Amazon Organizations

用户指南

Amazon Organizations: 用户指南

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅中国的 Amazon Web Services 服务入门。

Table of Contents

什么是 Amazon Organizations？

Amazon Organizations 是一项账户 (p. 5)管理服务，可将多个 Amazon Web Services 账户 整合到您创建并集中管理的组织中。Amazon 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 Amazon 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

Amazon Organizations 功能

Amazon Organizations 提供以下功能：

集中管理您的所有 Amazon Web Services 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 Amazon 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 Amazon 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。

与其他 Amazon 服务集成

> 您可以将 Amazon Organizations 中提供的多账户管理服务与选定 Amazon 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，请参阅可与 Amazon Organizations 一起使用的 Amazon 服务 (p. 71)。
>
> 当您启用某个Amazon服务代表您执行组织成员账户中的任务时，Amazon 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Amazon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 Amazon Organizations 服务创建您启用了信任访问权限的Amazon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 Amazon Organizations 与其他 Amazon 产品结合使用 (p. 68)。

全局访问

Amazon Organizations 是一项全局服务，具有单个终端节点，可从任何和所有Amazon Web Services 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 Amazon 服务一样，Amazon Organizations 具有最终一致性。Amazon Organizations 通过复制其区域内 Amazon 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 (p. 130)。

免费使用

Amazon Organizations 是为您的Amazon Web Services 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Amazon服务时，才会向您收费。有关其他Amazon产品定价信息，请参阅亚马逊云科技定价页。

Amazon Organizations 定价

不另外收取 Amazon Organizations 费用。您只需为成员账户中的用户和角色所使用的 Amazon 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Amazon服务定价的信息，请参阅Amazon定价。

访问 Amazon Organizations

您可以通过以下任何方式使用 Amazon Organizations:

Amazon Web Services Management Console

Amazon 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 Amazon 资源。您可以使用控制台在组织中执行任何任务。

Amazon 命令行工具

使用 Amazon 命令行工具，您可在系统的命令行中发出命令以执行 Amazon Organizations 和 Amazon 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 Amazon 任务的脚本，命令行工具也会十分有用。

Amazon 提供两组命令行工具：

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

Amazon 开发工具包

Amazon 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 Amazon 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。

Amazon Organizations HTTPS 查询 API

Amazon Organizations HTTPS 查询 API 使您能够以编程方式访问 Amazon Organizations 和 Amazon。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 Amazon Organizations API 参考。

对 Amazon 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 Amazon Organizations 支持论坛上发布反馈和问题。有关 Amazon 支持论坛的更多信息，请参阅论坛帮助。

其他 Amazon 资源

- Amazon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Amazon技能并获得实践经验。
- Amazon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Amazon构建创新应用程序的其他信息。
- Amazon Web Services Support Center – 用于创建和管理 Amazon 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 Amazon Trusted Advisor。
- Amazon Support – 提供有关 Amazon 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Amazon账单、账户、事件、滥用和其他问题的中央联系点。
- Amazon 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。

开始使用 Amazon Organizations

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

了解...

Amazon Organizations 术语和概念 (p. 4)

学习了解 Amazon 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。

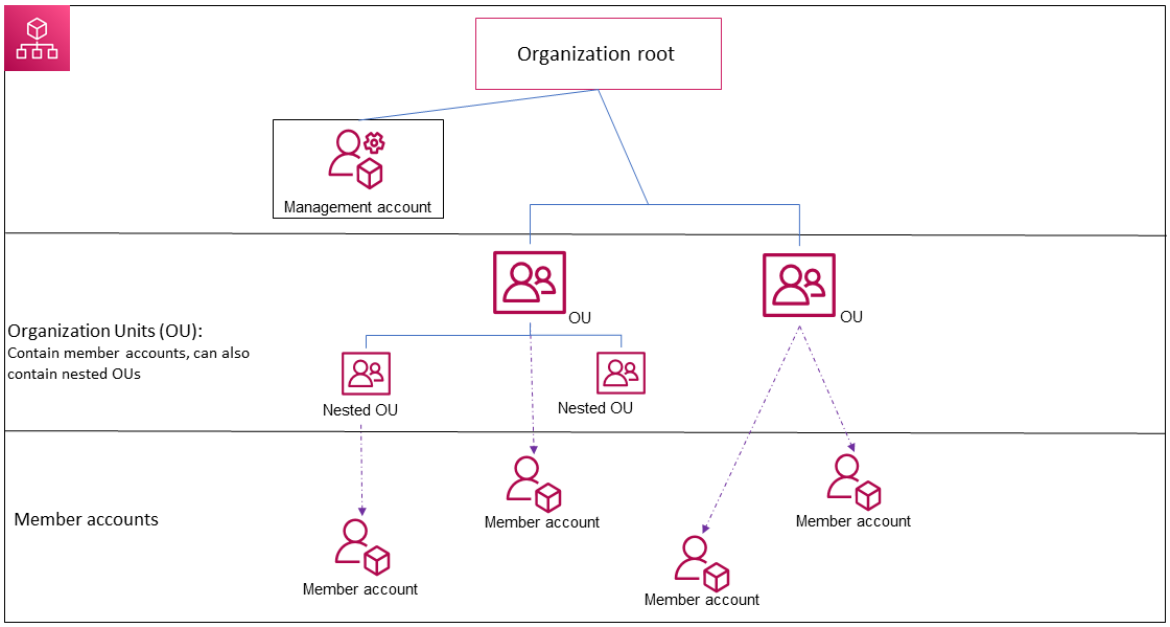
组织的整合账单

Amazon 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《Amazon Billing 用户指南》中。

Amazon Organizations 术语和概念

为了帮助您开始使用 Amazon 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。



组织

您为合并 Amazon 账户 (p. 5)（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 Amazon 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 (p. 5)放在树顶部，组织部门 (p. 5)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 (p. 5)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) (p. 5) 和账户 (p. 5)。

Note

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

组织部门（OU）

根 (p. 5)中账户 (p. 5)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Amazon Web Services 账户，其中包含您的Amazon资源以及可以访问这些资源的身份。

Tip

Amazon 账户与用户账户并非同一账户。Amazon用户是您使用 Amazon 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Amazon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
  - 管理邀请
  - 启用与支持的Amazon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。

邀请

邀请其他账户 (p. 5)加入您的组织 (p. 4)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 (p. 6)功能更改为支持组织中的所有功能 (p. 5)，也可以将邀请发送到所有成员。通过交换握手 (p. 5)信息，对各个账户发出邀请。在 Amazon Organizations 控制台中处理时，您可能看不到握手。但是，如果您使用 Amazon CLI 或 Amazon 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 Amazon Organizations 中的一项主要用途就是作为邀请 (p. 5)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 (p. 6)功能更改为支持 提供的 (p. 5)所有功能Amazon Organizations时，也可以使用握手。仅当您使用 Amazon Organizations API 或命令行工具（如 Amazon CLI）时，您通常需要直接与握手交互。

可用的功能集

- 所有功能 – Amazon 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。此外，您还可以启用与支持的 Amazon 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 Amazon Organizations 的更多高级功能。例如，您无法让与组织集成的其他Amazon服务在组织内的所有账户中运作，。要使用高级 Amazon Organizations 功能，您必须启用组织中的所有功能 (p. 5)。

Amazon Organizations 教程

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

教程：创建和配置组织 (p. 7)

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，并创建包含账户的 OU 层次结构。

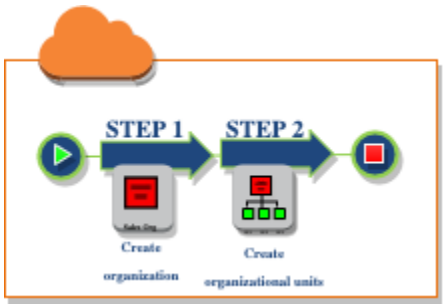
教程：使用 CloudWatch Events 监控组织的重要更改 (p. 11)

配置 Amazon CloudWatch Events，当组织中发生您指定的操作时，触发电子邮件、短信或日志条目形式的警报，监控组织中的重要更改。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 Amazon 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。

下图演示了本教程的主要步骤。



步骤 1：创建组织 (p. 8)

在此步骤中，您将使用现有的Amazon Web Services 账户作为管理账户来创建组织。您还将邀请一个 Amazon Web Services 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 (p. 9)

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。

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

Prerequisites

本教程假设您有权访问两个现有的Amazon Web Services 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。

Amazon Web Services Management Console

1. 以账户 111111111111 的管理员身份登录Amazon，并打开 Amazon 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 (p. 6)。

   Amazon创建组织，并向您显示Amazon Web Services 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Amazon Web Services 账户。

   如果您使用的账户使用未经过Amazon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 (p. 22)。

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。

Amazon Web Services Management Console

邀请现有账户加入

1. 导航到Amazon Web Services 账户页面，然后选择 Add an Amazon Web Services 账户 (添加亚马逊云科技账户)。
2. 在 Add an Amazon Web Services 账户 (添加亚马逊云科技账户) 页面上，选择 Invite an exisiting Amazon Web Services 账户 (邀请现有亚马逊云科技账户)。
3. 在 Email address or account ID of an Amazon Web Services 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 Amazon Web Services 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)。Amazon Organizations 向账户拥有者发送邀请。

   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 Amazon 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Amazon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 Amazon Organizations 控制台 并导航到 Invitations (邀请) 页面。

7. 在Amazon Web Services 账户页面上，选择 Accept (接受)，然后选择 Confirm (确认)。
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Amazon Web Services 账户。在本教程中，我们将此账户称为 333333333333。

Amazon Web Services Management Console

创建成员账户

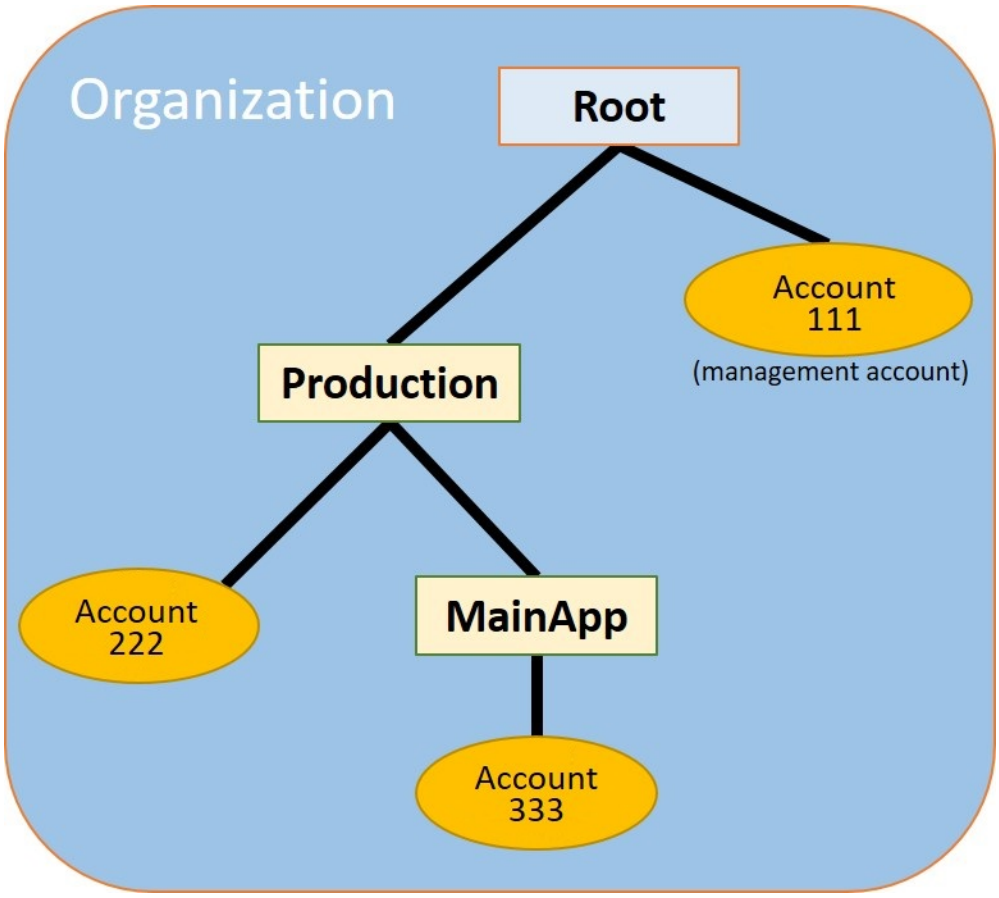
1. 在 Amazon Organizations 控制台的Amazon Web Services 账户页面上，选择 Add Amazon Web Services 账户 (添加亚马逊云科技账户)。
2. 在 Add an Amazon Web Services 账户 (添加亚马逊云科技账户) 页面上，选择 Create an Amazon Web Services 账户 (创建亚马逊云科技账户)。
3. 对于 Amazon Web Services 账户 name (亚马逊云科技账户名称)，输入账户的名称，例如 **`MainApp Account`**。
4. 对于 Email address 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 Amazon Organizations 创建具有默认名称的角色。
6. 选择 Create Amazon Web Services 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Amazon Web Services 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 Amazon 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。



Amazon Web Services 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 Amazon Organizations 控制台中，导航到Amazon Web Services 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 Amazon Web Services 账户（Amazon Web Services 账户）页面，然后选择 Production OU 旁边的三角形 ▶，从而展开它的树形图。

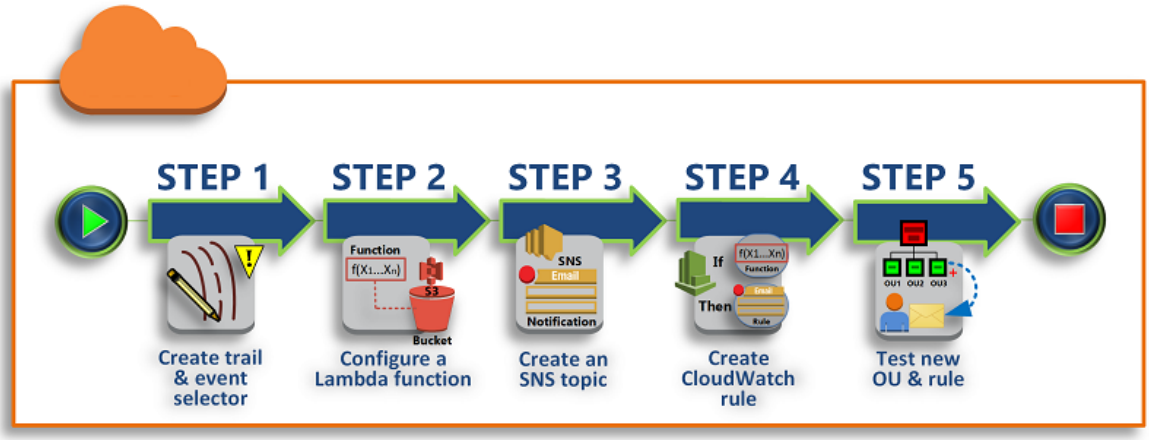
   这将 MainAppOU 显示为 Production (生产) 的子级。

9. 选中复选框 ☑（而不是其名称），选择 Actions (操作)，然后在Amazon Web Services 账户下选择 Move (移动)。
10. 在 Move Amazon Web Services 账户 '***member-account-name***' (移动亚马逊云科技账户“member-account-name”) 页面上，选择单选按钮 ◉（而不是其名称），然后选择 Move Amazon Web Services 账户 (移动亚马逊云科技账户)。
11. 选中复选框 ☑（而不是其名称），选择 Actions (操作)，然后在Amazon Web Services 账户下选择 Move (移动)。
12. 在 Move Amazon Web Services 账户 '***member-account-name***' (移动亚马逊云科技账户“member-account-name”) 对话框中，使用 Production (生产) 旁边的三角来展开该分支并公开MainApp。
13. 选择单选按钮 ◉（而不是其名称），然后在Amazon Web Services 账户中选择 Move Amazon Web Services 账户 (移动亚马逊云科技账户)。

教程：使用 CloudWatch Events 监控组织的重要更改

本教程介绍如何配置 CloudWatch Events，以监控对组织进行的更改。首先，学会配置一条规则，当用户调用特定 Amazon Organizations 操作时即触发该规则。然后，您可将 CloudWatch Events 配置为触发规则后运行 Amazon 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 (p. 12)

在 中创建称为跟踪Amazon 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 (p. 13)

创建 Amazon 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 (p. 14)

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 CloudWatch Events 规则 (p. 14)

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

步骤 5：测试您的 CloudWatch Events 规则 (p. 15)

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。

Tip

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 Amazon Organizations 中将 Amazon CloudTrail 和 CloudWatch Events 结合使用的更多信息，请参阅Amazon Organizations 中的日志记录和监控 (p. 117)。

Prerequisites

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 Amazon Web Services Management Console。IAM 用户必须有权在 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 CloudWatch 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，Amazon 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 Amazon Web Services 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 Amazon 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 CloudWatch Events 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Amazon，然后通过 https://console.amazonaws.cn/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，Amazon Organizations 不会在 CloudWatch Events 配置设置中作为一个选项出现，CloudTrail 也不会捕获 Amazon Organizations 的相关信息。
3. 在导航窗格中，选择 Trails。
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：
   - 如果您已有一个存储桶，选择 Create a new S3 bucket (创建新存储桶) 旁边的 No (否)，然后从 S3 bucket (S3 存储桶) 列表中选择存储桶名称。
   - 如果您需要创建存储桶，请选择 Create a new S3 bucket (创建新存储桶) 旁边的 Yes (是)，然后在 S3 bucket (S3 存储桶) 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。
7. 选择创建。
8. 选择您刚刚创建的 `My-Test-Trail` 跟踪。
9. 选择 Management events 旁边的铅笔图标。
10. 对于 Read/Write events，依次选择 All、Save、Configure。

如果警报规则匹配传入的 API 调用，CloudWatch Events 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 CloudWatch Events 规则发送给函数。

创建记录 CloudWatch Events 事件的 Lambda 函数

1. 从 Amazon Lambda 打开 https://console.amazonaws.cn/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 a function (创建函数)。
3. 在 Create function (创建函数) 页面上，选择 Blueprints (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 custom role (创建自定义角色)，然后在 Amazon Lambda requires access to your resources (Amazon Lambda 需要访问您的资源) 页面底部，选择 Allow (允许)。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。
   c. 选择创建函数。
7. 在下一页上，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. 选择保存。

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 CloudWatch Events 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.amazonaws.cn/sns/v3/ 打开 Amazon SNS 控制台。
2. 在导航窗格中，选择 Topics。
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 Create topic (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 Create subscription。
   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)。Amazon 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 CloudWatch Events 规则

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

要创建 CloudWatch Events 规则

1. 从 https://console.amazonaws.cn/cloudwatch/ 打开 CloudWatch 控制台。
2. 和以前一样，您必须将控制台设置为美国东部（弗吉尼亚北部）区域，或有关 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. 在导航窗格中，选择 Rules (规则)，然后选择 Create rule (创建规则)。
4. 对于 Event source (事件源)，执行以下操作：
   a. 选择 Event pattern。
   b. 选择 Build event pattern to match events by service。
   c. 对于 Service Name，选择 Organizations。
   d. 对于 Event Type (事件类型)，选择 Amazon API Call via CloudTrail (通过 CloudTrail 进行的 Amazon API 调用)。
   e. 选择 Specific operation(s) (特定操作)，然后输入您希望监控的 API：CreateAccount 和 CreateOrganizationalUnit。您还可以选择所需的任何其他内容。有关可用 Amazon Organizations API 的完整列表，请参阅 Amazon Organizations API 参考。
5. 在 Targets (目标) 下，对于 Function (函数)，选择您在上一过程中创建的函数。
6. 在 Targets (目标) 下，选择 Add target (添加目标)。
7. 在新目标行中，选择下拉标题，然后选择 SNS topic (SNS 主题)。
8. 对于 Topic (主题)，选择您在上一过程中创建的名为 OrganizationCloudWatchTopic 的主题。

9. 选择 Configure details。
10. 在 Configure rule details (配置规则详细信息) 页面上，对于 Name (名称)，输入 **`OrgsMonitorRule`**，将 State (状态) 保持选中状态，然后选择 Create rule (创建规则)。

步骤 5：测试您的 CloudWatch Events 规则

在此步骤中，您将创建一个组织部门（OU），然后观察 CloudWatch Events 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。

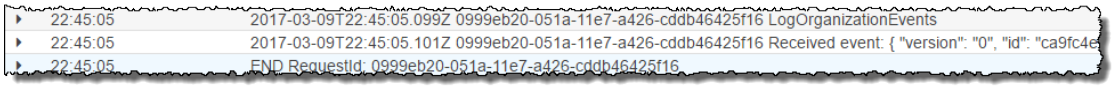
Amazon Web Services Management Console

创建 OU

1. 打开 Amazon Organizations 控制台的Amazon Web Services 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 CloudWatch Events 日志条目

1. 从 https://console.amazonaws.cn/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 Amazon 资源。

清理您的 Amazon 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 CloudWatch 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 CloudWatch Events，以监控对组织的更改。您配置了一条规则，当用户调用特定 Amazon 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。

Amazon Organizations 的最佳实践

在创建和运营组织时，我们建议您遵循以下最佳实践：

主题

管理账户的最佳实践

请遵循以下建议，来帮助保护 Amazon Organizations 中管理账户的安全。

> Note
>
> Amazon Organizations 正在将“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。在我们完成向新术语过渡期间，您可能会继续看到一些旧术语。如果您发现我们有所遗漏，请使用反馈链接告诉我们。

主题

仅将管理账户用于require管理账户的任务

我们建议您仅将管理账户及其用户和角色用于只能由该账户执行的任务。将您的所有Amazon资源存储在组织中的其他Amazon Web Services 账户中，并将它们保留在管理账户之外。唯一的例外是，我们建议您启用Amazon CloudTrail并在管理账户中保留相关的 CloudTrail 跟踪记录和日志。

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。

为管理账户的管理用户使用复杂的密码

- 您账户管理用户的安全性取决于其密码的强度。我们建议您使用长、复杂且未在其他任何地方使用的密码。大量密码管理器和复杂的密码生成算法和工具可帮助您实现这些目标。

为您的管理用户凭证启用 MFA

有关如何启用多重身份验证（MFA）的说明，请参阅在Amazon中使用多重身份验证（MFA）。

- 使用不依赖电池的基于硬件的设备来生成一次性密码（OTP）。这种方法有助于确保 MFA 无法复制，并且在长期存储期间不会出现电池损耗风险
  - 如果您确实使用基于电池的 MFA，请确保添加定期检查设备的流程，并在到期日期临近时进行更换。

  - 创建一个计划，处理需要全天候访问令牌的需求逻辑。
- 强烈建议您不要将物理 MFA 用于保护此管理账户以外的任何其他目的。如果重复使用物理 MFA，它可能会造成操作混乱和不必要的 MFA 暴露。
- 根据您的信息安全策略存储 MFA 设备，但不要与用户的关联密码位于同一位置。确保不同的资源（人员、数据和工具）访问密码的流程和访问 MFA 的流程各采用不同的访问权限。
- 对 MFA 设备或其存储位置的任何访问都应记录和监视。

将电话号码添加到账户联系信息中

- 虽然有一些针对固定电话、SIP 和移动电话号码的可信攻击载体，但总体而言，这些载体的复杂性远超风险。
- 预置电话号码有多种选项，但我们推荐使用专用 SIM 卡和手机，并长期存放在安全位置。务必要确保负责支付此电话合约移动账单的团队了解该号码的重要性，即使该号码在很长时间内不会发送或接收任何电话。
- 重要的是，这个电话号码在企业内不为人所知。将该号码记录在Amazon联系信息控制台页面，并与您的账单团队共享其详细信息。不要将其记录在其他任何地方。这种方法有助于降低将与 SIM 卡绑定的电话号码移动到另一个 SIM 卡相关的攻击载体的风险。
- 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。
- 对电话或其存储位置的任何访问都应记录和监视。

查看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，请定期审查您企业中有权访问与其相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。但是，有必要每月或每季度对这些信息进行一次审查，以确保只有正确的人才能访问。

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。

主题

为成员账户管理用户使用复杂的密码

- 您账户的管理用户的安全性取决于其密码的强度。我们建议您使用长、复杂且未在其他任何地方使用的密码。大量密码管理器和复杂的密码生成算法和工具可帮助您实现这些目标。

为您的管理用户凭证启用 MFA

有关如何启用多重身份验证（MFA）的说明，请参阅在Amazon中使用多重身份验证（MFA）。

- 我们建议您使用不依赖电池的基于硬件的设备来生成一次性密码（OTP）。这种方法有助于确保 MFA 无法复制，并且在长期存储期间不会出现电池损耗风险

  - 如果您确实使用基于电池的 MFA，请确保添加定期检查设备的流程，并在到期日期临近时进行更换。
  - 创建一个计划，处理需要全天候访问令牌的需求逻辑。
- 如果您选择使用虚拟 MFA 应用程序，那么与我们针对管理账户管理用户的建议不同 (p. 17)，对于成员账户，您可以为多个成员账户重新使用单个 MFA 设备。您可以通过在虚拟 MFA 应用程序中打印并安全存储用于配置账户的二维码来解决地理限制问题。根据您的信息安全策略，记录二维码的用途，并将其密封并存储在您所在时区内的无障碍保险箱中。然后，当需要在其他地理位置访问时，可以检索二维码的本地副本，并将其用于在新位置配置虚拟 MFA 应用程序。
- 根据您的信息安全策略存储 MFA 设备，但不要与管理用户的关联密码位于同一位置。确保不同的资源（人员、数据和工具）访问密码的流程和访问 MFA 设备的流程各采用不同的步骤。
- 对 MFA 设备或其存储位置的任何访问都应记录和监视。
- 如果您丢失或损坏了 MFA 设备，您可能需要联系客户支持，以便从您的账户中删除 MFA。在执行此操作之前，他们必须验证发出请求的人是否拥有与账户关联的电子邮件地址、电话号码和安全问题。因此，请确保您拥有这些信息，并确保及时更新并安全地存储。

将管理账户的电话号码添加到成员账户联系信息

- 您通常可以依赖组织管理账户中的电话号码 (p. 18)来进行任何关键账户恢复。因此，我们认为，为成员账户的联系信息管理一个单独电话号码是不必要的操作开销。因此，我们建议您添加与管理账户相同的电话号码。无论您使用的号码与管理账户是否相同，请将所用电话号码以及任何活跃安全问题的准确列表保存在与凭证本身类似的安全位置。

查看并跟踪谁有访问权限

- 正如我们为管理账户所建议的 (p. 18)，您应定期审查您企业内有权访问您成员账户中管理用户的电子邮件地址、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。但是，有必要每月或每季度对这些信息进行一次审查，以确保只有正确的人才能访问。

创建和管理组织

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

- 创建组织 (p. 20)。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 (p. 22)。启用所有功能是使用 Amazon 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。
- 查看有关组织的详细信息 (p. 28)。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 (p. 33)。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Amazon Web Services 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Amazon Web Services 账户 (p. 44)。
- 验证您的电子邮件地址后，邀请现有Amazon Web Services 账户 (p. 37)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Amazon Web Services Management Console或者通过使用 Amazon CLI 或其中一个 SDK API。

最小权限

要使用您当前的Amazon Web Services 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`。

Amazon Web Services Management Console

创建 组织

1. 登录到 Amazon Organizations 控制台。您必须以某个 IAM 用户的身份登录或代入组织管理账户中的某个 IAM 角色。
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Amazon Web Services 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）(p. 5)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 (p. 22)。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。

Amazon CLI & Amazon SDKs

创建 组织

您可以使用以下命令之一创建组织：

- Amazon CLI：create-organization

  以下示例创建组织，并使当前已登录的Amazon Web Services 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 Amazon CLI 中所述。

- Amazon 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Amazon组织的Amazon Web Services 账户，请参阅在组织中创建Amazon Web Services 账户 (p. 44)。
- 若要邀请现有账户加入您的组织，请参阅邀请Amazon Web Services 账户加入组织 (p. 36)。

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，Amazon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Amazon Web Services 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 (p. 28)。
- 若要更改与管理账户关联的电子邮件地址，请参阅《Amazon Billing 用户指南》中的管理Amazon Web Services 账户。

Amazon Web Services Management Console

若要重新发送验证请求

1. 登录到 Amazon Organizations 控制台。您必须以某个 IAM 用户的身份登录或代入组织管理账户中的某个 IAM 角色。
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Amazon Web Services 账户加入您的组织。有关更多信息，请参阅邀请Amazon Web Services 账户加入组织 (p. 36)。

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。

启用组织中的所有功能

Amazon Organizations 有两个可用的功能集：

- 所有功能 (p. 5) – 此功能集是使用 Amazon 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 Amazon Organizations 中提供的高级账户管理功能，例如与支持的Amazon服务的集成 (p. 71)。
- 整合账单功能 (p. 6) – 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，Amazon 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Amazon 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。
- Amazon 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 Amazon 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。
- 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。

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

Amazon Web Services 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 Amazon Organizations 控制台。 您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 在 Settings (设置) 页面选择 Begin process (开始流程)。
3. 在 Enable all features (启用所有功能) 页面上，确认您了解在选择 Begin process (开始流程) 进行切换之后便无法再恢复到仅整合账单功能。

   Amazon 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 Amazon 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 Amazon 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)。

Amazon CLI & Amazon 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：

- Amazon 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。

- Amazon SDK：EnableAllFeatures

Notes

- 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。
- 在您发出请求以启用所有功能之后，到所有账户接受或者出现超时的过程中，将自动取消其他账户等待接受的加入组织邀请。在启用所有功能的流程完成之前，您无法发出新邀请。
- 完成启用所有功能的流程之后，您可以再次邀请账户加入组织。该流程没有变化，不过所有邀请中包括信息，让收件人知道接受邀请之后将对其应用所有适用策略。

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 (p. 27)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 Amazon 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

如果您执行以下过程中的步骤，则组织中的管理账户可以在成员账户上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

Amazon Web Services Management Console

同意在组织中启用所有功能的请求

1. 在 Amazon Organizations 控制台处登录到 Amazon Organizations 控制台。 您必须以 IAM 用户身份或采用成员账户中的 IAM 角色登录。
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。

Amazon CLI & Amazon 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。

- Amazon 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"
            }
        ]
    }
}
```

- Amazon 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

Amazon Web Services Management Console

完成流程以启用所有功能

1. 登录到 Amazon Organizations 控制台。 您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
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。

Amazon CLI & Amazon 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。

- Amazon 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"
            }
        ]
    }
}
```

- Amazon SDK：
  - AcceptHandshake
  - AcceptHandshake

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

在 Amazon 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`

Amazon Web Services Management Console

查看组织的详细信息

1. 登录到 Amazon Organizations 控制台。 您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
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。

Amazon CLI & Amazon 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：

- Amazon 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 Amazon CLI 中所述。

- Amazon SDK：DescribeOrganization

查看根的详细信息

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

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Amazon Web Services 账户。

Amazon Web Services Management Console

查看根的详细信息

1. 登录到 Amazon Organizations 控制台。 您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 导航到Amazon Web Services 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。

Amazon CLI & Amazon 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：

- Amazon 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"
                }
            ]
        }
    ]
}
```

- Amazon SDK：ListRoots

查看 OU 的详细信息

在 Amazon 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

Amazon Web Services Management Console

查看 OU 的详细信息

1. 登录到 Amazon Organizations 控制台。 您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。

2. 在Amazon Web Services 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。

Amazon CLI & Amazon 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：

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

以下示例说明如何使用 Amazon 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"
    }
}
```

- Amazon SDK：
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

查看账户的详细信息

在 Amazon 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Amazon Web Services 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

Amazon Web Services Management Console

查看Amazon Web Services 账户的详细信息

1. 登录到 Amazon Organizations 控制台。 您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 导航到Amazon Web Services 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。

Amazon CLI & Amazon SDKs

查看Amazon Web Services 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：

- Amazon 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"
    }
}
```

- Amazon SDK：
  - ListAccounts
  - DescribeAccount

通过删除管理账户来删除组织

当您不再需要组织时，可将其删除。此操作会从组织中移除管理账户，并删除组织本身。先前管理账户将成为独立Amazon Web Services 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 Amazon 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Amazon Web Services 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，请参阅作为成员账户退出组织 (p. 53)。
- 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。这可以阻止您删除组织，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。

最小权限

要删除组织，您必须以管理账户中的 IAM 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

Amazon Web Services Management Console

从组织中移除管理账户并删除组织

1. 登录到 Amazon Organizations 控制台。您必须以某个 IAM 用户的身份登录或代入组织管理账户中的某个 IAM 角色。
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 (p. 51)。
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)。
5. （可选）如果您还希望关闭管理账户，则可以按照关闭Amazon Web Services 账户 (p. 55)中的步骤操作。

Amazon CLI & Amazon SDKs

从组织中移除管理账户并删除组织

您可以使用以下命令之一删除组织：

- Amazon CLI：delete-organization

  以下示例将删除使用其凭证的Amazon Web Services 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。

- Amazon SDK：DeleteOrganization

管理您组织中的Amazon Web Services 账户

组织是您共同管理的Amazon Web Services 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 (p. 32)。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 Amazon Web Services 账户列表 (p. 50)。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Amazon Web Services 账户加入您的组织 (p. 36)。创建邀请、管理您已创建的邀请以及接受或拒绝邀请。
- 创建Amazon Web Services 账户作为您组织的一部分 (p. 44)。创建和访问自动成为您组织一部分的Amazon Web Services 账户。
- 更新您组织中的备用联系人 (p. 47)。更新组织中您的 Amazon Web Services 账户 的备用联系人。
- 从您的组织中删除Amazon Web Services 账户 (p. 51)。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）Amazon Web Services 账户 (p. 55)。您可以关闭不再使用的Amazon Web Services 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 Amazon Web Services 账户有什么影响？ (p. 35)
- 对您在组织中创建的 Amazon Web Services 账户有什么影响？ (p. 36)

对加入组织的Amazon Web Services 账户的影响？

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

- Amazon Organizations 创建名为 的服务相关角色。`AWSServiceRoleForOrganizations (p. 71)`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 Amazon Organizations 将为该账户重新创建该角色。
- 您可以为组织的其他Amazon服务启用服务信任 (p. 71)。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，Amazon Organizations 不会自动创建 IAM 角色 OrganizationAccountAccessRole (p. 48)。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 在受邀成员账户中创建 OrganizationAccountAccessRole (p. 47)。

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Amazon Web Services 账户的影响？

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

- Amazon Organizations 创建名为 的服务相关角色。`AWSServiceRoleForOrganizations (p. 71)`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 Amazon Organizations 将为该账户重新创建该角色。
- Amazon Organizations 会创建 IAM 角色 OrganizationAccountAccessRole (p. 48)。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。
- 如果您为组织启用了对其他 Amazon 服务的服务信任 (p. 71)，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Amazon Web Services 账户加入组织

在创建组织并验证您与管理账户关联的电子邮件地址后，才能邀请现有Amazon Web Services 账户加入您的组织。

您邀请账户时，Amazon Organizations 将向账户所有者发送邀请，该所有者确定接受还是拒绝邀请。您可以使用 Amazon Organizations 控制台启动和管理您发送到其他账户的邀请。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Amazon Web Services 账户的管理员，则还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。

当某个受邀账户加入您的组织时，您不会 自动拥有对该账户的完全管理员控制权限，这不同于已创建的账户。如果您希望管理账户具有对受邀成员账户的完全管理控制权，您必须在成员账户中创建 `OrganizationAccountAccessRole` IAM 角色并将权限授予管理账户以担任该角色。要进行此配置，请在受邀账户成为成员之后，按照在受邀成员账户中创建 OrganizationAccountAccessRole (p. 47)中的步骤操作。

> Note
>
> 当您在您组织中创建账户而不是邀请现有账户加入时，Amazon Organizations 将自动创建一个 IAM 角色（默认情况下，名为 `OrganizationAccountAccessRole`），您可使用该角色为管理账户中的用户授予对已创建账户的管理员访问权限。

Amazon Organizations 会 在受邀成员账户中创建一个服务相关角色以支持 Amazon Organizations 与其他 Amazon 服务之间的集成。有关更多信息，请参阅 Amazon Organizations 和服务相关角色 (p. 71)。

有关每天可以发送的邀请数，请参阅最大值和最小值 (p. 125)。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Amazon Web Services 账户 (p. 44)。

Important

出于法律和账单限制，您只能邀请管理账户所属的Amazon销售商和Amazon分区的Amazon Web Services 账户。例如，在 Amazon EMEA 组织中，你可以同时拥有 Amazon Inc. 和 Amazon Canada 账户。

- 如果您的组织的管理账户是由 Amazon Internet Services Pvt. Ltd (AISPL) 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记录卖家。例如，作为印度的 Amazon 卖家，您只能邀请其他 AISPL 账户加入您的组织。您不能合并来自 AISPL 和 Amazon 或者来自任何其他 Amazon 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Amazon分区。位于商业Amazon Web Services 区域分区的账户不能位于具有来自中国地区分区或 Amazon GovCloud（US）区域分区的账户的组织中。

向Amazon Web Services 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 (p. 22)。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

要邀请Amazon Web Services 账户加入您的组织，您必须拥有以下权限：

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

Amazon Web Services Management Console

邀请其他账户加入组织

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 如果您的电子邮件地址已经过Amazon验证，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 (p. 22)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Amazon Web Services 账户页面，然后选择 Add an Amazon account (添加亚马逊云科技账户)。
4. 在 Add an Amazon Web Services 账户 (添加亚马逊云科技账户) 页面上，选择 Invite an existing Amazon account (邀请现有亚马逊云科技账户)。
5. 在 Invite an existing Amazon（邀请现有亚马逊云科技账户）页面，为 Email address or account ID of the Amazon Web Services 账户 to invite（待邀请的亚马逊云科技账户的电子邮件地址或账户 ID）输入与待邀请账户关联的电子邮件地址或其账户 ID。
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Amazon Web Services 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 Amazon Web Services 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。

   Amazon Organizations 会发送邀请到您邀请加入组织的账户所有者的电子邮件地址。此电子邮件消息包括指向 Amazon Organizations 控制台的链接，账户拥有者在此控制台中可以查看详细信息并选择接受或拒绝邀请。此外，受邀账户的拥有者可以绕过此电子邮件消息，直接转到 Amazon Organizations 控制台，查看邀请并接受或拒绝它。

   对此账户的邀请立即计入组织的最大账户数；Amazon 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。

Amazon CLI & Amazon 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：

- Amazon 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"
    }
}
```

- Amazon SDK：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Amazon Web Services 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`

Amazon Web Services Management Console

查看或取消从您的组织发送到其他账户的邀请

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
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)。

   Amazon 会发送电子邮件消息到账户拥有者，说明您已取消邀请。除非您发送新邀请，否则账户无法再加入组织。

Amazon CLI & Amazon 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：

- Amazon CLI：list-handshakes-for-organization、cancel-handshake
- 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
    }
}
```

- Amazon SDK：ListHandshakesForOrganization、CancelHandshake

接受或拒绝来自组织的邀请

您的Amazon Web Services 账户可能会收到加入某个组织的邀请。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。

最小权限

要接受或拒绝加入 Amazon 组织的邀请，您必须拥有以下权限：

- `organizations:ListHandshakesForAccount` – 在 Amazon Organizations 控制台中查看邀请列表时需要。
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.

Amazon Web Services 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 Amazon 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 用户身份登录受邀账户，或担任 IAM 角色。
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。

     Amazon将发送电子邮件消息到组织概览账户的拥有者，说明您接受了邀请。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。

     Amazon将发送电子邮件消息到组织概览账户的拥有者，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。

Amazon CLI & Amazon 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：

- Amazon 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。

- Amazon SDK：AcceptHandshake、DeclineHandshake

在组织中创建Amazon Web Services 账户

此页面介绍如何在 Amazon Organizations 中您的组织内创建账户。要了解有关Amazon和创建单个Amazon Web Services 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Amazon Web Services 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Amazon Web Services 账户 (p. 45)
- 访问具有管理账户访问权角色的成员账户 (p. 48)

Important

- 当您在组织中创建成员账户时，Amazon Organizations 将自动在成员账户中创建一个 Amazon Identity and Access Management (IAM) 角色 `OrganizationAccountAccessRole`，以允许管理账户中的 IAM 用户对成员账户进行完全管理控制。

  此外，Amazon 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。

  Amazon 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 Amazon 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 Amazon Organizations 和服务相关角色 (p. 71)。

- 如果此组织使用 Amazon Control Tower 进行管理，则稍后使用 Amazon Control Tower 控制台或 API 中的 Amazon 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 Amazon Control Tower 注册。有关更多信息，请参阅《Amazon Control Tower 用户指南》中的引用 Amazon Control Tower 的外部资源。

Note

Amazon Web Services 账户作为组织的一部分创建，不会自动订阅Amazon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Amazon Web Services 账户

登录到组织的管理账户时，您可以创建自动属于组织的成员账户。为此，请完成以下步骤。

使用以下过程创建账户时，Organizations 会自动将管理账户中的以下信息复制到新成员账户中：

- 账户名称
- 电话号码
- 公司名称
- 自定义 URL
- 公司联系电子邮件
- 沟通语言
- Marketplace（某些Amazon Web Services 区域内账户的供应商）

Amazon不会为账户自动收集作为独立账户使用所需的全部信息。如果您需要从组织中删除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 作为成员账户退出组织 (p. 53)。

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）。

Amazon Web Services Management Console

创建自动属于组织的Amazon Web Services 账户

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 在Amazon Web Services 账户页面上，选择 Add an Amazon Web Services 账户 (添加亚马逊云科技账户)。
3. 在 Add an Amazon Web Services 账户（添加 Amazon Web Services 账户）页面上，选择 Create an Amazon Web Services 账户（创建 Amazon Web Services 账户）（默认已选中）。
4. 在 Create an Amazon Web Services 账户（添加 Amazon Web Services 账户）页面上，为 Amazon Web Services 账户 name（Amazon Web Services 账户 名称）输入您想要为此账户分配

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Amazon Web Services 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，Amazon 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 IAM 用户的新账户授予访问权。
7. （可选）在 Add tags (添加标签) 部分中，向新账户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`。您最多可以向账户附加 50 个标签。
8. 选择 Create Amazon Web Services 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 (p. 130)。
   - 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 Amazon 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 Amazon Organizations 中的日志记录和监控 (p. 117)。
   - 如果错误仍然存在，请联系 Amazon Web Services Support。

   此时将显示Amazon Web Services 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，您可以按照访问和管理组织中的成员账户 (p. 47)中的步骤访问账户。

Amazon CLI & Amazon SDKs

创建自动属于组织的Amazon Web Services 账户

您可以使用以下命令之一创建账户：

- Amazon 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"
  }
}
```

- Amazon SDK：CreateAccount

更新您组织中的备用联系人

您可以使用 Amazon Organizations 控制台，或者以编程方式使用 Amazon CLI 或 Amazon 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《Amazon 账户管理参考》中的访问或更新备用联系人。

访问和管理组织中的成员账户

在组织中创建账户时，Amazon 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。我们使用默认名称引用本指南中的角色。Amazon Organizations 不创建任何其他 IAM 用户、组或其他角色。要访问组织中的账户，您必须使用以下方法之一：

- 您在 Amazon Organizations 外部创建的Amazon Web Services 账户包含一个具有对该账户的完全访问权限的 IAM 管理员用户。您可以使用这些凭证登录。
- 如果您通过使用作为 Amazon 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。请参阅访问具有管理账户访问权角色的成员账户 (p. 48)。
- 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 Amazon Organizations 创建的账户中的角色相同。如需创建此角色，请参阅在受邀成员账户中创建 OrganizationAccountAccessRole (p. 47)。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 (p. 48)中的步骤访问它。

  最小权限

  要从组织中的任何其他账户访问Amazon Web Services 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。

在受邀成员账户中创建 OrganizationAccountAccessRole

默认情况下，如果您创建属于组织的成员账户，Amazon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 (p. 48)。

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。

Amazon Web Services Management Console

在成员账户中创建 Amazon Organizations 管理员角色

1. 通过以下网址登录到 IAM 控制台：https://console.aws.amazon.com/iam/。您必须以 IAM 用户身份登录，或者在有权创建 IAM 角色和策略的成员账户中担任 IAM 角色。您可以使用在创建成员账户时为您创建的 IAM 管理员用户。
2. 在 IAM 控制台中，导航至 Roles (角色)，然后选择 Create Role (创建角色)。
3. 选择其他Amazon Web Services 账户。
4. 输入您希望向其授予管理员访问权的管理账户的 12 位账户 ID 编号，并选择 Next: Permissions (下一步：权限)。

   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《IAM 用户指南》中的我何时应使用外部 ID？。
5. 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。有关更多信息，请参阅《IAM 用户指南》中的在Amazon中使用多重身份验证（MFA）。
6. 在附加权限策略页面上，选择名为 `AdministratorAccess` 的 Amazon 托管策略，然后选择下一步：标签。
7. 在 Add tags (optional) (添加标签(可选)) 页面上，选择 Next: Review (下一步: 审核)。
8. 在 Review 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)。
9. 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。
10. 通过以下网址登录到 IAM 控制台：https://console.aws.amazon.com/iam/。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。
11. 导航到 Policies (策略)，然后选择 Create Policy (创建策略)。
12. 对于 Service，选择 STS。
13. 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。
14. 选择 Resources (资源)，确保已选择 Specific (特定)，然后选择 Add ARN (添加 ARN)。
15. 输入Amazon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 Add（添加）。
16. 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。
17. 选择Review policy（查看策略）。
18. 输入新策略的名称，然后选择 Create policy (创建策略) 以保存您的更改。
19. 选择导航窗格中的 Groups (组)，然后选择要用于委派成员账户的管理权限的组的名称（不是复选框）。
20. 请选择 Permissions 选项卡。
21. 选择 Attach Policy (附加策略)，选择您在步骤 11–18 中创建的策略，然后选择 Attach Policy (附加策略)。

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 (p. 48)。

访问具有管理账户访问权角色的成员账户

使用 Amazon Organizations 控制台创建成员账户时，Amazon 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。您可以按照在受邀成员账户中创建 OrganizationAccountAccessRole (p. 47)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。

Amazon Web Services 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Step 11 (p. 49)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 Actions (操作) 部分中，在搜索框键入 **`assume`** 以筛选列表，然后选择 AssumeRole 选项。
5. 在 Resources (资源) 部分中，选择 Specific (特定)，选择 Add ARN to restrict access (添加 ARN 以限制访问)，然后键入成员账号和您在上一部分中创建的角色的名称（我们建议将其命名 `OrganizationAccountAccessRole`）。
6. 当对话框显示正确的 ARN 时，选择 Add (添加)。
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. 选择Review policy（查看策略）。
9. 在 Name (名称) 字段中，输入您的策略名称。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 Groups (组)，然后选择其成员能够代入成员账户中角色的组的名称（不是复选框）。如果需要，您可以创建新组。
12. 在 Permissions (权限) 选项卡上，然后在 Managed Policies (托管策略) 下，选择 Attach policy (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 (p. 49)到Step 10 (p. 49)中创建的策略的名称。还可以筛选出所有Amazon托管式策略，方法是选择 Policy Type (策略类型)，然后选择 Customer Managed (客户托管)。
14. 选中策略旁边的复选框，然后选择 Attach Policy (附加策略)。

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

Amazon Web Services 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 Amazon 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。选择右上角的角色名称（无论您指定什么作为Display Name (显示名称)），然后选择 Back to ***UserName*** (返回到 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》中的向用户授予切换角色的权限。
- 有关使用要担任的您已授予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（Amazon Web Services Management Console）。
- 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：使用 IAM 角色委派跨Amazon Web Services 账户的访问权。
- 有关关闭Amazon Web Services 账户的信息，请参阅关闭Amazon Web Services 账户 (p. 55)。

导出组织的所有 Amazon Web Services 账户详细信息

借助 Amazon 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 Amazon 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 Amazon Web Services 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`（已邀请）、`CREATED`（已创建）或 `ADDED`（已添加）。
- 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`

Amazon Web Services Management Console

将组织中的所有 Amazon Web Services 账户导出到 .csv 文件

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 选择 Actions（操作），然后对于 Amazon Web Services 账户（Amazon Web Services 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。

Amazon CLI & Amazon SDKs

导出包含账户详细信息的 .csv 文件的唯一方法是使用Amazon Web Services Management Console。您不能使用 Amazon 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。此页面介绍了您在删除账户之前需要了解的信息，并提供了删除账户的过程。

有关删除管理账户的信息，请参阅通过删除管理账户来删除组织 (p. 33)。

主题

从组织中删除账户前需知

删除账户之前，您需要了解以下内容：

- 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 Amazon Organizations 控制台、API 或 Amazon 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。Amazon 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Amazon免费套餐）Amazon活动收费。
- 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，Amazon Web Services 账户的拥有者将负责所有新的Amazon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Amazon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。有关如何禁用或更改Amazon服务的委托管理员账户的更多信息，请参阅该服务对应的文档
- 即使在从组织内删除已创建的账户（使用 Amazon 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，请通过 https://aws.amazon.com/contact-us/ 与我们联系。
- 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。

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。
- 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Amazon Web Services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Amazon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。

从组织中删除成员账户

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。这些过程仅适用于成员账户。要移除管理账户，您必须删除组织 (p. 33)。

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 Amazon Artifact 控制台的 Amazon 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 IAM 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`

如果您选择以步骤 6 中成员账户中的 IAM 用户或角色登录，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 IAM 用户必须具有 `aws-portal:ModifyBilling` 和 `aws-portal:ModifyPaymentMethods` 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《Amazon Billing 用户指南》中的激活对账单和成本管理控制台的访问权。

Amazon Web Services Management Console

从组织中删除成员账户

1. 登录到 Amazon Organizations 控制台。您必须以某个 IAM 用户的身份登录或代入组织管理账户中的某个 IAM 角色。
2. 在Amazon Web Services 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 Amazon Web Services 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Amazon Web Services 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Amazon Web Services 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 Amazon 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，Amazon 会自动将您的浏览器重定向至成员账户的 Amazon 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 StartedAmazon 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。

Amazon CLI & Amazon 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：

- Amazon 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。

- Amazon SDK：RemoveAccountFromOrganization

作为成员账户退出组织

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。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。

要删除的账户不得是为组织启用的任何Amazon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。有关如何禁用或更改Amazon服务的委托管理员账户的更多信息，请参阅该服务对应的文档

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 Amazon Artifact 控制台的 Amazon 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。

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。

最小权限

要退出 Amazon 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 IAM 用户必须具有 `aws-portal:ModifyBilling` 和 `aws-portal:ModifyPaymentMethods` 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《Amazon Billing 用户指南》中的激活对账单和成本管理控制台的访问权。

Amazon Web Services Management Console

作为成员账户退出组织

1. 在 Amazon Organizations 控制台处登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或采用成员账户中的 IAM 角色登录。
2. 在 Organizations Dashboard (Organizations 控制面板) 页面上，选择 Leave organization (离开组织)。
3. 执行下列步骤之一：
   - 如果您的账户具有作为独立账户运行所需的全部信息，则将显示一个确认对话框。确认您选择删除账户。系统将您重定向到 控制台的 Getting StartedAmazon 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。
   - 如果您的账户没有所有必需信息，请执行以下步骤：
     a. 这将显示一个对话框，其中说明您必须完成一些额外步骤。单击链接。
     b. 完成提供的所有注册步骤。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. 在出现一个指明注册过程已完成的对话框时，请选择 Leave organization。
     d. 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 StartedAmazon 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。
4. 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。

Amazon CLI & Amazon 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：

- Amazon 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。
- Amazon SDK：LeaveOrganization

关闭Amazon Web Services 账户

本主题仅适用于 Amazon Web Services 账户

要关闭 Amazon.com 购物账户，请参阅 http://www.amazon.com/gp/help/customer/display.html?nodeId=GDK92DNLSGWTV6MP。

如果您的企业中不再需要某个成员账户，并想要确保没有人会使该账户产生费用，您可以遵循本节中的说明从 Amazon Organizations 控制台中关闭此账户。您还可以从 Amazon 账单控制台关闭 Amazon Web Services 账户。要了解更多信息，请参阅《Amazon 账单用户指南》中的 关闭账户。

接着，除了以根用户身份登录查看从前的账单或联系 Amazon Web Services Support 以外，任何 Amazon 活动都不能再使用此账户。有关更多信息，请参阅就您的账单联系客户支持。

关闭账户的影响

当您关闭 Amazon Web Services 账户 时，在账户关闭之前，您应该考虑一些影响。

- 如果关闭账户，将无法重复使用根用户的电子邮件地址。
- 要关闭组织的管理账户，必须首先移除 (p. 52)或关闭组织中的所有成员账户。关闭管理账户时，只要在企业中没有成员账户，就会自动删除企业。
- 如果您使用 Amazon Control Tower，则在尝试关闭账户之前，您需要取消管理账户。请参阅《Amazon Control Tower 用户指南》中的取消管理成员账户。
- 如果您有与 Amazon GovCloud (US) 账户关联的 Amazon Web Services 账户，则在关闭 Amazon GovCloud (US) 账户之前，您需要关闭标准账户。要了解重要的关闭前细节，请参阅《Amazon GovCloud (US) 用户指南》中的 关闭 Amazon GovCloud (US) 账户。

我们推荐的但不是确保安全性所必需的最佳实践：

作为最佳实践，我们建议您根据 授予完成工作所需的最低权限的安全最佳实践，删除对来自 IAM 权限或策略的对已关闭账户的引用。这不是安全问题，因为 Amazon 关闭账户后永远不会重用 ID 号。如果您在 IAM 策略中有已关闭账户的 ID，IAM Access Analyzer 将通知您。

从您关闭账户之时起至 90 天到期：

- 已关闭的账户将在您的企业中显示为“SUSPENDED”（已暂停）状态。
- 如果您决定在 90 天内重新开立账户，在账户关闭前未终止的部分活动资源可能会继续产生费用。有关更多信息，请参阅知识中心中的 如何终止在我的 Amazon Web Services 账户 上不再需要的活动资源？。
- 您将能够登录以查看过去的账单和访问 Amazon Web Services Support。

90 天宽限期到期后：

- 关闭的 Amazon Web Services 账户 在您的企业中不再可见。

关闭Amazon Web Services 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。

Amazon Management Console

关闭Amazon Web Services 账户

Note

或者，您可以关闭来自 Billing and Cost Management 控制台的 Amazon 成员账户。要了解更多信息，请参阅《Amazon 账单用户指南》中的 关闭账户。

1.
2. 在 Amazon Web Services 账户 页面上，选择您想要关闭的成员账户。
3. 在 Account details（账户详细信息）页面上，选择页面顶部的账户名称旁边的 Close（关闭）。
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 Close Account（关闭账户）。

关闭Amazon Web Services 账户后，您无法再使用其访问Amazon服务或资源。有关更多信息，请参阅知识中心内的如何重新打开已关闭的Amazon Web Services 账户？。

Amazon CLI & Amazon SDKs

关闭Amazon Web Services 账户

您可以使用以下命令之一关闭 Amazon 账户：

- Amazon 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。

- Amazon SDK：CloseAccount

保护账户免遭关闭

如果您要保护 Amazon Web Services 账户 免遭意外关闭，您可以创建一个 IAM 策略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 策略：

- 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账户被关闭 (p. 57)。
- 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 (p. 65)。要查看示例，请参阅 防止带标签的账户被关闭 (p. 57)。

防止 Amazon Web Services 账户 关闭的 IAM 策略示例

此类别中的示例

- 防止带标签的账户被关闭 (p. 57)
- 防止本策略中列出的账户被关闭 (p. 57)

防止带标签的账户被关闭

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账户被关闭

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在 Resource 元素中明确指定的账户。

```
{
    "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"
            ]
        }
    ]
}
```

管理组织单元 (OU)

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。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，在您首次设置组织时由 Amazon Organizations 为您创建。

要确定组织中账户的结构，您可以执行以下任务：

- 查看 OU 的详细信息 (p. 30)
- 创建 OU (p. 59)
- 重命名 OU (p. 60)
- 编辑附加到 OU 的标签 (p. 61)
- 将账户移动到 OU 或者在根和 OU 之间移动 (p. 62)

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。

Amazon Web Services Management Console

以“树”视图形式在组织中导航

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 在 Amazon Web Services 账户（Amazon Web Services 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。

Amazon Web Services Management Console

要使用无层次结构的账户平面列表形式查看组织

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 在Amazon Web Services 账户页面上的 Organization (组织) 部分顶部，将 View Amazon Web Services 账户 only (仅限查看亚马逊云科技账户) 切换图标选为 On (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

如果此组织使用 Amazon Control Tower 进行管理，请使用 Amazon Control Tower 控制台或 API 创建 OU。如果您在 Organizations 中创建 OU，则该 OU 未向 Amazon Control Tower 注册。有关更多信息，请参阅《Amazon Control Tower 用户指南》中的引用 Amazon 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`

Amazon Web Services Management Console

创建 OU

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 导航到Amazon Web Services 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Amazon Web Services 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 (p. 58)，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 (p. 62) 或者为其附加策略。

Amazon CLI & Amazon SDKs

创建 OU

您可以使用以下命令之一创建 OU：

- Amazon 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"
    }
}
```

- Amazon SDK：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

要在 Amazon 组织的根中重命名 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:UpdateOrganizationalUnit`

Amazon Web Services Management Console

重命名 OU

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 在 Amazon Web Services 账户（Amazon Web Services 账户）页面，导航到要重命名的 OU (p. 58)，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)。

Amazon CLI & Amazon SDKs

重命名 OU

您可以使用以下命令之一重命名 OU：

- Amazon 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"
    }
}
```

- Amazon SDK：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Amazon组织中根内的 OU 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:DescribeOrganizationalUnit` – 仅当使用 Organizations 控制台时才需要
- `organizations:TagResource`
- `organizations:UntagResource`

Amazon Web Services Management Console

编辑附加到 OU 的标签

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 在 Amazon Web Services 账户（Amazon Web Services 账户）页面上，导航到要编辑其标签的 OU (p. 58) 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)。

Amazon CLI & Amazon 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：

- Amazon 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。
- Amazon SDK：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`

Amazon Web Services Management Console

将账户移动到 OU

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。

2. 在Amazon Web Services 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 Amazon Web Services 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 Amazon Web Services 账户 (亚马逊云科技账户) 下，选择 Move (移动)。
5. 在 Move Amazon Web Services 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 Amazon Web Services 账户 (移动亚马逊云科技账户)。

Amazon CLI & Amazon SDKs

将账户移动到 OU

您可以使用以下命令之一移动账户：

- Amazon CLI：move-account

  以下示例将Amazon Web Services 账户从根移动到 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。
- Amazon SDK：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`

Amazon Web Services Management Console

删除 OU

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 在Amazon Web Services 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)。

Amazon Organizations 将删除 OU 并将其从列表中删除。

Amazon CLI & Amazon SDKs

删除 OU

您可以使用以下命令之一删除 OU：

- Amazon 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。
- Amazon SDK：DeleteOrganizationalUnit

为 Amazon Organizations 资源添加标签

标签 是自定义的属性标签，您将其添加到 Amazon 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。您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 Amazon 标记策略。

当前，在以管理账户登录时，Amazon Organizations 支持以下标记操作：

- 您可以向以下组织资源添加标签：
  - Amazon Web Services 账户
  - 组织部门
  - 组织的根

您可以在以下时间添加标签：

- 在创建资源时 (p. 66) – 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 (p. 66) – 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 Amazon 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按事物进行资源分组，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。标签可帮助您控制谁可以访问和管理组成组织的组件 (p. 114)。

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。

- Amazon Web Services 账户
  - 创建账户 (p. 44)
  - 邀请账户 (p. 37)
- 组织部门（OU）(p. 59)

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`

Amazon Web Services Management Console

添加、更新或删除现有资源的标签

1. 登录到 Amazon Organizations 控制台。 您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 导航到并选择账户、根或 OU，并点击其名称以打开其详细信息页面。
3. 在 Tags (标签) 选项卡上，选择 Manage tags (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 Remove (删除)。

   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。
5. 根据需要，多次重复执行上一步骤。
6. 选择保存更改。

Amazon CLI & Amazon 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：

- Amazon CLI：tag-resource
- Amazon SDK：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：

- Amazon CLI：untag-resource
- Amazon SDK：UntagResource

将 Amazon Organizations 与其他 Amazon 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Amazon服务，以在您的组织及其代表您的账户中执行任务。这涉及向信任服务授予权限，但不会以其他方式影响 IAM 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

我们强烈推荐启用和禁用信任访问权限，方法是仅使用信任服务的控制台或其Amazon CLI或 API 操作等效操作。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，请参阅可与 Amazon Organizations 一起使用的 Amazon 服务 (p. 71)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 Amazon 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 策略明确允许这些操作。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Amazon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：Amazon 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 Amazon 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 Amazon CLI）允许访问。这允许服务代表您在 Amazon 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 (p. 108)。
  - `organizations:ListAWSServiceAccessForOrganization` – 在您使用 Amazon 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 Amazon 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 Amazon Organizations 中具有权限的凭证的人应使用 Amazon Organizations 控制台、Amazon CLI 或 Amazon 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 Amazon Organizations 权限如下：

     - `organizations:EnableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – 仅在您使用 Amazon Organizations 控制台时为必需

     有关在 Amazon 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 (p. 70)。
  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 Amazon 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，请参阅可与 Amazon Organizations 一起使用的 Amazon 服务 (p. 71)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 Amazon服务，您可以删除授予此访问权限的 IAM 权限，。
> 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。 (p. 17)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 Amazon 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 Amazon 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 Amazon 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 (p. 108)。
  - `organizations:ListAWSServiceAccessForOrganization` – 在您使用 Amazon 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 Amazon 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，请参阅可与 Amazon Organizations 一起使用的 Amazon 服务 (p. 71)处的服务特定说明。
  2. 在 Amazon Organizations 中具有权限的人之后可使用 Amazon Organizations 控制台、Amazon CLI 或 Amazon 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 Amazon Organizations 权限如下：

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – 仅在您使用 Amazon Organizations 控制台时为必需

     有关在 Amazon 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 (p. 70)。

如何允许或禁止可信访问

如果您只有 Amazon Organizations 的权限并且要代表另一 Amazon 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

我们强烈推荐启用和禁用信任访问权限，方法是仅使用信任服务的控制台或其Amazon CLI或 API 操作等效操作。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，请参阅可与 Amazon Organizations 一起使用的 Amazon 服务 (p. 71)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 Amazon 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 策略明确允许这些操作。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Amazon服务的文档。

Amazon Web Services Management Console

启用信任服务访问权限

1. 登录到 Amazon Organizations 控制台。 您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
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 Amazon 服务的管理员，他们现在可以启用另一服务以使用 Amazon Organizations。

禁用信任服务访问权限

1. 登录到 Amazon Organizations 控制台。 您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
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)。

Amazon CLI, Amazon API

允许或禁止信任服务访问

您可以使用以下 Amazon CLI 命令或 API 操作允许或禁止可信服务访问：

- Amazon CLI：Amazon organizations enable-aws-service-access

- Amazon CLI：Amazon organizations disable-aws-service-access
- Amazon API：EnableAWSServiceAccess
- Amazon API：DisableAWSServiceAccess

Amazon Organizations 和服务相关角色

Amazon 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 Amazon 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，Amazon 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，Amazon Organizations 将使用名为 `AWSServiceRoleForOrganizations` 的服务相关角色预置成员账户。仅 Amazon Organizations 服务自身可以代入此角色。此角色具有允许 Amazon Organizations 为其他Amazon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 (p. 6)（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 (p. 5)，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 Amazon 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 Amazon 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**
>
> Amazon 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。

可与 Amazon Organizations 一起使用的 Amazon 服务

通过 Amazon Organizations，您可以将多个Amazon Web Services 账户合并到一个组织中，大规模地执行账户管理活动。合并账户可简化您使用其他 Amazon 服务的方式。您可以将 Amazon Organizations 中提供的多账户管理服务与精选 Amazon 服务结合使用，以在您组织的所有账户上执行任务。

下表列出了可与 Amazon Organizations 一起使用的 Amazon 服务，以及在组织范围级别使用每项服务的优势。

信任访问权限 – 您可以启用兼容的Amazon服务，以便跨组织中的所有Amazon Web Services 账户执行操作。有关更多信息，请参阅将 Amazon Organizations 与其他 Amazon 产品结合使用 (p. 68)。

委托管理员 – 兼容的Amazon服务可以将组织中的Amazon成员账户注册为该服务中组织账户的管理员。

Amazon 服务	与 Amazon Organizations 一起使用的优势	支持可信访问	支持委派管理员	
Amazon Account Management (p. 76) 管理组织的所有 Amazon Web Services 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 (p. 77)	✓是 了解更多 (p. 78)	
Amazon CloudFormation Stacksets (p. 78) 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 (p. 79)	✓是 了解更多 (p. 79)	
Amazon Detective (p. 79) 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 Detective 与 Amazon 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。	✓是 了解更多 (p. 80)	✓是 了解更多 (p. 81)	
Amazon DevOps Guru (p. 82) 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，会通知用户。	您可以与 Amazon Organizations 集成，以管理来自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 (p. 82)	✓是 了解更多 (p. 83)	

Amazon 服务	与 Amazon Organizations 一起使用的优势	支持可信访问	支持委派管理员	
Amazon Firewall Manager (p. 84) 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。	您可以在组织中跨账户集中配置和管理 Amazon WAF 规则。	✓是 了解更多 (p. 84)	✓是 了解更多 (p. 86)	
Amazon GuardDuty (p. 87) GuardDuty 是一项持续的安全监控服务，可以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Amazon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组织中所有账户的 GuardDuty。添加成员账户会自动为所选 Amazon Web Services 区域中的这些账户启用 GuardDuty。您还可以自动为添加到组织的新账户激活 GuardDuty。 有关更多信息，请参阅《Amazon GuardDuty 用户指南》中的 GuardDuty 和 Organizations。	✓是 了解更多 (p. 87)	✓是 了解更多 (p. 88)	

Amazon 服务	与 Amazon Organizations 一起使用的优势	支持可信访问	支持委派管理员	
Amazon Inspector (p. 88) 可以自动扫描 Amazon 工作负载是否存在漏洞，以发现驻留在 Amazon ECR 中的 Amazon EC2 实例和容器映像是否存在软件漏洞及意外网络暴露。	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 Amazon Organizations 管理多个账户。	✓是 了解更多 (p. 89)	✓是 了解更多 (p. 90)	
Amazon License Manager (p. 91) 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 (p. 91)	✓是 了解更多 (p. 92)	
Amazon Web Services Marketplace (p. 93) 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。	您可以在组织的账户内共享 Amazon Web Services Marketplace 订阅和购买的许可证。	✓是 了解更多 (p. 93)	✗否	

Amazon 服务	与 Amazon Organizations 一起使用的优势	支持可信访问	支持委派管理员	
Amazon 网络管理器 (p. 94) 您可以跨 Amazon 账户、区域和本地位置集中管理 Amazon Cloud WAN 核心网络和 Amazon Transit Gateway 网络。	您可以跨组织中的多个 Amazon 账户，集中管理和监控您的全球网络以及中转网关和相关连接的资源。	✓是 了解更多 (p. 95)	✓是 了解更多 (p. 95)	
Amazon Resource Access Manager (p. 95) 将您拥有的指定 Amazon 资源与其他账户共享。	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。 有关可共享资源的列表，请参阅《Amazon RAM 用户指南》中的可共享资源。	✓是 了解更多 (p. 96)	✗否	

Amazon 服务	与 Amazon Organizations 一起使用的优势	支持可信访问	支持委派管理员	
Amazon Security Hub (p. 97) 在 Amazon 中查看安全状态，并检查环境是否符合安全行业标准和最佳实践。	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 (p. 98)	✓是 了解更多 (p. 98)	
Amazon Systems Manager (p. 98) 启用您的 Amazon 资源的可见性和控制。	您可以使用 Systems Manager Explorer，跨组织中的所有 Amazon Web Services 账户同步操作数据。 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。	✓ Yes（仅限 Systems Manager Explorer） 了解更多 (p. 99)	✓是 了解更多 (p. 101)	

Amazon Account Management、 和 Amazon Organizations

Amazon Account Management 可帮助您管理组织中所有 Amazon Web Services 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《Amazon Account Management 用户指南》中的在您的组织中使用 Amazon Account Management。

以下信息可帮助您将 Amazon Account Management 与 Amazon 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 (p. 68)。

账户管理功能需要具有 Amazon 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。

您可以通过运行 Organizations Amazon CLI 命令，或者调用某个 Amazon SDK 中的 Organizations API 操作来启用信任访问权限。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 启用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作启用信任服务访问权限：

- Amazon CLI：enable-aws-service-access

  您可以运行以下命令以启用 Amazon 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。
- Amazon 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 (p. 69)。

只有 Amazon Organizations 管理账户中的管理员可以禁用对 Amazon 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。

您可以通过运行 Organizations Amazon CLI 命令，或者调用某个 Amazon SDK 中的 Organizations API 操作来禁用信任访问权限。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作禁用信任服务访问：

- Amazon CLI：disable-aws-service-access

  您可以运行以下命令以禁用 Amazon 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。
- Amazon 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 Amazon Web Services 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 IAM 用户或角色能够将某个成员账户配置为该组织的账户管理委托管理员。

有关为账户管理功能启用委托管理员账户的说明，请参阅《Amazon Account Management 参考指南》中的启用委托管理员账户Amazon Account Management。

Amazon CLI, Amazon API

如果要使用 Amazon CLI 或某个 Amazon SDK 配置委托管理员账户，您可以使用以下命令：

- Amazon CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

- Amazon SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务 `principal account.amazonaws.com` 确定为参数。

Amazon CloudFormation StackSets 和 Amazon Organizations

利用 Amazon CloudFormation StackSets，您可通过一个操作跨多个Amazon Web Services 账户和Amazon Web Services 区域创建、更新或删除堆栈。StackSets 与 Amazon 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 Amazon 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 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《Amazon CloudFormation 用户指南》中的使用 Amazon CloudFormation StackSets。

以下信息可帮助您将 Amazon CloudFormation StackSets 与 Amazon 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 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 Amazon 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，然后该实例将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 Amazon CloudFormation 用户指南中的使用 Amazon 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。Amazon 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 Amazon 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 (p. 68)。

只有 Organizations 管理账户的管理员有权启用对其他Amazon服务的可信访问权限。您可以使用 Amazon CloudFormation 控制台或 Organizations 控制台启用信任访问权限。

您只能使用 Amazon CloudFormation StackSets 启用信任访问权限。

要使用 Amazon CloudFormation Stacksets 启用信任访问权限，请参阅 Amazon CloudFormation 用户指南中的使用 Amazon Organizations 启用信任访问权限。

为 Amazon 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 Amazon 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 Amazon CloudFormation Stacksets 的管理分开。

有关如何将成员账户指定为组织中的 Amazon CloudFormation Stacksets，请参阅《Amazon CloudFormation 用户指南》中的注册委托管理员。

Amazon Detective 和 Amazon 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 Amazon 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 Amazon 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 (p. 68)。

> 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 Amazon 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 Amazon Organizations 控制台启用信任访问权限。

Amazon Web Services 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 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
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 Amazon 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 Amazon 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 (p. 69)。

只有 Amazon 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 Amazon Organizations 控制台禁用信任访问权限。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
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 Amazon 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 Amazon 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 IAM 用户或角色能够将某个成员账户配置为该组织的 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。

Amazon CLI, Amazon API

如果要使用 Amazon CLI 或某个 Amazon SDK 配置委托管理员账户，您可以使用以下命令：

- Amazon CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal detective.amazonaws.com
```

- Amazon SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务 `principal 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 Amazon 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 Amazon 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 Amazon 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 (p. 68)。

> **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 Amazon 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 (p. 68)。

您可以使用 Amazon Organizations 控制台或 DevOps Guru 控制台启用信任访问权限。

Amazon Web Services 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 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。

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 Amazon 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 Amazon 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 (p. 69)。

只有 Amazon 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 Amazon Organizations 控制台禁用信任访问权限。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
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 Amazon 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 Amazon 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 IAM 用户或角色能够将某个成员账户配置为该组织中的 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。

Amazon CLI, Amazon API

如果要使用 Amazon CLI 或某个 Amazon SDK 配置委托管理员账户，您可以使用以下命令：

- Amazon CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal devops-guru.amazonaws.com
```

- Amazon SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务 `principal 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。

Amazon Firewall Manager 和 Amazon Organizations

Amazon 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Amazon Web Services 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 Amazon WAF 规则，创建 Amazon Shield Advanced 保护、配置和审计 Amazon Virtual Private Cloud（Amazon VPC）安全组，并部署 Amazon 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 Amazon Firewall Manager 的更多信息，请参阅 Amazon Firewall Manager 开发人员指南。

以下信息可帮助您将 Amazon Firewall Manager 与 Amazon 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 (p. 68)。

您可以使用 Amazon Firewall Manager 控制台或 Amazon Organizations 控制台启用可信访问。

Important

强烈建议您尽可能使用 Amazon Firewall Manager 控制台或工具来实现与 Organizations 的集成。这可让 Amazon 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 Amazon 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 (p. 68)。
如果您使用 Amazon 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 Amazon Organizations 管理账户登录，才能在组织内配置一个账户作为 Amazon Firewall Manager 管理员账户。有关更多信息，请参阅《Amazon Firewall Manager 开发人员指南》中的设置 Amazon Firewall Manager 管理员账户。

您可以使用Amazon Organizations控制台，通过运行 Amazon CLI 命令，或者通过调用其中一个 Amazon SDK 中的 API 操作来启用信任访问权限。

Amazon Web Services 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 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 在 Services (服务) 页面上，找到 Amazon 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 Amazon Organizations 的管理员，请告诉 Amazon 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 Amazon Organizations。

Amazon CLI, Amazon API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作启用信任服务访问权限：

- Amazon CLI：enable-aws-service-access

  您可以运行以下命令以启用 Amazon 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。
- Amazon 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 (p. 69)。

您可以使用 Amazon Firewall Manager 或者 Amazon Organizations 工具禁用信任访问权限。

Important

强烈建议您尽可能使用 Amazon Firewall Manager 控制台或工具来禁用与 Organizations 的集成。这可让 Amazon 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 Amazon 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 Amazon 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《Amazon Firewall Manager 开发人员指南》中的指定另一个账户作为 Amazon Firewall Manager 管理员账户中的说明更改或撤消 Amazon Firewall Manager 管理员账户。

如果您撤消此管理员账户，则必须登录 Amazon Organizations 管理账户并为 Amazon Firewall Manager 设置一个新的管理员账户。

您可以使用Amazon Organizations控制台，通过运行 Organizations Amazon CLI 命令，或者通过调用某个 Amazon SDK 中的 Organizations API 操作来禁用信任访问权限。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 在 Services（服务）页面上，找到 Amazon 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 Amazon Organizations 的管理员，请告诉 Amazon 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 Amazon Organizations。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作禁用信任服务访问：

- Amazon CLI：disable-aws-service-access

  您可以运行以下命令以禁用 Amazon 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。
- Amazon 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 IAM 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《Amazon Firewall Manager 开发人员指南》中的设置 Amazon Firewall Manager 管理员账户。

Amazon GuardDuty 和 Amazon 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Amazon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 Amazon Organizations 管理 GuardDuty 账户。

使用以下信息可帮助您将 Amazon GuardDuty 与 Amazon 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 (p. 68)。

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 Amazon 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 Amazon CLI 或某个 Amazon 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 (p. 69)。

您只能使用 Organizations 工具禁用信任访问权限。

您可以通过运行 Organizations Amazon CLI 命令，或者调用某个 Amazon SDK 中的 Organizations API 操作来禁用信任访问权限。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作禁用信任服务访问：

- Amazon 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。
- Amazon 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）

Amazon Inspector 和 Amazon 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 Amazon 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 Amazon Organizations 管理多个账户。

可以使用以下信息帮助您将 Amazon Inspector 与 Amazon 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 (p. 68)。

Amazon Inspector 需要具有对 Amazon 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 Amazon CLI 或某个 Amazon 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 Amazon CLI 命令，或者调用某个 Amazon SDK 中的 Organizations API 操作来启用信任访问权限。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 启用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作启用信任服务访问权限：

- Amazon 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。
- Amazon 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 (p. 69)。

只有 Amazon Organizations 管理账户中的管理员可以使用 Amazon Inspector 禁用信任访问权限。

您可以仅使用 Organizations 工具禁用信任访问权限。

您可以通过运行 Organizations Amazon CLI 命令，或者调用某个 Amazon SDK 中的 Organizations API 操作来禁用信任访问权限。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作禁用信任服务访问：

- Amazon 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。
- Amazon API：DisableAWSServiceAccess

为 Amazon Inspector 启用委托管理员账户

借助 Amazon Inspector，您可以通过 Amazon Organizations 服务使用授权管理员管理组织中的多个账户。

Amazon 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 IAM 用户或角色能够将某个成员账户配置为该组织中 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`。

Amazon CLI, Amazon API

如果要使用 Amazon CLI 或某个 Amazon SDK 配置委托管理员账户，您可以使用以下命令：

- Amazon CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- Amazon SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，并将账户服务 `principal account.amazonaws.com` 确定为参数。

为 Amazon Inspector 禁用委托管理员

只有 Amazon 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。

Amazon License Manager、 和 Amazon Organizations

Amazon License Manager 简化了将软件供应商许可证迁移到云的过程。在 Amazon 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。

通过将 License Manager 与 Amazon Organizations 相关联，您可以在整个组织中启用计算资源的跨账户发现。

有关 License Manager 的更多信息，请参阅 License Manager 指南。

以下信息可帮助您将 Amazon License Manager 与 Amazon 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 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，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。

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`

有关更多信息，请参阅使用 License Manager 管理账户角色和使用 License Manager 成员账户角色。

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`

使用 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 (p. 68)。

您只能使用 Amazon License Manager 启用信任访问权限。

使用 License Manager 启用信任访问权限

您必须使用 Amazon Organizations 管理账户登录 License Manager，并将其与您的 License Manager 账户相关联。有关信息，请参阅配置 Amazon License Manager 指南设置。为方便起见，我们还将对此进行了总结。

Important

该过程是一个单向过程。您不能撤消此过程。

在 Organizations 和 License Manager 之间启用信任访问权限

1. 使用组织的管理账户登录到Amazon Web Services Management Console。
2. 导航到 License Manager 控制台，然后选择 Settings (设置)。
3. 选择编辑。
4. 选择 Link Amazon Organizations accounts (关联 Amazon Organizations 账户)。

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 (p. 69)。

您只能使用 Organizations 工具禁用信任访问权限。

您可以通过运行 Organizations Amazon CLI 命令，或者调用某个 Amazon SDK 中的 Organizations API 操作来禁用信任访问权限。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作禁用信任服务访问：

- Amazon CLI：disable-aws-service-access

  您可以运行以下命令以禁用 Amazon 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。
- Amazon 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。为方便起见，我们还对此进行了总结。

为 License Manager 注册委托管理员账户

1. 使用组织的管理账户登录到Amazon Web Services Management Console。
2. 导航到 License Manager 控制台，然后选择 Settings (设置)。
3. 在 Delegated administrators (委托管理员) 下，选择 Delegate administrator (委托管理员)。
4. 输入您想分配的Amazon Web Services 账户的账户 ID 号，然后选择 Delegate (委托)。您不能使用管理账户的 ID。它必须是成员账户。

Amazon Web Services Marketplace、 和 Amazon Organizations

Amazon Web Services 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。

Amazon Web Services Marketplace 使用您在 Amazon Web Services Marketplace 中购买的 Amazon 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，Amazon Web Services Marketplace 创建和管理这些账户的新许可证。

有关更多信息，请参阅《Amazon Web Services Marketplace 买家指南》中的 Amazon Web Services Marketplace 的服务相关角色。

以下信息可帮助您将 Amazon Web Services Marketplace 与 Amazon 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 Web Services Marketplace 在您组织中的组织账户内执行支持的操作。

只有在禁用 Amazon Web Services 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。Amazon Web Services 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 Amazon Web Services 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 (p. 68)。

您可以使用 Amazon Web Services Marketplace 控制台或 Amazon Organizations 控制台启用可信访问。

> **Important**
>
> 强烈建议您尽可能使用 Amazon Web Services Marketplace 控制台或工具来实现与 Organizations 的集成。这可让 Amazon Web Services 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 Amazon Web Services 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 (p. 68)。
> 如果您使用 Amazon Web Services 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。

要使用 Amazon Web Services Marketplace 控制台启用可信访问权限，请执行以下操作：

请参阅《Amazon Web Services Marketplace 买家指南》中的为 Amazon Web Services Marketplace 创建服务相关角色。

使用 Amazon Web Services 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 (p. 68)。

您只能使用 Organizations 工具启用信任访问权限。

您可以通过运行 Organizations Amazon CLI 命令，或者调用某个 Amazon SDK 中的 Organizations API 操作来禁用信任访问权限。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作禁用信任服务访问：

- Amazon CLI：disable-aws-service-access

  您可以运行以下命令以禁用 Amazon Web Services 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。
- Amazon API：DisableAWSServiceAccess

Amazon Network Manager 与 Amazon Organizations

借助 Network Manager，您可以跨 Amazon 账户、区域和本地位置集中管理 Amazon Cloud WAN 核心网络和 Amazon Transit Gateway 网络。借助多账户支持，您可以为您的任何 Amazon 账户创建单个全球网络，然后使用 Network Manager 控制台将来自多个账户的中转网关注册到该全球网络。

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。
- 在 Network Manager 控制台中为 Network Manager 启用可信访问时，控制台还会启用 Amazon CloudFormation StackSets 服务。Network Manager 使用 StackSets 来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 Amazon Organizations 管理多个账户。

以下信息可帮助您将 Amazon Network Manager 与 Amazon Organizations 集成。

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.amazon.aws.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 (p. 68)。

只有 Organizations 管理账户的管理员有权启用对其他Amazon服务的可信访问权限。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 Amazon Organizations 管理多个账户。

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。

Amazon Resource Access Manager 和 Amazon Organizations

Amazon Resource Access Manager（Amazon RAM）可让您与其他Amazon Web Services 账户共享您指定的Amazon资源。这是一种集中式服务，跨多个账户为共享不同类型的 Amazon 资源提供一致的体验。

Amazon RAM有关 的更多信息，请参阅 Amazon RAM 用户指南。

以下信息可帮助您将 Amazon Resource Access Manager 与 Amazon 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 RAM 在您组织中的组织账户内执行支持的操作。

只有在禁用 Amazon 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。Amazon 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 Amazon 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 (p. 68)。

您可以使用 Amazon Resource Access Manager 控制台或 Amazon Organizations 控制台启用可信访问。

> Important
>
> 强烈建议您尽可能使用 Amazon Resource Access Manager 控制台或工具来实现与 Organizations 的集成。这可让 Amazon 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 Amazon 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 (p. 68)。
> 如果您使用 Amazon 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 Amazon RAM 控制台或 CLI 启用信任访问权限

请参阅《Amazon RAM 用户指南》中的允许与 Amazon Organizations 共享。

您可以通过运行 Organizations Amazon CLI 命令，或者调用某个 Amazon SDK 中的 Organizations API 操作来启用信任访问权限。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 启用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作启用信任服务访问权限：

- Amazon CLI：enable-aws-service-access

  您可以运行以下命令以启用 Amazon 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。

- Amazon API：EnableAWSServiceAccess

使用 Amazon 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 (p. 69)。

您可以使用 Amazon Resource Access Manager 或者 Amazon Organizations 工具禁用信任访问权限。

> Important
>
> 强烈建议您尽可能使用 Amazon Resource Access Manager 控制台或工具来禁用与 Organizations 的集成。这可让 Amazon 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 Amazon 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 Amazon 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 Amazon Resource Access Manager 控制台或 CLI 启用信任访问权限

请参阅《Amazon RAM 用户指南》中的允许与 Amazon Organizations 共享。

您可以通过运行 Organizations Amazon CLI 命令，或者调用某个 Amazon SDK 中的 Organizations API 操作来禁用信任访问权限。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作禁用信任服务访问：

- Amazon CLI：disable-aws-service-access

  您可以运行以下命令以禁用 Amazon 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。
- Amazon API：DisableAWSServiceAccess

Amazon Security Hub、 和 Amazon Organizations

Amazon Security Hub 提供了您在 Amazon 中的安全状态的全面视图，可帮助您检查环境是否符合安全行业标准和最佳实践。

Security Hub 从您的Amazon Web Services 账户、您使用的Amazon服务以及受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。

当您同时使用 Security Hub 和 Amazon Organizations 时，您可以自动为您的所有账户启用 Security Hub，包括添加的新账户。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《Amazon Security Hub 用户指南》。

以下信息可帮助您将 Amazon Security Hub 与 Amazon 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 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 (p. 68)。

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《Amazon 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，选择 Settings (设置)。
3. 在 Delegated Administrator (委托管理员) 中，输入账户 ID。

Amazon Systems Manager 和 Amazon Organizations

Amazon Systems Manager 是功能的集合，可以实现对 Amazon 资源的可见性和控制。Systems Manager 中的两项功能可以与 Organizations 搭配使用，以便在组织的所有Amazon Web Services 账户中运行。

- Systems Manager Explorer 是一个可自定义的操作控制面板，用于报告有关Amazon资源的信息。您可以使用 Organizations 和 Systems Manager Explorer，跨组织里的所有Amazon Web Services 账户同步操作数据。有关更多信息，请参阅《Amazon 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《Amazon Systems Manager 用户指南》中的 Amazon Systems Manager Change Manager。

以下信息可帮助您将 Amazon Systems Manager 与 Amazon 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 (p. 68)。

您可以使用 Amazon Systems Manager 控制台或 Amazon Organizations 控制台启用可信访问。

> Important
>
> 强烈建议您尽可能使用 Amazon Systems Manager 控制台或工具来实现与 Organizations 的集成。这可让 Amazon Systems 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 Amazon Systems 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 (p. 68)。
> 如果您使用 Amazon Systems 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 Systems Manager 控制台启用信任访问权限

您必须使用 Amazon Organizations 管理账户并创建资源数据同步。有关更多信息，请参阅《Amazon Systems Manager 用户指南》中的设置 Explorer 以显示来自多个账户和区域的数据。

您可以使用Amazon Organizations控制台，通过运行 Amazon CLI 命令，或者通过调用其中一个 Amazon SDK 中的 API 操作来启用信任访问权限。

Amazon Web Services 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 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
> 2. 在 Services (服务) 页面上，找到 Amazon 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 Amazon Organizations 的管理员，请告诉 Amazon 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 Amazon Organizations。

Amazon CLI, Amazon API

> 使用 OrganizationsCLI/SDK 启用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作启用信任服务访问权限：

- Amazon CLI：enable-aws-service-access

  您可以运行以下命令以启用 Amazon 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。
- Amazon 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 (p. 69)。

Systems Manager 需要对 Amazon Organizations 的信任访问权限才能在组织中跨Amazon Web Services 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。

您可以使用 Amazon Systems Manager 或者 Amazon Organizations 工具禁用信任访问权限。

> **Important**
>
> 强烈建议您尽可能使用 Amazon Systems Manager 控制台或工具来禁用与 Organizations 的集成。这可让 Amazon Systems 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 Amazon Systems 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 Amazon Systems 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 Systems Manager 控制台禁用信任访问权限

请参阅《Amazon Systems Manager 用户指南》中的删除 Systems Manager Explorer 资源数据同步。若要重新启用可信的访问，必须为 Systems Manager Explorer 创建新的资源数据同步。

您可以使用Amazon Organizations控制台，通过运行 Organizations Amazon CLI 命令，或者通过调用某个 Amazon SDK 中的 Organizations API 操作来禁用信任访问权限。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录到 Amazon Organizations 控制台。您必须以 IAM 用户身份或担任组织管理账户中的 IAM 角色登录。
2. 在 Services（服务）页面上，找到 Amazon 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 Amazon Organizations 的管理员，请告诉 Amazon 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 Amazon Organizations。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作禁用信任服务访问：

- Amazon CLI：disable-aws-service-access

您可以运行以下命令以禁用 Amazon 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。

- Amazon 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Amazon Web Services 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。

指定一个成员账户作为 Systems Manager 的委托管理员

有关 Systems Manager Explorer 的信息，请参阅《Amazon Systems Manager 用户指南》中的配置委托管理员。

有关 Systems Manager Change Manager 的信息，请参阅《Amazon Systems Manager 用户指南》中的为 Change Manager 设置组织和委托账户。

Amazon Well-Architected Tool–和–Amazon Organizations

Amazon Well-Architected Tool 可帮助您记录工作负载的状态并将其与最新的 Amazon 架构最佳做法进行比较。

将 Amazon Well-Architected Tool 与 Organizations 结合使用让 Amazon Well-Architected Tool 和 Organizations 客户能够简化与组织的其他成员共享 Amazon Well-Architected Tool 资源的过程。

有关更多信息，请参阅 Amazon Well-Architected Tool 用户指南中的共享您的 Amazon Well-Architected Tool 资源。

以下信息可帮助您将 Amazon Well-Architected Tool 与 Amazon 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 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 Amazon 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。Amazon 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 Amazon WA Tool 启用信任访问权限

允许更新 Amazon 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 (p. 68)。

您可以使用 Amazon Well-Architected Tool 控制台或 Amazon Organizations 控制台启用可信访问。

> Important
>
> 强烈建议您尽可能使用 Amazon Well-Architected Tool 控制台或工具来实现与 Organizations 的集成。这可让 Amazon 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 Amazon 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 (p. 68)。
> 如果您使用 Amazon 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 Amazon WA Tool 控制台启用可信访问权限

请参阅 Amazon Well-Architected Tool 用户指南中的共享您的 Amazon Well-Architected Tool 资源。

使用 Amazon 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 (p. 69)。

您可以使用 Amazon Well-Architected Tool 或者 Amazon Organizations 工具禁用信任访问权限。

> Important
>
> 强烈建议您尽可能使用 Amazon Well-Architected Tool 控制台或工具来禁用与 Organizations 的集成。这可让 Amazon 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 Amazon 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 Amazon 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 Amazon WA Tool 控制台禁用信任访问权限

请参阅 Amazon Well-Architected Tool 用户指南中的共享您的 Amazon Well-Architected Tool 资源。

您可以通过运行 Organizations Amazon CLI 命令，或者调用某个 Amazon SDK 中的 Organizations API 操作来禁用信任访问权限。

Amazon CLI, Amazon API

> 使用 Organizations CLI/SDK 禁用信任服务访问权限
>
> 您可以使用以下 Amazon CLI 命令或 API 操作禁用信任服务访问：
>
> - Amazon CLI：disable-aws-service-access

您可以运行以下命令以禁用 Amazon 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。

- Amazon API：DisableAWSServiceAccess

Amazon VPC IP 地址管理器 (IPAM) 和 Amazon 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 Amazon 工作负载的 IP 地址。

使用 Amazon 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 Amazon Organizations 集成。

使用以下信息可帮助您将 Amazon VPC IP 地址管理器（IPAM）与 Amazon 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 Amazon 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 (p. 68)。

> **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 Amazon 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 Amazon 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 `AmazonServiceRoleForIPAM`。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 Amazon Organizations 集成。

Note

您不能使用 Amazon Organizations 控制台或 `enable-aws-service-access` 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 (p. 69)。

只有 Amazon Organizations 管理账户中的管理员可以使用 Amazon 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 Amazon CLI 命令，或者调用某个 Amazon SDK 中的 Organizations API 操作来禁用信任访问权限。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 禁用信任服务访问权限

您可以使用以下 Amazon CLI 命令或 API 操作禁用信任服务访问：

- Amazon 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。
- Amazon 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 Amazon 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《Amazon Amazon 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 IAM 用户或角色能够将某个成员账户配置为该组织的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 Amazon 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 Amazon Amazon CLI 删除委托管理员，请参阅《Amazon Amazon 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 Amazon Organizations 集成。

中的安全性Amazon Organizations

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

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

- 云的安全性 – Amazon负责保护在Amazon云中运行Amazon服务的基础设施。Amazon还向您提供可安全使用的服务。作为 Amazon 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 Amazon Organizations 的合规性计划，请参阅合规性计划范围内的 Amazon 服务。
- 云中的安全性 - 您的责任由您使用的 Amazon 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。您还会了解如何使用其他Amazon服务以帮助您监控和保护 Organizations 资源。

主题

Amazon Identity and Access Management、 和 Amazon Organizations

访问 Amazon Organizations 需要凭证。这些凭证必须有权访问Amazon资源，例如 Amazon Simple Storage Service（Amazon S3）存储桶、Amazon Elastic Compute Cloud（Amazon EC2）实例或 Amazon Organizations 组织部门（OU）。以下部分提供了有关如何使用 Amazon 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，Amazon Organizations 使用与其他Amazon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 Amazon 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 Amazon 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 Amazon 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

- 使用标签和 Amazon Organizations 的基于属性的访问控制 (p. 114)

身份验证

您可以以下面任一类型的身份访问 Amazon：

- Amazon Web Services 账户根用户 - 注册Amazon时，您需要提供与您的Amazon Web Services 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 Amazon 资源的完全访问权限。

  Important

  出于安全考虑，建议仅使用根用户凭证创建管理员用户，此类用户是对您的Amazon Web Services 账户具有完全访问权限的 IAM 用户。随后，您可以使用此管理员用户来创建具有有限权限的其他 IAM 用户和角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 最佳实践和创建您的第一个 IAM 管理员用户和组。
- IAM 用户 – IAM 用户就是您的Amazon Web Services 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Amazon网页（如Amazon Web Services Management Console、Amazon开发论坛或Amazon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 Amazon Command Line Interface（Amazon CLI）以编程方式访问Amazon服务时，可以使用这些密钥。软件开发工具包和 Amazon 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 Amazon 工具，则必须自行对请求签名。Amazon 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。有关验证请求的更多信息，请参阅《Amazon 一般参考》中的 签名版本 4 签名流程。
- 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Amazon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 Amazon 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，Amazon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Amazon Web Services 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Amazon Web Services 账户的访问权限。
  - Amazon服务访问 – 可以使用您账户中的 IAM 角色向Amazon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Amazon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 Amazon 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Amazon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 用户指南中的对 Amazon EC2 上的应用程序使用角色。

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 Amazon Organizations 资源。例如，您必须拥有权限来创建 OU 。

下面几节介绍如何管理 Amazon Organizations 的权限。

- 管理您的 Amazon 组织的访问权限 (p. 108)
- 为 Amazon Organizations 使用基于身份的策略（IAM 策略） (p. 111)

- 使用标签和 Amazon Organizations 的基于属性的访问控制 (p. 114)

管理您的 Amazon 组织的访问权限

所有Amazon资源（包括组织中的根、OU、账户和策略）都归Amazon Web Services 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 Amazon 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 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。

Amazon Organizations 资源和操作

此部分讨论如何将 Amazon Organizations 概念映射到其 IAM 等效概念。

资源

在 Amazon 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 Amazon Organizations 中所用资源的 ARN 格式的完整列表，请参阅《IAM 用户指南》中的 Amazon Organizations 定义的资源。

操作

Amazon 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 策略的 `Action` 元素中引用大多数操作来控制可使用操作的人员。有关可在 IAM 策略中用作权限的 Amazon Organizations 操作的列表，请参阅《IAM 用户指南》中的 Amazon Organizations 定义的 API 操作权限。

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

Amazon 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 策略的 `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 Amazon 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Amazon Web Services 账户的所有账户 ID 的替代方法。您可以在 元素中指定 (p. 28)组织 ID`Condition`，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》的Amazon全局条件上下文键中对 `PrincipalOrgID` 的说明。

- `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 Amazon 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 Amazon 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》中的 aws:PrincipalOrgPaths。

  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/"
        ]
    }
}
```

有关所有可以在 IAM 策略中用作权限的 Amazon Organizations 特定条件键，请参阅《IAM 用户指南》中的 Amazon Organizations 的条件上下文键。

了解资源所有权

Amazon Web Services 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委托人实体（即根账户、IAM 用户或 IAM 角色）的Amazon Web Services 账户。对于Amazon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 Amazon 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 Amazon 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 策略语法和说明的信息，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 策略）。附加到资源的策略称作基于资源的策略。Amazon Organizations 仅支持基于身份的策略（IAM 策略）。

主题

基于身份的权限策略（IAM 策略）

您可以将策略附加到 IAM 身份以允许这些身份对Amazon资源执行操作。例如，可以：

- 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 Amazon Organizations 资源（例如， 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 Amazon 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 Amazon 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、组、角色和权限的更多信息，请参阅IAM 用户指南中的身份（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。Amazon 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 Amazon 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，Amazon 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，Amazon 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 Amazon 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》https://docs.amazonaws.cn/IAM/latest/UserGuide/reference_policies_elements_effect.html中的 IAM JSON 策略元素：效果。
- Principal – 在基于身份的策略（IAM 策略）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）。Amazon Organizations 目前仅支持基于身份的策略，而不是基于资源的策略。

有关 IAM 策略语法和说明的信息，请参阅《IAM 用户指南》中的 IAM JSON 策略参考。

为 Amazon 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 Amazon（IAM）身份（用户、组和角色）来控制对Amazon 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 Amazon Organizations 的基于属性的访问控制 (p. 114)。

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 Amazon 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 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧的导航栏中，选择 Policies (策略)。

   如果这是您首次选择 Policies，则会显示 Welcome to Managed Policies 页面。选择开始使用。
3. 在页面的顶部，选择 Create policy (创建策略)。
4. 选择 JSON 选项卡。
5. 输入以下 JSON 策略文档：

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

6. 选择 Review policy (审核策略)。

   Note

   您可以随时在可视化编辑器和 JSON 选项卡之间切换。不过，如果您进行更改或在可视化编辑器选项卡中选择 Review policy (查看策略)，IAM 可能会调整您的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 Review policy (查看策略) 页面上，为创建的策略输入 Name (名称) 和 Description (说明)（可选）。查看策略摘要以查看您的策略授予的权限。然后，选择创建策略以保存您的工作。

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 IAM 策略中可供分配的所有权限的列表，请参阅《IAM 用户指南》中的 Amazon Organizations 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 Amazon 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Amazon Web Services 账户的管理访问权。它仅授予对指定 OU 中的账户执行 Amazon 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 Amazon 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《IAM 用户指南》中的 Amazon Organizations 定义的资源。

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 Amazon IAM Identity Center (successor to Amazon Single Sign-On) 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《IAM 用户指南》中的 Amazon Organizations 定义的资源。

使用标签和 Amazon 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Amazon资源和Amazon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。

Amazon Organizations 可标记的资源包括Amazon Web Services 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 Amazon 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 (p. 114)
- 检查附加到发出请求的 IAM 用户或角色的标签 (p. 115)
- 检查请求中作为参数包含的标签 (p. 115)

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Amazon Web Services Management Console、Amazon Command Line Interface（Amazon CLI）或其中一个 Amazon 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 Amazon 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 Amazon Web Services 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。

Amazon 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。Amazon Organizations 目前支持两种 Amazon 服务，帮您监控组织和组织内部的活动。

主题

使用 Amazon Organizations 记录 Amazon CloudTrail API 调用

Amazon Organizations 与 Amazon CloudTrail 集成，后者是在 Amazon 中记录用户、角色或 Amazon Organizations 服务所执行操作的服务。CloudTrail 将对 Amazon Organizations 的所有 API 调用均作为事件捕获，包括来自 Amazon Organizations 控制台的调用和对 Amazon 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 Amazon Organizations 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history (事件历史记录) 中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向 Amazon 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《Amazon CloudTrail 用户指南》。

> **Important**
>
> 您只能在美国东部（弗吉尼亚北部）区域查看 Amazon Organizations 的所有 CloudTrail 信息。如果无法在 CloudTrail 控制台中看到您的 Amazon 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 Amazon 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。

Amazon OrganizationsCloudTrail 中的 信息

在您创建 Amazon Web Services 账户 时，将在该账户上启用 CloudTrail。当 Amazon Organizations 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他Amazon服务事件一同保存在 Event history (事件历史记录) 中。您可以在 Amazon Web Services 账户 中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录Amazon Web Services 账户中的事件（包括 Amazon Organizations 的事件），请创建跟踪。通过跟踪，CloudTrail 可将日志文件传送至 Simple Storage Service（Amazon S3）存储桶。在您的 Amazon Web Services 账户中启用了 CloudTrail 日志记录时，对 Amazon Organizations 操作的 API 调用在 CloudTrail 日志文件中跟踪，它们随其他Amazon服务记录一起写入到这些文件中。您可以配置其他Amazon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 Amazon Organizations 操作，Amazon 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 Amazon 服务发出

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

了解 Amazon Organizations 日志文件条目

跟踪记录是一种配置，可用于将事件作为日志文件传送到您指定的 Simple Storage Service（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"
}
```


Amazon CloudWatch Events

Amazon Organizations在组织中发生管理员指定的操作时， 可以与 CloudWatch Events 配合生成事件。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 CloudWatch Events 规则来监视这些操作，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 Amazon Lambda 函数，记录操作的详细信息以备稍后查看。

有关如何使用 CloudWatch Events 监控组织中关键活动的教程，请参阅教程：使用 CloudWatch Events 监控组织的重要更改 (p. 11)。

要了解有关 CloudWatch Events 的更多信息，包括如何对其进行配置和启用，请参阅 Amazon CloudWatch Events 用户指南。

Amazon Organizations 的合规性验证

作为多个 Amazon 合规性计划的一部分，第三方审核员将评估 Amazon Web Services的安全性与合规性，例如 SOC、PCI、FedRAMP 和 HIPAA。

要了解 或其他 Amazon Web Services 是否在特定合规性计划范围内，请参阅合规性计划范围内的 Amazon Web Services。有关常规信息，请参阅Amazon Web Services合规性计划。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅、在 Amazon Artifact 中下载报告。

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

- 安全性与合规性快速入门指南安全性与合规性快速入门指南 – 这些部署指南讨论了架构注意事项，并提供了在Amazon上部署注重安全性和合规性的基准环境的步骤。
- 《Amazon Web Services 上的 HIPAA 安全性和合规性架构设计》– 该白皮书介绍了公司如何使用 Amazon Web Services 创建符合 HIPAA 要求的应用程序。

  Note

  并非所有 Amazon Web Services都符合 HIPAA 要求。有关更多信息，请参阅符合 HIPAA 要求的服务参考。
- Amazon合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- Amazon Config 开发人员指南中的使用规则评估资源 – 此 Amazon Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub：此 Amazon Web Service 提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践规范。

Amazon Organizations 中的故障恢复能力

Amazon全球基础设施围绕Amazon Web Services 区域和可用区构建。Amazon Web Services 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Amazon Web Services 区域和可用区的更多信息，请参阅Amazon全球基础设施。

中的基础设施安全性Amazon Organizations

作为一项托管式服务，Amazon Organizations 由 亚马逊云科技：安全流程概览白皮书中所述的Amazon全球网络安全程序提供保护。

您可以使用Amazon发布的 API 调用通过网络访问 Organizations。客户端必须支持传输层安全性（TLS）。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 终端节点。有关可用的 FIPS 终端节点的更多信息，请参阅美国联邦信息处理标准 (FIPS) 第 140-2 版。

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 Amazon Security Token Service (Amazon STS) 生成临时安全凭证来对请求进行签名。

Amazon Organizations 引用

使用本部分中的主题查找 Amazon Organizations 各方面的详细参考信息。

主题

Amazon Organizations 的配额

本节指定影响 Amazon Organizations 的配额。

命名指南

下面是在 Amazon Organizations 中创建时的名称指南（包括账户、组织单位 (OU)、根和策略的名称）：

- 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 Amazon 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 Amazon Organizations 中的实体的默认最大数量。

> **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，您在使用 Service Quotas 控制台、Amazon CLI 或 Amazon SDK 时，必须使用 `us-east-1` 来访问 Organizations 配额。

组织中的Amazon Web Services 账户数量	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，则撤销此计数。
组织中的根数量	1
组织中的 OU 数量	1000
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 天内关闭的成员账户数量	企业中 10% 的活动成员账户可以在 30 天内关闭。可关闭的账户最大数量为 200 个，即使 10% 的活动账户超过 200 个，也仅可关闭 200 个。
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。
您可以附加到根、OU 或账户的标签数	50

可用于 Amazon Organizations 的 Amazon 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Amazon托管式策略。您无法修改或删除 Amazon 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 Amazon Identity and Access Management（IAM）的 Amazon Organizations 托管式策略

IAM 托管式策略由Amazon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Amazon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Amazon托管式策略的列表。使用 Filter policies (筛选策略) 下拉菜单，选择 Amazon 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：	arn:aws:iam::aws:policy/AWSOrganizationsFullAccess

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

 "Action":"organizations:*",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[

 "account:PutAlternateContact",

 "account:DeleteAlternateContact",

 "account:GetAlternateContact"
         ],
         "Resource":"*"
```

策略名称	描述	ARN
	<pre>}, { "Effect":"Allow", "Action":"iam:CreateServiceLinkedRole", "Resource":"*", "Condition":{ "StringEquals":{ "iam:AWSServiceName":"organizations.amazonaws.com" } } }] }</pre>	
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： <pre>{ "Version":"2012-10-17", "Statement":[{ "Effect":"Allow", "Action":["organizations:Describe*", "organizations:List*"], "Resource":"*" }, { "Effect":"Allow", "Action":["account:GetAlternateContact"], "Resource":"*" }] }</pre>	arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess

更新 Organizations Amazon托管式策略

下表显示了Amazon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 Amazon Organizations 文档历史记录 (p. 134)页面上的 RSS 源。

更改	说明	日期
AWSOrganizationsFullAccess – 已进行更新，以允许创建组织。	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

更改	说明	日期
AWSOrganizationsFullAccess - 已更新为允许通过 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:DeleteAlternateContac` 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 22 日
AWSOrganizationsReadOnlyAccess - 已更新为允许通过 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 22 日

Amazon Organizations 故障排除

如果您在使用 Amazon 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 Amazon Organizations 时可能遇到的拒绝访问或其他常见问题。

主题

当我向 Amazon 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 策略附加到您的 IAM 用户或您所属的组来授予权限。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 IAM 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 Amazon 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 IAM 用户或角色具有正确的权限。临时安全凭证权限派生自 IAM 用户或角色，因此权限范围仅限于相应 IAM 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Amazon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《Amazon 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 Amazon Organizations 控制台、API 或 Amazon 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 Amazon 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。Amazon 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 Amazon 免费套餐）Amazon 活动收费。有关更多信息，请参阅 作为成员账户退出组织 (p. 53)。

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Amazon Web Services 账户前，请从组织中删除它 (p. 51)，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 (p. 125)。

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 (p. 125)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 Amazon Web Services 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 (p. 22)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，Amazon Organizations 使用称为最终一致性的分布式计算模型。您在 Amazon 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。Amazon 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 Amazon 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
- Amazon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。

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 Amazon 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 Amazon Organizations API 参考。

> Note
>
> 您可以使用 Amazon Organizations 开发工具包之一，代替对 Amazon 查询 API 进行直接调用。Amazon 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 Amazon Organizations 和 Amazon 的编程访问。例如，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 Amazon 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 Amazon 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。Amazon 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 Amazon Organizations API 参考中的各个操作页面。

主题

Endpoints

Amazon 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Amazon终端节点和区域的更多信息，请参阅《Amazon 一般参考》中的区域和终端节点。

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 Amazon 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 Amazon 根账户凭证处理日常的 Amazon Organizations 工作。您可以使用 IAM 用户的凭证或临时凭证，例如您用于 IAM 角色的凭证。

要对您的 API 请求进行签名，您必须使用 Amazon 签名版本 4。有关使用签名版本 4 的信息，请参阅 https://docs.amazonaws.cn/general/latest/gr/signature-version-4.html 常规参考 中的Amazon签名版本 4 签名流程。

Amazon 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：

- Amazon安全凭证 – 提供有关您可用于访问Amazon的凭证类型的一般信息
- IAM 最佳实践 – 提供有关使用 IAM 服务的建议，以帮助保护您的Amazon资源，包括 Amazon Organizations 中的资源。
- 临时凭证 – 说明如何创建和使用临时安全凭证

Amazon Organizations 的文档历史记录

下表介绍了 Amazon Organizations 的主要文档更新。

- API 版本：2016-11-28

变更	说明	日期
更新了 AWSOrganizationsFullAccess 托管式策略以启用组织创建操作。	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
将公告更新为可以使用 Amazon Organizations 控制台更新备用联系人。	Organizations 现在可以通过 Amazon Organizations控制台为组织内的账户更新备用联系人。宣布账户管理参考中的新功能和要点以供说明。	2022 年 2 月 22 日
Organizations 托管策略更新 - 对现有策略的更新	更新了 AWSOrganizationsFullAccess 和 AWSOrganizationsReadOnlyAccess 托管策略，以允许通过 Amazon 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 22 日
Organizations 与 Amazon DevOps Guru 的集成。	您可以将 Amazon DevOps Guru 与 Amazon Organizations 集成，以全面监控所有组织账户中的应用程序运行状况，并加深了解。	2022 年 1 月 3 日
Organizations 与 Amazon Detective 的集成。	您可以将 Amazon Detective 与 Amazon 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 Amazon 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《Amazon 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 Amazon 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 Amazon 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 Amazon CloudFormation StackSets 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 Amazon 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	Amazon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 Amazon Organizations 控制台的 2.0 版本 (p. 134)	Amazon推出了一个新版本的Amazon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 Amazon Web Services Marketplace 的集成	您现在可以启用 Amazon Web Services 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Amazon Web Services 账户内。	2020 年 11 月 18 日
中国的Amazon Web Services 区域现在支持将 Amazon Resource Access Manager 作为 Organizations 的可信服务。 (p. 134)	现在，当您在中国使用 Organizations 和 Amazon RAM 时，您可以将与 Organizations 集成的 Amazon RAM 功能作为信任服务使用。	2020 年 11 月 18 日
Organizations 现在支持与 Amazon 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 (p. 134)	Amazon 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 Amazon 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 Amazon 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《Amazon 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 支持创建时标记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
与 Amazon 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 Amazon 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
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 通知将发布到管理账户的 CloudTrail 日志。	2018 年 6 月 28 日
账户删除现在是自助服务	您现在可以删除在 Amazon Organizations 内创建的账户，无需联系 Amazon Web Services Support。	2017 年 12 月 19 日
Amazon 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 Amazon Organizations 与其他 Amazon 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 (p. 134)	客户现在可以在 Amazon Web Services 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 Amazon Organizations 文档版本。	2017 年 2 月 17 日

Amazon词汇表

有关最新Amazon术语，请参阅Amazon一般参考中的Amazon术语表。