS Organizations 与集成，全面监控所有组织账户的应用程序运行状况并获得见解。	2022 年 1 月 3 日
Organizations 与 Amazon Detective 的集成	您可以将 Amazon Detective 与 AWS Organizations 集成，以确保可以通过 Detective 行为图了解所有组织账户的活动。	2021 年 12 月 16 日
Organizations 与 AWS Config 的集成现在支持多账户多区域数据聚合。	您可以使用委托管理员账户聚合组织所有成员账户中的资源配置和合规性数据。有关更多信息，请参阅《AWS Config 开发人员指南》中的多账户多区域数据聚合。	2021 年 6 月 16 日
Organizations 与 AWS Firewall Manager 的集成现在支持委托管理员	现在，您可以将组织中的某个成员账户指定为整个组织的 Firewall Manager 管理员。这样可以更好地将权限与组织的管理账户分离开来。	2021 年 4 月 30 日
Organizations 备份策略现在支持持续备份	您可以使用 AWS Backup 持续备份功能与组织的备份策略一起使用。	2021 年 3 月 10 日

Organizations 与 AWS CloudFormation StackSets 的集成现在支持委托管理员	现在，您可以将组织中的一个成员帐户指定为整个组织的AWS CloudFormation StackSets管理员。这样可以更好地将权限与组织的管理账户分离开来。	2021 年 2 月 18 日
启用所有功能时继续邀请账户	AWS更新了启用组织中的所有功能的流程。您现在可以继续邀请新账户加入您的组织，同时等待现有账户对其邀请作出响应。	2021 年 2 月 3 日
推出 AWS Organizations 控制台的 2.0 版本	AWS推出了一个新版本的AWS控制台。所有文档都已更新，以反映执行任务的新方式。	2021 年 1 月 21 日
Organizations 现在支持与 AWS Marketplace 的集成	您现在可以启用 AWS Marketplace，以便在组织中的所有账户中更轻松地共享您的软件许可证。	2020 年 12 月 3 日
Organizations 现支持与 Amazon S3 Lens 的集成	Amazon S3 Lens 既支持信任访问权限，也支持 Organizations 中的委托管理员。有关详细信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon S3 Storage Lens。	2020 年 11 月 18 日
跨账户备份副本	当您使用备份策略备份组织中的资源时，您现在可以将备份副本存储在组织中的其他AWS账户内。	2020 年 11 月 18 日

中国的 AWS 区域 现在支持将 AWS Resource Access Manager 作为 Organizations 信任的服务	现在，当您在中国使用 Organizations 和 AWS RAM 时，您可以将与 Organizations 集成的 AWS RAM 功能作为信任服务使用。	2020 年 11 月 18 日
Organizations 现在支持与 AWS Security Hub 的集成	您可以在组织中的所有账户中启用 Security Hub，并将组织的一个成员账户指定为 Security Hub 的委托管理员账户。	2020 年 11 月 12 日
已重命名主账户	AWS Organizations 将“主账户”的名称更改为“管理账户”。此次只更新了名称，功能上没有任何变化。	2020 年 10 月 20 日
新的最佳实践部分和主题	新增了有关 AWS Organizations 最佳实践的部分。新部分包括一些主题，讨论管理账户和成员账户根用户和密码管理的最佳实践。	2020 年 10 月 6 日
添加了新的最佳实践部分和前两页	新增了一个部分，其中介绍了一些描述 AWS Organizations 的主题。此更新包括组织管理账户的最佳实践主题和成员账户的最佳实践主题。	2020 年 10 月 2 日

Organizations 备份策略现在支持使用 VSS（卷影复制服务）在 Windows EC2 实例上进行应用程序一致性备份	备份策略支持新的“advanced_backup_settings ”部分。这个新部分的第一个条目是名为 WindowsVSS 的 ec2 设置，该设置可以启用或禁用。有关详细信息，请参阅《AWS Backup 开发人员指南》中的创建启用 VSS 的 Windows 备份。	2020 年 9 月 24 日
Organizations 支持 tag-on-create 和基于标签的访问控制	您可以在创建 Organizations 资源时为它们添加标签。您可以使用标签策略标准化 Organizations 资源上的标签使用情况。您可以使用 IAM 策略来限制仅访问具有指定标签键和值的资源。	2020 年 9 月 15 日
添加了 AWS Health 作为信任的服务。	您可以聚合组织中账户的 AWS Health 事件。	2020 年 8 月 4 日
人工智能 (AI) 服务选择退出策略	您可以使用 AI 服务选择退出策略来控制 AWS AI 服务是否可以存储和使用通过这些服务处理的客户内容（AI 内容），以促进 AWS AI 服务和技术的发展和持续改进。	2020 年 7 月 8 日
添加了备份策略以及与 AWS Backup 的集成	可以使用备份策略为组织中的所有账户创建和强制执行备份策略。	2020 年 6 月 24 日
支持 IAM 访问分析器的委托管理	使您能够将组织中的访问分析器的管理访问权限委派给指定的成员账户。	2020 年 3 月 30 日

与 AWS CloudFormation 集成 StackSets	您可以创建服务托管的堆栈集，以将堆栈实例部署到由 AWS Organizations 管理的账户。	2020 年 2 月 11 日
与 Compute Optimizer 集成	Compute Optimizer 已添加为可用于组织账户的服务。	2020 年 2 月 4 日
标签策略	您可以使用标签策略帮助在组织账户中跨资源标准化标签。	2019 年 11 月 26 日
与 Systems Manager 集成	您可以在 Systems Manager Explorer 中跨组织中的所有AWS 账户同步操作数据。	2019 年 11 月 26 日
aws：PrincipalOrgPaths	新的全局条件键检查发出请求的 IAM 用户、IAM 角色或AWS 账户根用户的 AWS Organizations 路径。	2019 年 11 月 20 日
与 AWS Config 规则集成	您可以使用 AWS Config API 操作跨组织中的所有AWS 账户来管理 AWS Config 规则。	2019 年 7 月 8 日
新增的可信访问服务	将 Service Quotas 作为可用于组织账户的服务添加。	2019 年 6 月 24 日
与 AWS Control Tower 集成	将 AWS Control Tower 作为可用于组织账户的服务添加。	2019 年 6 月 24 日
与 AWS Identity and Access Management 集成	IAM 为您的组织实体（组织根、OU 和账户）提供服务上次访问数据。您可以使用此数据，将访问限制为仅您需要的 AWS 服务。	2019 年 6 月 20 日
标记账户	您可标记和取消标记组织中的账户，以及查看组织中账户上的标签。	2019 年 6 月 6 日

服务控制策略（SCP）中的资源、条件和 NotAction 元素	现在，您可以指定 SCP 中的资源、条件和 NotAction 元素以拒绝跨组织或组织部门 (OU) 中账户的访问。	2019 年 3 月 25 日
新增的可信访问服务	将 AWS License Manager 和 Service Catalog 添加为可用于组织中的账户的服务。	2018 年 12 月 21 日
新增的可信访问服务	将 AWS CloudTrail 和 AWS RAM 作为可用于组织账户的服务添加。	2018 年 12 月 4 日
新增的可信访问服务	将 AWS Directory Service 作为可用于组织账户的服务添加。	2018 年 9 月 25 日
电子邮件地址验证	您必须先验证您拥有与管理账户关联的电子邮件地址，然后才能邀请现有账户加入您的组织。	2018 年 9 月 20 日
CreateAccount 通知	CreateAccount 通知会发布到管理账户的 CloudTrail 日志中。	2018 年 6 月 28 日
新增的可信访问服务	将 AWS Artifact 作为可用于组织账户的服务添加。	2018 年 6 月 20 日
新增的可信访问服务	将 AWS Config 和 AWS Firewall Manager 作为可用于组织账户的服务添加。	2018 年 4 月 18 日
可信服务访问	您现在可允许或禁止对要在组织账户中运行的精选 AWS 服务的访问。IAM Identity Center 是最初受支持的可信服务。	2018 年 3 月 29 日

账户删除现在是自助服务	您现在可以删除在 AWS Organizations 内创建的账户，无需联系 AWS Support。	2017 年 12 月 19 日
增加了对新服务 AWS IAM Identity Center 的支持	AWS Organizations 现在支持与 AWS IAM Identity Center (IAM Identity Center) 集成。	2017 年 12 月 7 日
AWS 为所有组织账户添加了服务相关角色	名为 `AWSServiceRoleForOrganizations` 的服务相关角色已添加到组织中的所有账户，以实现 AWS Organizations 与其他 AWS 服务之间的集成。	2017 年 10 月 11 日
您现在可以删除已创建的账户	客户现在可以在 AWS Support 的帮助下从其组织中删除已创建的账户。	2017 年 6 月 15 日
服务启动	新服务推出时随附的初始 AWS Organizations 文档版本。	2017 年 2 月 17 日

AWS 术语表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 词汇表。

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。