亚马逊云科技

用户指南

Amazon Organizations

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 (PDF)。

Table of Contents

什么是 Amazon Organizations？

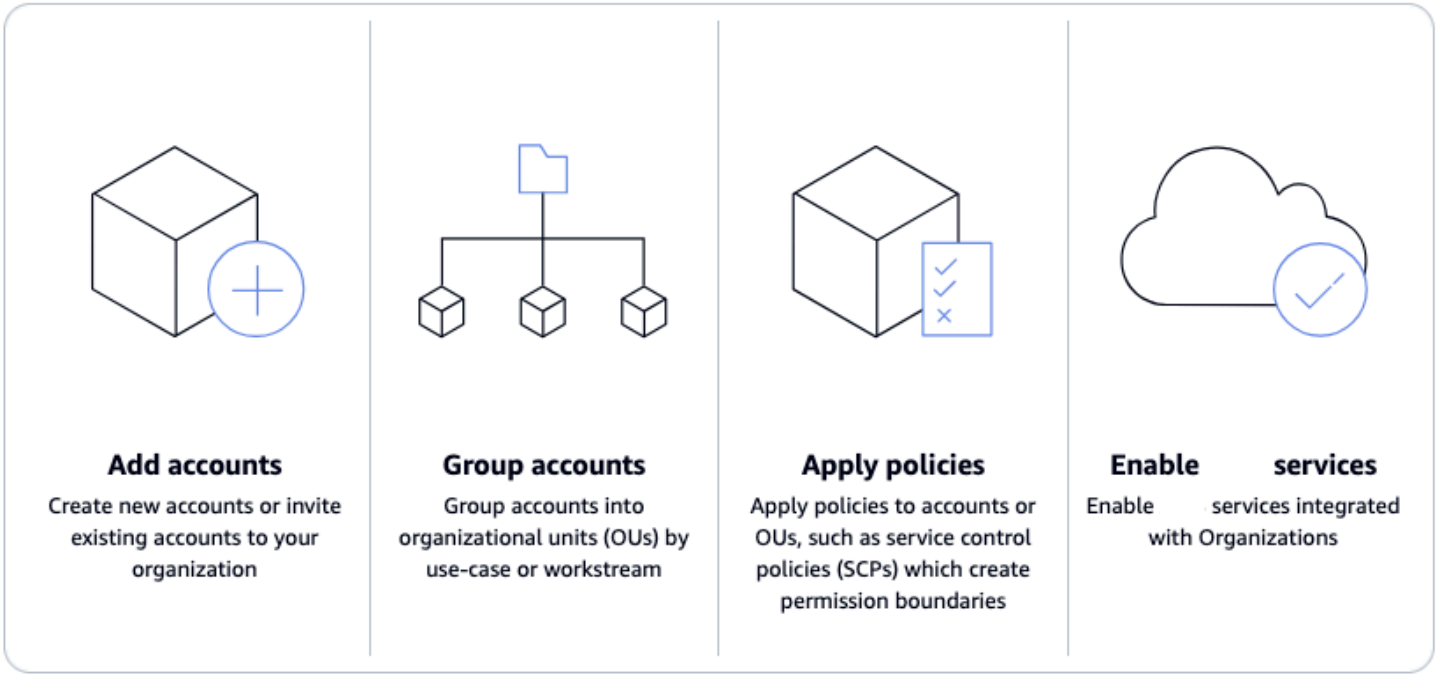
在扩展 Amazon 资源时集中管理您的环境

Amazon Organizations 随着 Amazon 资源的增长和扩展，可以帮助你集中管理和治理环境。通过使用 Organizations，您可以创建账户并分配资源，对账户进行分组以组织工作流，应用策略以满足治理的需要，并通过对所有账户使用统一的付款方式来简化账单。

Organizations 与其他组织集成， Amazon Web Services 服务 因此您可以定义中央配置、安全机制、审计要求以及组织中不同账户的资源共享。有关更多信息，请参阅 与其他 Amazon Organizations 人一起使用 Amazon Web Services 服务。

下图展示了有关如何使用 Amazon Organizations的高级别说明：

- 添加账户
- 账户分组
- 应用策略
- 启用 Amazon Web Services 服务。



主题

- 的功能 Amazon Organizations

- 的用例 Amazon Organizations
- 的术语和概念 Amazon Organizations
- 的配额和服务限制 Amazon Organizations
- 区域支持 Amazon Organizations
- Amazon Organizations 的计费和定价
- 对 Amazon Organizations 的支持和反馈

的功能 Amazon Organizations

Amazon Organizations 提供以下功能：

管理你的 Amazon Web Services 账户

Amazon Web Services 账户 是权限、安全性、成本和工作负载的自然界限。随着云环境的扩展，一个建议的最佳做法是使用多账户环境。您可以使用 Amazon Command Line Interface (Amazon CLI)、或，以编程方式创建新账户 SDKs，并使用集中为这些账户配置推荐的资源和权限 APIs，从而简化账户的Amazon CloudFormation StackSets创建。

定义和管理组织

创建新帐户时，可以将其分组为组织单位 (OUs)，或者为单个应用程序或服务提供服务的帐户组。应用标签策略以对组织中的资源进行分类或跟踪，并为用户或应用程序提供基于属性的访问控制。此外，您可以将支持的责任委托 Amazon Web Services 服务 给账户，以便用户可以代表您的组织对其进行管理。

保护和监控账户

您可以集中为安全团队提供工具和访问权限，使其能够代表组织管理安全需求。例如，您可以跨账户提供只读安全访问权限，使用 Amazon GuardDuty 检测和缓解威胁，使用 IA M Access Analyzer 查看对资源的意外访问，使用 A mazon Macie 保护敏感数据。

控制访问和权限

设置 Amazon IAM Identity Center 来提供使用活动目录访问 Amazon Web Services 账户 和资源的权限，并根据单独的工作角色自定义权限。您也可以将组织策略应用于用户、账户或 OUs。例如，服务控制策略 (SCPs) 使您能够控制对组织内 Amazon 资源、服务和区域的访问权限。资源控制策略 (RCPs) 使您能够集中防止意外使用您的 Amazon 资源。聊天机器人策略使您可以控制聊天应用程序（例如 Slack 和 Microsoft Teams）对组织账户的访问权限。

跨账户共享资源

您可以使用 Amazon Resource Access Manager (Amazon RAM) 在组织内共享 Amazon 资源。例如，您可以一次创建 Amazon Virtual Private Cloud（Amazon VPC）子网并在整个组织共享。您还可以使用 Amazon License Manager 集中同意软件许可，并使用 Amazon Service Catalog 跨账户共享 IT 服务和自定义产品目录。

审计环境是否合规

您可以跨账户激活 Amazon CloudTrail，这将创建云环境中所有活动的日志，成员账户无法关闭或修改这些日志。此外，您可以设置策略以按照您指定的节奏强制执行备份 Amazon Backup，或者为跨账户和的资源定义推荐 Amazon Web Services 区域 的Amazon Config配置设置。

集中管理账单和成本

Organizations 提供了统一的整合账单。此外，您可以使用 Amazon Cost Explorer 跨账户查看资源使用情况并跟踪成本，以及使用 Amazon Compute Optimizer 优化计算资源的使用情况。

的用例 Amazon Organizations

以下是一些用例 Amazon Organizations：

自动创建工作负载 Amazon Web Services 账户 并对其进行分类

您可以自动创建 Amazon Web Services 账户 以快速启动新的工作负载。将账户添加到用于即时应用安全策略、非接触式基础设施部署和审计的用户定义组。创建单独的群组来对开发和生产账户进行分类，并使用它Amazon CloudFormation StackSets为每个群组提供服务和权限。

定义和强制实施审计和合规策略

您可以应用服务控制策略 (SCPs) 来确保您的用户仅执行符合您的安全和合规性要求的操作。使用 Amazon CloudTrail 创建整个组织所执行所有操作的集中日志。跨账户和 Amazon Web Services 区域 使用查看和强制执行标准资源配置Amazon Config。使用 Amazon Backup 自动应用常规备份。Amazon Control Tower用于为您的 Amazon 工作负载应用预打包的安全性、运营和合规性监管规则。

为安全团队提供工具和访问权限，同时鼓励开发

创建安全组并为其提供对所有资源的只读访问权限，从而识别和缓解安全问题。您可以允许该小组管理 Amazon， GuardDuty以便他们能够主动监控和缓解对您的工作负载的威胁，并允许 IAM Access Analyzer 快速识别对您的资源的意外访问。

跨账户共享通用资源

Organizations 可让您轻松跨账户共享关键的中央资源。例如，您可以通过共享中央 Amazon Directory Service for Microsoft Active Directory，来让应用程序可以访问您的中央身份存储。

跨账户共享关键的中央资源

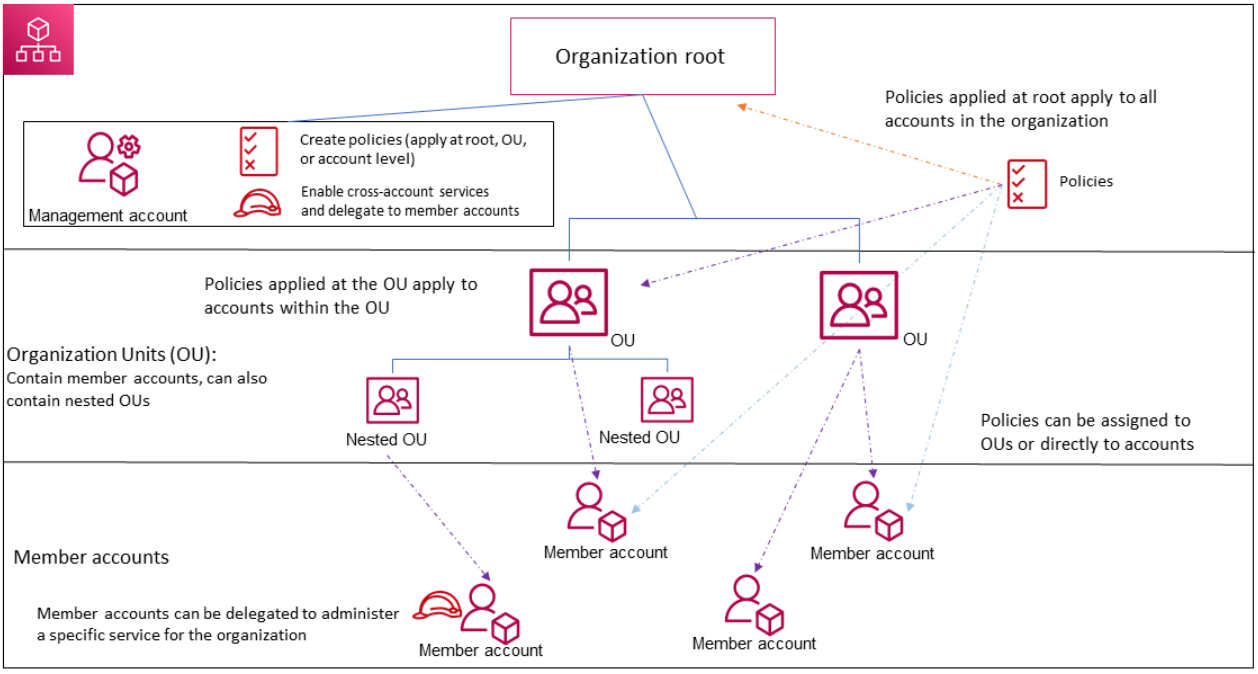
将 Amazon Directory Service for Microsoft Active Directory 作为应用程序的中央身份存储共享。使用 Amazon Service Catalog 在指定账户中共享 IT 服务，从而让用户可以快速发现和部署经批准的服务。通过集中定义一次应用程序资源，然后使用 Amazon Resource Access Manager（Amazon RAM）在组织中共享这些资源，从而确保在您的 Amazon Virtual Private Cloud（Amazon VPC）子网上创建这些资源。

的术语和概念 Amazon Organizations

本主题解释了的一些关键概念 Amazon Organizations。

下图显示了一个由五个账户组成的组织，这些账户在根目录下组织成四个组织单位 (OUs)。该组织还有几项政策附加到其中一些账户 OUs 或直接附在账户上。

有关这些项目中每一项的描述，请参阅本主题中的定义。



主题

可用的功能集

所有功能（推荐）

所有功能都是可用的默认功能集 Amazon Organizations。您可以为整个组织设置集中策略和配置要求，在组织内创建自定义权限或功能，通过统一的账单管理和组织账户，以及代表组织将责任委派给其他账户。您还可以使用与其他 Amazon Web Services 服务 的集成，来定义组织中所有成员账户的集中配置、安全机制、审计要求和资源共享。有关更多信息，请参阅 与其他 Amazon Organizations 人一起使用 Amazon Web Services 服务。

除管理功能外，所有功能模式还提供整合账单的所有功能。

整合账单

整合账单是提供共享账单功能的功能集，但不包括的更高级的功能 Amazon Organizations。例如，您不能允许其他 Amazon 服务与您的组织集成，以便在其所有账户中运行，也不能使用策略来限制不同账户中的用户和角色可以执行的操作。

您可以为最初仅支持整合账单功能的组织启用所有功能。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。有关更多信息，请参阅 通过以下方式为组织启用所有功能 Amazon Organizations。

组织结构

组织

组织是您可以按照树形层次结构来集中管理和组织的 Amazon Web Services 账户集合，其中根位于顶部，组织单元嵌套在根下。每个账户可以直接位于根目录中，也可以放置在层次结构 OUs 中的一个中。

每个组织都包括：

- 一个管理账户
- 零个或多个成员账户
- 零个或多个组织单位 (OUs)
- 零个或多个策略。

一个组织的功能由您启用的功能集决定。

根

管理根（根）包含在管理账户中，是组织 Amazon Web Services 账户的起点。根是位于组织层次结构中最顶层的容器。在此根目录下，您可以创建组织单位 (OUs) 来对您的账户进行逻辑分组，并将其组织 OUs 成最符合您需求的层次结构。

如果您将管理策略应用于根目录，则该策略将应用于所有组织单位 (OUs) 和帐户，包括该组织的管理帐户。

如果您将授权策略（例如，服务控制策略 (SCP)）应用于根目录，则该策略将应用于组织中的所有组织单位 (OUs) 和成员帐户。该策略不会应用到组织的管理账户。

> **Note**
>
> 你只能有一个根。 Amazon Organizations 创建组织时会自动为您创建根目录。

组织部门（OU）

组织单位（OU）是组织内的一组 Amazon Web Services 账户。OU 也可以包含其他组织单位，OUs 使您能够创建层次结构。例如，您可以将属于同一部门的所有账户归入一个部门 OU。同样，您可以将所有运行安全服务的账户归入一个安全 OU。

OUs 当你需要对组织中的一部分账户应用相同的控制时，这很有用。嵌套 OUs 可实现更小的管理单元。例如，您可以为每个工作负载创建 OUs ，然后在每个工作负载 OU OUs 中创建两个嵌套工作负载，将生产工作负载与预生产工作负载分开。除了直接分配给团队级 OU 的任何控制之外，它们还 OUs 继承父组织单位的策略。包括根目录和在最低层 Amazon Web Services 账户 创建的层级 OUs，你的层次结构可以深度为五级。

Amazon Web Services 账户

Amazon Web Services 账户是您的 Amazon 资源的容器。您可以在中创建和管理您的 Amazon 资源 Amazon Web Services 账户，并 Amazon Web Services 账户 提供访问和计费的管理功能。

使用多个 Amazon Web Services 账户 是扩展环境的最佳实践，因为它提供了成本计费边界，隔离了安全资源，为个人和团队提供了灵活性，此外还可以适应新流程。

> **Note**
>
> Amazon 账户不同于用户。用户是您使用 Amazon Identity and Access Management（IAM）创建的身份，可以是具有长期凭证的 IAM 用户，也可以是具有短期凭证的 IAM 角色。一个 Amazon 账户可以而且通常确实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

管理账户是 Amazon Web Services 账户 您用来创建组织的。从管理账户中可以执行以下操作：

- 在组织中创建其他账户
- 邀请其他账户加入您的组织和管理邀请
- 指定委派管理员账户
- 从组织中移除账户
- 将策略附加到组织内的根目录、组织单位 (OUs) 或账户等实体
- 启用与支持的 Amazon 服务的集成，为组织中的所有账户提供服务功能。

管理账户是组织的最终所有者，对组织的安全、基础设施和财务策略拥有最终控制权。此账户具有付款人账户的角色，并负责支付其组织中账户产生的所有费用。

> **Note**
>
> 您无法更改组织中的管理账户。

成员帐户

除管理账户外 Amazon Web Services 账户，成员账户是组织的一部分。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。您还可以将策略应用到成员账户。

> **Note**
>
> 一个成员账户一次属于一个组织。您可以将成员账户指定为委派管理员账户。

委派管理员

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

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

邀请和握手

邀请

邀请是请求其他账户加入组织的过程。邀请只能由组织的管理账户发出。邀请扩展到与受邀账户相关联的账户 ID 或电子邮件地址。受邀账户接受邀请后，它将成为组织中的成员账户。如果组织需要所有当前成员账户批准将仅支持整合账单功能更改为支持组织中的所有功能，也可以将邀请发送到所有成员。通过交换握手信息，对各个账户发出邀请。在 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，则必须直接使用握手。

握手

握手是在双方之间交换信息的多步骤过程。它的主要用途之一 Amazon Organizations 是用作邀请的底层实现。握手消息在握手发起方和接收方之间传递并由双方进行响应。消息的传递方式有助于确保双方知道当前状态是什么。将组织从仅支持整合账单功能更改为支持 提供的所有功能 Amazon Organizations 时，也可以使用握手。通常，只有在使用 Amazon Organizations API 或命令行工具（例如）时，才需要直接与握手交互。 Amazon CLI

组织政策

策略是一个 “文档”，其中包含一个或多个语句，用于定义要应用于一组的控件 Amazon Web Services 账户。 Amazon Organizations 支持授权策略和管理策略。

授权策略

授权策略可帮助您集中管理 Amazon Web Services 账户 整个组织的安全性。

服务控制策略 (SCP)

服务控制策略是一种对组织中 IAM 用户和 IAM 角色的最大可用权限进行集中控制的策略。

这意味着 SCPs 要指定以主体为中心的控制。 SCPs 创建权限护栏，或对成员账户中委托人可用的最大权限设置限制。当您想要对组织中的委托人集中实施一致的访问控制时，可以使用 SCP。

这可能包括指定您的 IAM 用户和 IAM 角色可以访问哪些服务，他们可以访问哪些资源，或者他们可以在什么条件下提出请求（例如，来自特定区域或网络）。有关更多信息，请参阅 SCPs。

资源控制政策 (RCP)

资源控制策略是一种对组织中资源的最大可用权限进行集中控制的策略。

这意味着 RCPs 要指定以资源为中心的控制措施。 RCPs 为成员账户中的资源的最大可用权限创建权限护栏或设置限制。如果您想对组织中的资源集中实施一致的访问控制，请使用 RCP。

这可能包括限制对资源的访问权限，使其只能由属于您的组织的身份进行访问，或者指定组织外部身份可以访问您的资源的条件。有关更多信息，请参阅 RCPs。

管理策略

管理策略可帮助您在整个组织中集中配置 Amazon Web Services 服务 和管理其功能。

声明性政策

声明式策略是一种策略，允许您在整个组织中大规模集中声明和强制执行给定 Amazon Web Services 服务 配置所需的配置。附加后，当服务添加新功能时，配置将始终保持不变 APIs。有关更多信息，请参阅声明性策略。

备份策略

备份策略是一种策略，允许您集中管理备份计划并将其应用于组织账户中的 Amazon 资源。有关更多信息，请参阅备份策略。

标签策略

标签策略是一种策略，允许您标准化附加到组织账户中 Amazon 资源的标签。有关更多信息，请参阅标签策略。

聊天机器人策略

聊天机器人策略是一种策略，允许你控制聊天应用程序（例如 Slack 和 Microsoft Teams）对组织帐户的访问权限。如需了解更多信息，请参阅 Chatbot 政策。

AI 服务选择退出策略

AI 服务选择退出策略是一种策略，允许您控制组织中所有账户的 Amazon AI 服务数据收集。有关更多信息，请参阅 AI 服务选择退出政策。

的配额和服务限制 Amazon Organizations

本主题介绍的配额和服务限制 Amazon Organizations。

命名指南

以下是您在中创建的名称的指导原则 Amazon Organizations，包括帐户名称、组织单位 (OUs)、根和策略：

- 名称必须由 Unicode 字符组成。
- 名称的最大字符串长度因对象而异。有关每个对象的实际限制的信息，请参阅 Amazon Organizations API 参考并找到创建该对象的 API 操作，然后查看该操作的 Name 参数详细信息。例如：账户名称或者 OU 名称。

注意事项

由于更新，服务配额代码可能会随着时间的推移而发生变化。这不会影响配额值或名称。要查找特定配额的配额代码，请使用ListServiceQuotas操作，然后在输出中查找所需配额的QuotaCode响应。

最大值和最小值

以下是中实体的默认最大值。 Amazon Organizations

> **Note**
>
> 您可以使用服务限额控制台请求增加其中一些值。
> Organizations 是一项物理托管在美国东部（弗吉尼亚北部）区域（us-east-1）的全球服务。因此，在使用 us-east-1 Service Quotas 控制台、或 Amazon SDK 时，必须使用来访问 Organi Amazon CLI zations 配额。

描述	限制
组织 Amazon Web Services 账户 中的人数	10 – 一个组织中允许的原定设置最大账户数。如果您需要更多，则可以使用服务限额控制台请求增加。 注意：只有组织的管理账户才能提交此配额增加请求。根据客户的资格和要求，最多可以准予将限制增加到 1 万个账户。对于新创建的账户和组织，此配额可能能会低于默认的 10 个账户。 发送到账户的邀请将计入此限额。如果受邀账户拒绝邀请、管理账户取消邀请或邀请过期，则撤销此计数。 账户注销后，不会停止计算此配额的使用情况，直到账户永久注销为止。有关何时永久注销账户的更多信息，请参阅《Amazon 账户管理参考指南》中的 Post-closure period。 一些服务存在账户限制，账户限制与组织中允许的最大账户数量分开计算。有关更多信息，请参阅按 Amazon 服务划分的限制。
组织中的根数量	1
组织 OUs 中的人数	1000
组织中的每种类型的策略数量	服务控制策略：2000 资源控制策略：1000 声明性政策：1000 备份策略：1000 标签策略：1000 聊天机器人策略：1000 AI 服务选择退出策略：1000
策略文档的最大大小	服务控制策略：5120 个字符 资源控制策略：5120 个字符

描述	限制
	声明性策略：10,000 个字符 备份策略：10000 个字符 聊天机器人策略：1 万个字符 AI 服务选择退出策略：2500 个字符 标签策略：10000 个字符 注意：如果您使用保存策略 Amazon Web Services Management Console，则 JSON 元素之间和引号之外的多余空格（例如空格和换行符）将被移除且不计算在内。如果您使用 SDK 操作或保存策略 Amazon CLI，则策略将完全按照您提供的方式保存，并且不会自动删除字符。
根中的最大 OU 嵌套数	根 OUs 深处有五个关卡。
您可在 24 小时内可以执行的最大邀请尝试次数	您组织中允许的最大账户数或 20 个账户（以较大值为准）。已接受的邀请不计入此配额。一旦某个邀请被接受，您就可以发送另一个同一天的邀请。 如果您的组织中允许的最大账户数少于 20，则如果您尝试邀请超过组织所能容纳的账户数，则会出现“超出账户限制”异常。但是，您可以在一天内取消邀请并发送多次新邀请（最多 20 次尝试）。
您可以同时创建的成员账户数量	5 – 一个创建完成后即可开始另一个，但正在进行中的只能有五个。
您可以在 30 天的周期内关闭的成员账户数量	组织中 10% 的成员账户，最多 1000 个成员账户。 • < 100 个账户 – 您最多可以关闭 10 个成员账户 • 100 – 1 万个账户 – 您最多可以注销 10% 的成员账户 • > 1 万个账户 – 您最多可以注销 1000 个成员账户 达到此配额后，您可以注销额外的账户或等待您的配额重置。有关更多信息，请参阅《Amazon 账户管理指南》中的关闭Amazon账户。

描述	限制
您可以同时关闭的成员账户数量	3 – 同一时间只能处理三个账户关闭。一个账户关闭完成后，您就可以关闭另一个账户。
可以附加到策略的实体数	无限制
您可以附加到根、OU 或账户的标签数	50
基于资源的委托策略的最大大小	40000 个字符

按 Amazon 服务划分的限制

大多数都 Amazon Web Services 服务 支持您在组织中可以拥有的最大账户数量。但一些服务存在账户限制，账户限制与组织中允许的最大账户数量分开计算。

下表展示了具有单独账户限制的服务。

Amazon 服务	限制	能否增加
Amazon IAM Identity Center	3000	是
Amazon Application Migration Service	5000	否
Amazon Directory Service	250	是

有关更多信息，请参阅《IAM Identity Center 用户指南》中的 Amazon IAM Identity Center quotas，以及《Application Migration Service 用户指南》中的 Amazon MGN service quota limits。

握手的过期时间

以下是中握手的超时时间。 Amazon Organizations

描述	限制
邀请加入组织	15 天
请求启用组织中的所有功能	90 天
握手将被删除，不再显示在列表中	握手完成后 30 天

可附加到实体的策略数

最小值和最大值取决于策略类型以及您要将策略附加到的实体。下表显示了各种策略类型以及可将每种类型附加到的实体数。

> **Note**
>
> 这些数字仅适用于那些直接附加到 OU 或账户的策略。通过继承影响 OU 或账户的策略不计入这些限制。所有策略限制都属于硬限制。

策略类型	附加到实体的数量上限	附加到根的数量上限	每个 OU 附加的数量上限	每个账户附加的数量上限
服务控制策略	1 — 启用 SCPs时，每个实体必须始终至少连接一个 SCP。您无法从实体上删除最后一个 SCP。	5	5	5
资源控制政策	1 — 启用后，该`RCPFullAWSAccess` 策略会自动附加到根目录、每个 OU 以及组织中的每个账户 RCPs。您无法分	5	5	5

策略类型	附加到实体的数量上限	附加到根的数量上限	每个 OU 附加的数量上限	每个账户附加的数量上限
	离此策略，它会计入 5 个策略的配额。			
声明性政策	0	10	10	10
备份策略	0	10	10	10
标签策略	0	10	10	10
聊天机器人策略	0	5	5	5
AI 服务选择退出策略	0	5	5	5

> **Note**
>
> 一个组织中只能有一个根。

节流限制

下表 Amazon Organizations APIs 按管理类别列出了这些类别，并显示了它们在账户和组织层面各自的限制率。

Amazon Organizations 使用令牌桶算法实现 API 限制。使用此算法，您的账户拥有一个持有特定数量的令牌的存储桶。存储桶中的令牌数表示您在任何给定秒钟的节流配额。

速率是每秒将代币添加到代币桶中的固定速度。

Burst 是可以添加的最大代币数量和每秒可以使用的最大代币数量。

例如，`DescribeAccount`API 的基准速率限制 Amazon Web Services 账户 为每秒 20 个请求，突发速率限制为每秒 30 个请求。每秒 30 个请求的突发速率允许您暂时超过每秒 20 个请求的基准速率。

你可以在第一秒钟内发出 20 个请求，这是基准速率。在接下来的几秒钟内，你可以发出 30 个请求，超过基准，但保持在 30 的突发速率之内。但是，在第三秒钟中，如果您尝试发出的请求超过 20 个，则会受到限制，因为您已超过基准速率并且已使用突发容量。

只要每秒的平均请求量在一段时间内保持在基准限制之内，突发速率就可以在不受到限制的情况下处理临时的流量峰值。

账户管理限制

下表列出了 Amazon Organizations APIs 用于账户管理的。

Amazon Organizations API	每账户限制（速率、突发量）	每组织限制（速率、突发量）
CloseAccount	0.05、1	
CreateAccount, CreateGovCloudAccount	0.1、3	
DescribeAccount	20、30	24、36
DescribeCreateAccountStatus	2、2	2、3
LeaveOrganization	1、1	
ListCreateAccountStatus	5、8	6、10

握手管理限制

下表列出了账户 Amazon Organizations APIs 的握手。

Amazon Organizations API	每账户限制（速率、突发量）	每组织限制（速率、突发量）
AcceptHandshake	1、2	5、5
DescribeHandshake	1、2	6、10
CancelHandshake	2、3	
DeclineHandshake	1、1	5、5
InviteAccountToOrganization	3、5	

Amazon Organizations API	每账户限制（速率、突发量）	每组织限制（速率、突发量）
ListHandshakesForAccount, ListHandshakesForOrganization	5、8	6、10

组织管理限制

下表列出了 Amazon Organizations APIs 用于组织管理的。

Amazon Organizations API	每账户限制（速率、突发量）	每组织限制（速率、突发量）
CreateOrganization, DeleteOrganization, EnableFullControl	1、1	
CreateOrganizationalUnit, DescribeOrganization	1、2	
MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit	2、3	
DescribeOrganizationalUnit	2、2	2、3
ListAccounts	8、12	9、15
ListChildren	6、10	7、12
ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent	5、8	6、10
ListRoots	1、2	1、3
ListTagsForResource	10、15	12、18
RemoveAccountFromOrganization	2、2	

Amazon Organizations API	每账户限制（速率、突发量）	每组织限制（速率、突发量）
TagResource, UntagResource	4、6	

策略管理限制

下表列出了 Amazon Organizations APIs 用于策略管理的。

Amazon Organizations API	每账户限制（速率、突发量）	每组织限制（速率、突发量）
CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy	2、3	
DescribePolicy	2、2	2、3
DisablePolicyType, EnablePolicyType	1、1	
ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy	5、8	6、10
UpdatePolicy	2、3	

服务管理限制

下表列出了 Amazon Organizations APIs 用于服务管理的。

Amazon Organizations API	每账户限制（速率、突发量）	每组织限制（速率、突发量）
启用AWSService访问，禁用AWSService访问	1、2	
清单 AWSServiceAccessForOrganization， ListDelegatedServicesForAccount	1、3	1、4
ListDelegatedAdministrators	5、8	6、10

Amazon Organizations API	每账户限制（速率、突发量）	每组织限制（速率、突发量）
RegisterDelegatedAdministrator, DeregisterDelegatedAdministrator	1、2	

区域支持 Amazon Organizations

Amazon Organizations 适用于所有 Amazon 商业区域和中国地区。 Amazon GovCloud (US) Regions

有关中功能差异的列表 Amazon GovCloud (US) Regions，请参阅Amazon Organizations 中的 Amazon GovCloud (US)。

有关中国地区功能差异的列表，Amazon Organizations 请参见中国。

Organizations 服务端点的位置：

- 面向商业组织的端点位于美国东部（弗吉尼亚州北部）区域
- 在 Amazon GovCloud （美国西部）适用于组织 Amazon GovCloud (US)
- 面向中国组织的端点位于由宁夏西云数据科技有限公司（西云数据）中国（宁夏）区域。

除了在中国管理的组织之外，所有组织实体都可以在全球范围内访问，这与当前 (IAM) 的工作方式类似。 Amazon Identity and Access Management 在创建和管理组织 Amazon Web Services 区域 时，您无需指定，但需要为在中国使用的账户创建一个单独的组织。您的用户 Amazon Web Services 账户可以在提供该服务的任何地理区域 Amazon Web Services 服务 中使用。

> **Note**
>
> 标签策略仅在部分区域中受支持
> 标签策略 是策略的一种类型，可帮助您在组织账户中跨资源标准化标签。只有支持 Organizations 的区域子网才支持标签策略。有关支持标签策略的区域列表，请参阅标签策略 | 支持区域。

可用清单 Amazon Web Services 区域

下表列出了可用的 Amazon Web Services 区域。

区域名称	区域	端点	协议
美国东部（俄亥俄州）	us-east-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
美国东部（弗吉尼亚州北部）	us-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
美国西部（加利福尼亚北部）	us-west-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
美国西部（俄勒冈州）	us-west-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
非洲（开普敦）	af-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
亚太地区（香港）	ap-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
亚太地区（海得拉巴）	ap-south-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
亚太地区（雅加达）	ap-southeast-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
亚太地区（马来西亚）	ap-southeast-5	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS

区域名称	区域	端点	协议
亚太地区（墨尔本）	ap-southeast-4	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
亚太地区（孟买）	ap-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
亚太地区（大阪）	ap-northeast-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
亚太地区（首尔）	ap-northeast-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
亚太地区（新加坡）	ap-southeast-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
亚太地区（悉尼）	ap-southeast-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
亚太地区（泰国）	ap-southeast-7	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
亚太地区（东京）	ap-northeast-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
加拿大（中部）	ca-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS

区域名称	区域	端点	协议
加拿大西部（卡尔加里）	ca-west-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
中国（北京）	cn-north-1	organizations.cn-northwest-1.amazonaws.com.cn	HTTPS
中国（宁夏）	cn-northwest-1	organizations.cn-northwest-1.amazonaws.com.cn	HTTPS
欧洲地区（法兰克福）	eu-central-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
欧洲地区（爱尔兰）	eu-west-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
欧洲地区（米兰）	eu-south-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
欧洲（西班牙）	eu-south-2	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS
欧洲地区（斯德哥尔摩）	eu-north-1	organizations.us-east-1.amazonaws.com	HTTPS
		organizations-fips.us-east-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
欧洲（苏黎世）	eu-central-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
以色列（特拉维夫）	il-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
墨西哥（中部）	mx-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
中东（巴林）	me-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
中东（阿联酋）	me-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
南美洲（圣保罗）	sa-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS

Amazon Organizations 的计费和定价

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。

谁为我组织中 Amazon 成员账户下的用户产生的使用量付费？

管理账户的所有者负责为组织中账户使用的所有使用量、数据和资源付费。

我的账单会反映我在组织中创建的组织单位结构吗？

您的账单不会反映您在组织中定义的结构。您可以在单独的 Amazon Web Services 账户中使用成本分配标签，来分类和跟踪 Amazon 成本，此分配将在组织的整合账单中可见。

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 支持 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。

有关多账户环境的最佳实践

请遵循这些建议，帮助您完成在中设置和管理多账户环境的过程。 Amazon Organizations

主题

账户和凭证

启用 root 访问权限管理以简化成员账户的 root 用户凭证的管理

我们建议您启用 root 访问权限管理，以帮助您监控和删除成员账户的 root 用户证书。根访问权限管理可防止根用户凭证的恢复，从而提高组织中的账户安全性。

- 删除成员账户的 root 用户凭证，以防止登录 root 用户。这还会阻止恢复成员帐户的根用户。
- 假设特权会话对成员账户执行以下任务：
  - 删除一项配置错误的存储桶策略，此策略拒绝所有主体访问 Amazon S3 存储桶策略。
  - 删除将会拒绝所有主体访问 Amazon SQS 队列的 Amazon Simple Queue Service 基于资源的策略。
  - 允许成员账户恢复其根用户证书。有权访问该成员账户的根用户电子邮件收件箱的人可以重置 root 用户密码并以成员账户 root 用户身份登录。

启用根访问管理后，新创建的成员账户将没有根用户证书，这样就无需在配置后提供额外的安全保护，例如MFA。 secure-by-default

有关更多信息，请参阅《用户指南》中的 “集中管理成员账户的根Amazon Identity and Access Management 用户证书”。

确保更新联系电话号码

要恢复对您的访问权限 Amazon Web Services 账户，请务必拥有一个有效且有效的联系电话号码，以便您能够接收短信或来电。我们建议您使用专用的电话号码，以确保该号码 Amazon 可以联系您以获

得账户支持和恢复资金。您可以通过 Amazon Web Services Management Console 或账户管理轻松查看和管理您的账户电话号码 APIs。

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

在 Amazon 联系信息控制台页面中记录电话号码，并与组织中必须知道该号码的特定团队共享其详细信息。这种方法可帮助尽可能减少将电话号码转移到其他 SIM 卡相关的风险。根据您现有的信息安全策略存储电话。但是，请勿将电话存储在与其他相关凭证信息相同的位置。对电话或其保管位置的任何访问都应记录和监控。如果与账户关联的电话号码发生变化，请根据相关流程更新现有文档中记录的电话号码。

为根用户使用组电子邮件地址

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

组织结构和工作负载

在单个组织中管理账户

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

根据业务目的而不是报告架构对工作负载进行分组

我们建议您将生产工作负载环境和数据隔离在面向工作负载的顶级工作负载 OUs下。您 OUs 应该基于一组通用的控制措施，而不是反映公司的报告结构。除了生产之外 OUs，我们建议您定义一个或多个非生产环境，其中 OUs 包含用于开发和测试工作负载的帐户和工作负载环境。有关其他指导，请参阅组织面向工作负载 OUs。

使用多个账户来整理工作负载

为您的 Amazon 资源 Amazon Web Services 账户 提供了自然的安全性、访问权限和计费界限。使用多个账户有很多好处，因为这样可以分配账户级别的限额和 API 请求速率限制，其他好处 详见此处。

我们建议您使用多个 组织范围的基础账户，例如安全账户、日志记录账户和基础设施账户。对于工作负载账户，您应 利用不同的账户来隔离生产工作负载和测试/开发工作负载。

服务和成本管理

使用 Amazon 服务控制台或 API/CLI 操作在组织层面启用服务

作为最佳实践，我们建议您 Amazon Organizations 使用该服务的控制台或 API Operations/CLI 命令等效命令启用或禁用要与之集成的任何服务。使用此方法，该 Amazon 服务可以为您的组织执行所有必需的初始化步骤，例如在禁用服务时创建任何必需的资源和清理资源。 Amazon 账户管理 是唯一需要使用 Amazon Organizations 控制台或启 APIs 用的服务。要查看与之集成的服务列表 Amazon Organizations，请参阅Amazon Web Services 服务 你可以和它一起使用 Amazon Organizations。

使用计费工具跟踪成本并优化资源使用情况

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

制定标记策略并在组织资源中强制使用标签

随着账户和工作负载的扩展，利用标签可以有效地帮助跟踪成本、控制访问权限和整理资源。要了解标记命名策略，请按照为资源添加标签中的指导进行操作。 Amazon 除资源外，您还可以在组织根目录 OUs、账户和策略上创建标签。有关更多信息，请参阅 制定标记策略。

入门 Amazon Organizations

以下主题提供了有助您开始使用 Amazon Organizations的信息。您也可以使用以下教程开始使用 Amazon Organizations执行任务。

教程：创建和配置组织

开始使用 step-by-step有关创建组织、邀请您的第一个成员帐户、创建包含您账户的 OU 层次结构以及应用一些服务控制策略的说明（SCPs）。

教程：使用 Amazon 监控组织的重要变更 EventBridge

通过将 Amazon 配置 EventBridge 为在组织中发生您指定的操作时以电子邮件、SMS 短信或日志条目形式触发警报，监控组织中的关键变化。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。

主题

报名参加 Amazon

主题

注册获取 Amazon Web Services 账户

如果您没有 Amazon Web Services 账户，请完成以下步骤来创建一个。

要注册 Amazon Web Services 账户

1. 打开https://portal.aws.amazon.com/billing/注册。

2. 按照屏幕上的说明操作。

   在注册时，将接到电话，要求使用电话键盘输入一个验证码。

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

Amazon 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择 “我的账户”，查看您当前的账户活动并管理您的账户。

保护 IAM 用户

注册后 Amazon Web Services 账户，开启多重身份验证 (MFA)，保护您的管理用户。有关说明，请参阅《IAM 用户指南》中的 为 IAM 用户启用虚拟 MFA 设备（控制台）。

要允许其他用户访问您的 Amazon Web Services 账户 资源，请创建 IAM 用户。为了保护您的 IAM 用户，请启用 MFA 并仅向 IAM 用户授予执行任务所需的权限。

有关创建和保护 IAM 用户的更多信息，请参阅《IAM 用户指南》中的以下主题：

- 在你的 IAM 用户中创建 Amazon Web Services 账户
- 适用于 Amazon 资源的访问权限管理
- 基于 IAM 身份的策略示例

正在访问 Amazon Organizations

您可以通过以下任何一种方式使用 Amazon Organizations ：

Amazon Web Services Management Console

Amazon Organizations 控制台是一个基于浏览器的界面，可用于管理您的 Amazon 组织和资源。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，你可以在系统的命令行中发出命令来执行 Amazon Organizations 和执行 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 提供了两组命令行工具：

- Amazon Command Line Interface

  Amazon Command Line Interface (Amazon CLI) 是用于管理您的统一工具 Amazon Web Services 服务。只需下载和配置一个工具，您就可以 Amazon Web Services 服务 从命令行控制多个工具，并通过脚本自动执行这些工具。

  有关安装和使用的信息 Amazon CLI，请参阅《Amazon Command Line Interface 用户指南》。

- Amazon Tools for Windows PowerShell

  Windows 工具 PowerShell 允许开发人员和管理员在 PowerShell 脚本环境中管理其 Amazon Web Services 服务 和资源。你可以使用与管理 Windows、Linux 和 macOS 环境相同的 PowerShell 工具来管理 Amazon 资源。

  有关安装和使用适用于 Windows 的工具的信息 PowerShell，请参阅《Amazon Tools for Windows PowerShell 用户指南》。

Amazon SDKs

Amazon SDKs 由各种编程语言和平台（例如 Java、Python、Ruby、.NET、iOS 和 Android）的库和示例代码组成。它们 SDKs 负责处理诸如对请求进行加密签名、管理错误和自动重试请求之类的任务。有关（包括如何下载和安装它们）的更多信息 Amazon SDKs，请参阅适用于 Amazon Web Services 的工具。

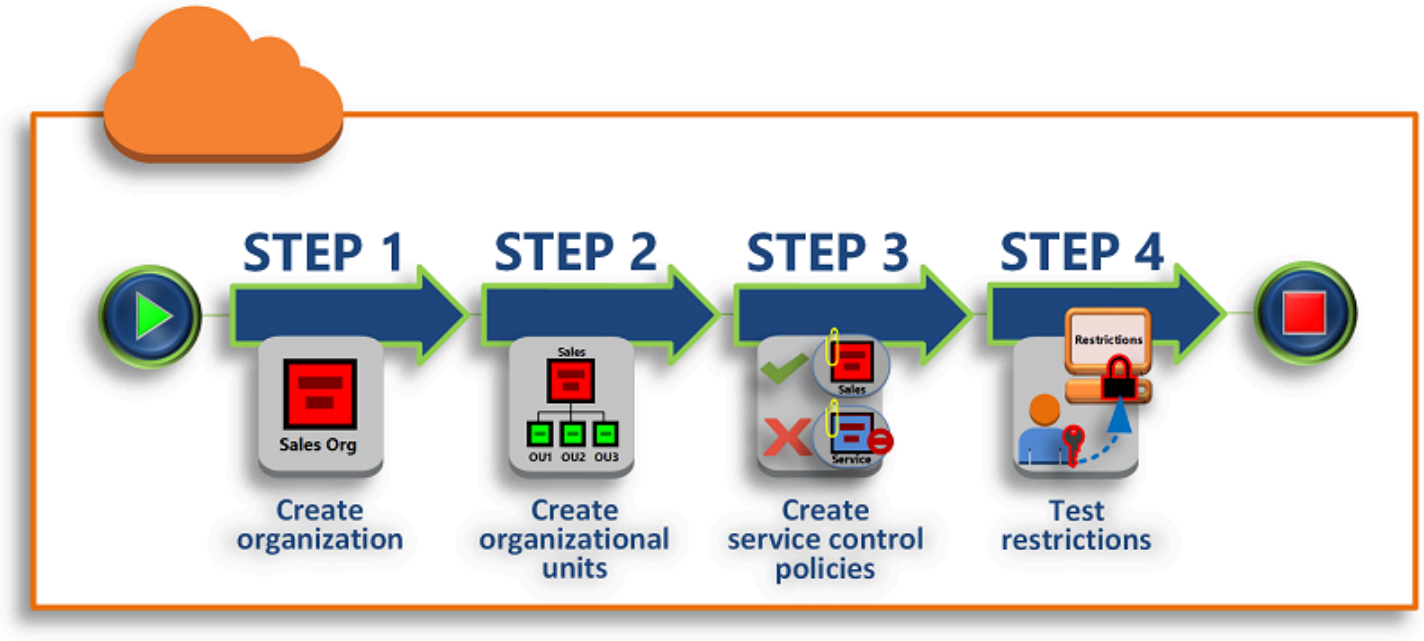
Amazon Organizations HTTPS 查询 API

Amazon Organizations HTTPS 查询 API 允许您以编程方式访问 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。

教程：创建和配置组织

在本教程中，您将创建您的组织并使用两个 Amazon 成员帐户对其进行配置。您可以在组织中创建其中一个成员账户，然后邀请另一个账户加入您的组织。接下来，您可以使用允许列表方法指定账户管理员只能委派明确列出的服务和操作。这允许管理员在允许贵公司的其他任何人使用新服务之前对其进行验证。 Amazon 这样，如果 Amazon 引入了新服务，则在管理员将该服务添加到相应策略的允许列表之前，该服务仍处于禁止状态。本教程还向您展示了如何使用拒绝列表来确保成员账户中的任何用户都无法更改 Amazon CloudTrail 创建的审核日志的配置。

下图演示了本教程的主要步骤。



步骤 1：创建组织

在此步骤中，您将使用当前账户 Amazon Web Services 账户 作为管理账户创建一个组织。您还可以 Amazon Web Services 账户 邀请一个人加入您的组织，然后创建第二个帐户作为成员帐户。

步骤 2：创建组织单元

接下来，在新组织中创建两个组织单位 (OUs)，并将成员帐户放入其中OUs。

步骤 3：创建服务控制策略

您可以使用服务控制策略（SCPs）限制可以委托给成员账户中的用户和角色的操作。在此步骤中，您将创建两个SCPs并将它们附加到组织OUs中的。

步骤 4：测试组织的策略

您可以以每个测试帐号的用户身份登录，并查看它们对帐号的影响。SCPs

本教程中的任何步骤都不会给您的 Amazon 账单带来费用。 Amazon Organizations 是一项免费服务。

先决条件

本教程假设您有权访问两个现有的 Amazon Web Services 账户 （在本教程中创建了第三个），并且您可以以管理员身份登录每个。

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 Amazon 身份登录并打开控制台。Amazon Organizations
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。

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 Amazon Organizations 的电子邮件地址验证。

您现在拥有一个组织，并且您的账户是其唯一成员。这是组织的管理账户。

邀请现有账户加入组织

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

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 “添加 Amazon Web Services 账户页面” 上，选择 “邀请现有用户” Amazon Web Services 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 身份证号，则可以改为输入。
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 “发送邀请”。 Amazon Organizations 向账户所有者发送邀请。

   > **Important**
   >
   > 如果有错误消息指示，请将其展开。如果错误指示您超出了组织的账户限制或因组织仍在初始化而无法添加账户，请在创建组织后等待一个小时，然后重试。如果错误仍然存在，请联系 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：
   - 打开从管理账户 Amazon 发送的电子邮件，然后选择接受邀请的链接。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)。

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

8. 注销成员账户，然后以管理账户管理员的身份登录。

创建成员账户

在本节的步骤中，您将创建 Amazon Web Services 账户 自动成为组织成员的。在本教程中，我们将此账户称为 333333333333。

Amazon Web Services Management Console

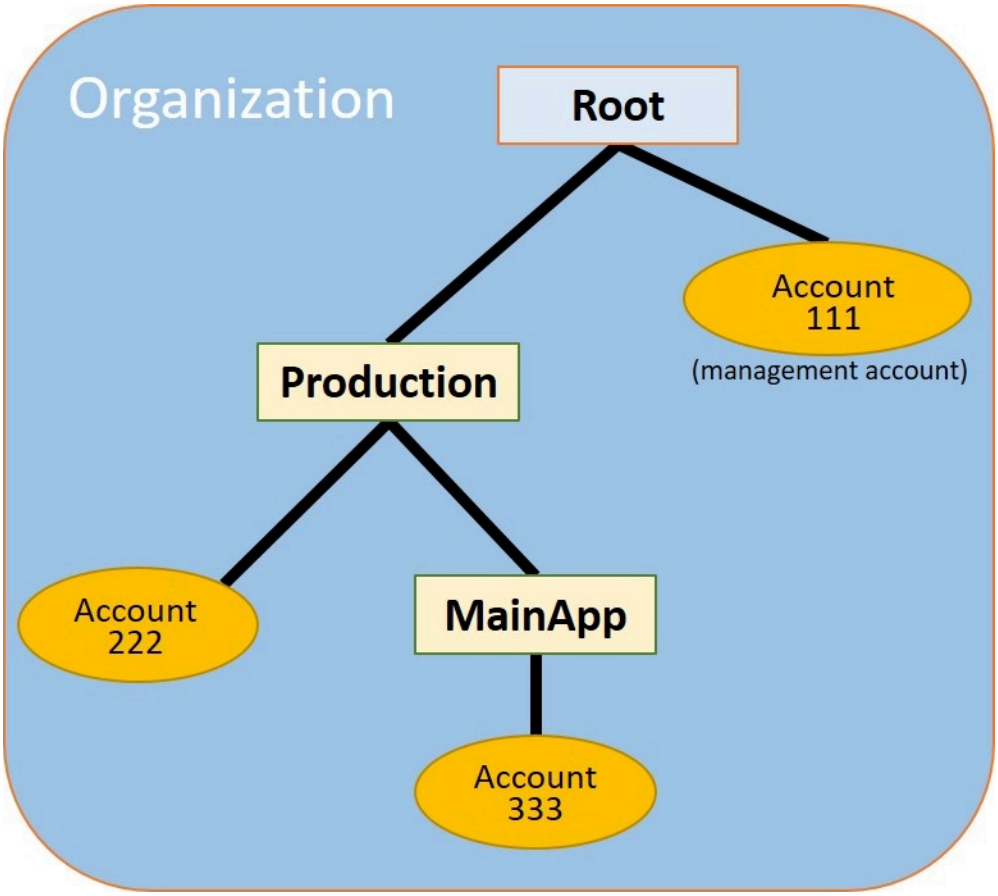
创建成员账户

1. 在 Amazon Organizations 控制台的Amazon Web Services 账户页面上，选择添加 Amazon Web Services 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角色名称，您可以将此项留空以自动使用默认的角色名称`OrganizationAccountAccessRole`，也可以提供自己的名称。此角色允许您在以管理账户中的IAM用户身份登录时访问新成员账户。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. 选择创建 Amazon Web Services 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

在本节的步骤中，您将创建组织单位 (OUs) 并将您的成员帐户放入其中。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。一个成员帐户移至生产 OU，另一个成员帐户移至 O MainApp U，后者是 Production 的子账户。



Amazon Web Services Management Console

要创建和填充 OUs

> **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. 选择操作下拉列表，然后在组织单位中，选择新建。
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，您可以将您的成员帐户转移到这些帐户中OUs。
8. 返回到Amazon Web Services 账户页面，然后选择 Production OU 旁边的三角形
   
   ，
   以展开该 OU 的树形图。这会将 MainAppOU 显示为生产的子项。
9. 在 333333333333 旁边，选中复选框
   
   （而
   不是其名称），选择操作，然后在 Amazon Web Services 账户 下选择移动。
10. 在 Amazon Web Services 账户 “移动” 333333333333” 页面上，
    选择 “制作” 旁边的三角形将其展开。在旁边 MainApp，选择单选按
    钮 
    （不
    是其名称），然后选择移动 Amazon Web Services 账户。
11. 在 222222222222 旁边，选中复选框
    
    （而
    不是其名称），选择操作，然后在 Amazon Web Services 账户 下选择移动。
12. 在移动 Amazon Web Services 账户 “22222222222222” 页面上，在 “制作” 旁边，选择单选按钮（不是其名称），然后选择 “移动”。 Amazon Web Services 账户

步骤 3：创建服务控制策略

在本节的步骤中，您将创建三个服务控制策略 (SCPs)，并将它们附加到根目录和上，OUs以限制组织账户中的用户可以执行的操作。第一种是SCP防止任何成员账户中的任何人创建或修改您配置的任何 Amazon CloudTrail 日志。管理账户不受任何影响SCP，因此在应用后 CloudTrail SCP，必须使用管理账户创建所有日志。

在根中为组织启用服务控制策略类型

您必须先为组织启用策略类型，然后才能附加任何类型的策略到该根或根中的任何 OU。默认情况下未启用策略类型。本节中的步骤向您展示如何为您的组织启用服务控制策略 (SCP) 类型。

Amazon Web Services Management Console

SCPs为您的组织启用

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

   将出现一个绿色横幅，通知您现在可以在组织SCPs中创建。

创建 SCPs

现在，您的组织中已启用服务控制策略，您可以创建本教程所需的三个策略。

Amazon Web Services Management Console

创建第一个SCP阻止 CloudTrail 配置操作的

1. 导航到策略页面，然后选择服务控制策略。
2. 在 Service control policies (服务控制策略) 页面上，选择 Create policy (创建策略)。
3. 对于 Policy name，输入 **`Block CloudTrail Configuration Actions`**。
4. 在 “策略” 部分的右侧服务列表中，选择 CloudTrail 该服务。然后选择以下操作：AddTags、CreateTrail、DeleteTrail、RemoveTagsStartLogging、StopLogging、和UpdateTrail。
5. 仍然在右侧窗格中，选择 “添加资源”，CloudTrail然后指定 “所有资源”。选择添加资源。

   左侧的策略语句应与以下内容类似。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. 选择创建策略。

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

Amazon Web Services Management Console

创建第二个策略，该策略将允许生产 OU 的已批准服务

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
}
```

4. 选择创建策略。

最终策略提供了禁止在 MainApp OU 中使用的服务的拒绝列表。在本教程中，您将屏蔽组织单位中的任何账户访问亚马逊 DynamoDB。MainApp

Amazon Web Services Management Console

创建第三个拒绝访问无法在 MainApp OU 中使用的服务的策略

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

   右侧的策略语句将更新为与以下内容类似的内容。

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

5. 选择创建策略以保存SCP。

将它们附加SCPs到你的 OUs

现在，您的根已SCPs存在并已启用，您可以将它们附加到根和OUs。

Amazon Web Services Management Console

将策略附加到根和 OUs

1. 导航到Amazon Web Services 账户页面。
2. 在Amazon Web Services 账户页面上，选择 Root (根)（其名称，而不是单选按钮）导航到其详细信息页面。
3. 在 Root (根) 详细信息页面上，选择 Policies (策略) 选项卡，然后在 Service Control Policies (服务控制策略) 下，选择 Attach (附加)。
4. 在附加服务控制策略页面上，选择SCP名称旁边的单选按钮`Block CloudTrail Configuration Actions`，然后选择附加。在本教程中，您将它附加到根目录，以便它影响所有成员帐户，以防止任何人更改您的配置 CloudTrail方式。

   根详细信息页面的 “策略” 选项卡现在显示两个已附加到根目录：一个SCPs是你刚刚附加的，另一个是默认的`FullAWSAccess`SCP。
5. 导航回Amazon Web Services 账户页面，然后选择 Production OU（它的名称，而不是单选按钮）导航到其详细信息页面。
6. 在 Production OU 的详细信息页面上，选择 Policies (策略) 选项卡。
7. 在 Service Control Policies (服务控制策略) 下，选择 Attach (附加)。
8. 在 Attach a service control policy (附加服务控制策略) 页面上，选择 `Allow List for All Approved Services` 旁边的单选按钮，然后选择 Attach (附加)。这允许 Production OU 的成员账户中的用户或角色访问批准的服务。
9. 再次选择 “策略” 选项卡，查看SCPs有两个策略已附加到 OU：一个是您刚刚附加的，另一个是默认的`FullAWSAccess`SCP。但是，由于`FullAWSAccess`SCP也是允许所有服务和操作的允许列表，因此您现在必须将其分离，SCP以确保只允许您批准的服务。
10. 要从生产 OU 中删除默认策略，请选择 F 的单选按钮ullAWSAccess，选择 “分离”，然后在确认对话框中选择 “分离策略”。

    删除此默认策略后，Production OU 下的所有成员账户将立即失去对您在前面步骤中附加的允许列表中未SCP包含的所有操作和服务的访问权限。任何使用未包含在所有已批准服务的允许

列表中的操作的请求SCP都将被拒绝。即使账户中的管理员通过将 IAM 权限策略附加到其中一个成员账户中的用户来授予对其他服务的访问权限，情况依然如此。

11. 现在，您可以附加SCP姓名`Deny List for MainApp Prohibited services`，以防止 MainApp OU 中账户中的任何人使用任何受限服务。

    为此，请导航到Amazon Web Services 账户页面，选择三角形图标以展开 Production O MainAppU 的分支，然后选择 OU（它的名称，而不是单选按钮）以导航到其内容。

12. 在MainApp详细信息页面上，选择策略选项卡。
13. 在 “服务控制策略” 下，选择 “附加”，然后在可用策略列表中，选择 “ MainApp 禁止服务的拒绝列表” 旁边的单选按钮，然后选择 “附加策略”。

步骤 4：测试组织的策略

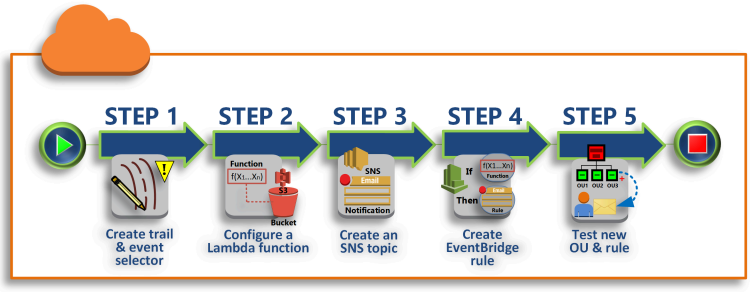
现在，您可以使用任何成员账户中的用户身份登录，并尝试执行各种 Amazon 操作：

- 如果您以管理账户用户身份登录，则可以执行IAM权限策略允许的任何操作。SCPs不影响管理账户中的任何用户或角色，无论该账户位于哪个 root 或 OU 中。
- 如果您以帐户 222222222222 中的用户身份登录，则可以执行允许列表允许的任何操作。 Amazon Organizations 拒绝任何试图在不在允许列表中的任何服务中执行操作的尝试。此外， Amazon Organizations 拒绝任何试图执行其中一个 CloudTrail 配置操作的尝试。
- 如果您以 333333333333 账户中的用户身份登录，则可以执行允许列表允许且拒绝列表未阻止的任何操作。 Amazon Organizations 将拒绝尝试执行允许列表策略中未列出的任何操作，并拒绝尝试执行拒绝列表策略中列出的任何操作。此外， Amazon Organizations 拒绝任何试图执行其中一个 CloudTrail 配置操作的尝试。

教程：使用 Amazon 监控组织的重要变更 EventBridge

本教程介绍如何配置 Amazon EventBridge（前身为 Amazon Ev CloudWatch ents）以监控您的组织是否有更改。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。接下来，您 EventBridge 将 Amazon 配置为在触发规则时运行 Amazon Lambda 函数，并将 Amazon SNS 配置为发送一封包含事件详细信息的电子邮件。

下图演示了本教程的主要步骤。



步骤 1：配置跟踪和事件选择器

在中创建名为跟踪的日志 Amazon CloudTrail。对其进行配置，捕获所有 API 调用。

步骤 2：配置 Lambda 函数

创建一个 Amazon Lambda 函数，将有关事件的详细信息记录到 S3 存储桶。

步骤 3：创建 Amazon SNS 主题，向订阅者发送电子邮件

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

步骤 4：创建亚马逊 EventBridge 规则

创建一条规则，告诉亚马逊 EventBridge 将指定 API 调用的详细信息传递给 Lambda 函数和 SNS 主题订阅者。

第 5 步：测试您的亚马逊 EventBridge 规则

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

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

先决条件

本教程假定：

- 您可以以 IAM 用户 Amazon Web Services Management Console 身份从组织中的管理账户登录。IAM 用户必须有权创建和配置登录信息 CloudTrail、Lambda 中的函数、Amazon SNS 中的主题以及亚马逊中的规则。 EventBridge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。
- 您可以访问现有的亚马逊简单存储服务 (Amazon S3) 存储桶（或者您有权创建存储桶），以接收 CloudTrail 您在步骤 1 中配置的日志。

> **Important**
>
> 目前， Amazon Organizations 仅在美国东部（弗吉尼亚北部）地区托管（尽管它在全球范围内可用）。要执行本教程中的步骤，必须将配置 Amazon Web Services Management Console 为使用该区域。

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）。您还可以在跟踪上配置事件选择器以捕获所有读/写 API 调用，这样 Amaz EventBridge on 就可以启动调用。

创建跟踪

1. 以 Amazon 组织管理账户管理员的身份登录，然后在打开 CloudTrail 控制台https://console.amazonaws.cn/cloudtrail/。
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，则 Amazon Organizations 不会作为选项显示在 Amazon EventBridge 配置设置中，也 CloudTrail 不会捕获相关信息 Amazon Organizations。
3. 在导航窗格中，选择 Trails（跟踪记录）。
4. 选择创建跟踪。
5. 对于 Trail name (跟踪名称)，输入 **`My-Test-Trail`**。
6. 执行以下选项之一以指定其日志 CloudTrail 的传送位置：
   - 如果您需要创建存储桶，请选择 Create new S3 bucket（创建新 S3 存储桶），然后在 Trail log bucket and folder（跟踪日志存储桶和文件夹）中输入新存储桶的名称。

> **Note**
>
> S3 存储桶的名称必须是全球唯一的。

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

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

当警报规则与传入的 API 调用匹配时，Amazon EventBridge 允许您从几种不同的方式中进行选择，以发送警报。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

在此步骤中，您将创建一个 Lambda 函数，用于记录由您稍后配置的 Amazon EventBridge 规则发送给它的 API 活动。

创建用于记录亚马逊事件的 Lambda 函数 EventBridge

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

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

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

7. 编辑 Lambda 函数的代码，如以下示例所示。

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

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

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

8. 选择 Create function (创建函数)。

步骤 3：创建 Amazon SNS 主题，向订阅者发送电子邮件

在此步骤中，您将创建 Amazon SNS 主题，向订阅者发送电子邮件信息。您将此主题作为稍后创建的 Amazon EventBridge 规则的目标。

创建 Amazon SNS 主题，向订阅者发送电子邮件

1. 从 https://console.amazonaws.cn/sns/v3/ 打开 Amazon SNS 控制台。
2. 在导航窗格中，选择 Topics（主题）。
3. 选择 创建新主题。

   a. 对于 Topic name (主题名称)，输入 **`OrganizationsCloudWatchTopic`**。

   b. 对于 Display name (显示名称)，输入 **`OrgsCWEvnt`**。

   c. 选择创建主题。

4. 现在，您可以创建该主题的订阅。选择您刚刚创建的主题的 ARN。
5. 选择创建订阅。

   a. 在 Create subscription (创建订阅) 页面上，为 Protocol (协议) 选择 Email (电子邮件)。

   b. 对于 Endpoint (终端节点)，输入您的电子邮件地址。

c. 选择创建订阅。 Amazon 向您在上一步中指定的电子邮件地址发送一封电子邮件。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：创建亚马逊 EventBridge 规则

既然您的账户中已存在所需的 Lambda 函数，那么您可以创建一个 Amazon EventBridge 规则，当满足规则中的条件时，该规则就会调用该规则。

创建 EventBridge 规则

1. 打开 Amazon EventBridge 控制台，网址为https://console.amazonaws.cn/events/。
2. 您必须将控制台设置为美国东部（弗吉尼亚州北部）区域，否则有关 Organizations 的信息不可用。在控制台右上角的导航栏中，选择美国东部（弗吉尼亚北部）区域。
3. 有关创建规则的说明，请参阅亚马逊 EventBridge 用户指南 EventBridge中的亚马逊规则。

第 5 步：测试您的亚马逊 EventBridge 规则

在此步骤中，您将创建组织单位 (OU) 并遵守 Amazon EventBridge 规则，生成日志条目，并向自己发送一封包含活动详细信息的电子邮件。

Amazon Web Services Management Console

创建 OU

1. 打开该Amazon Web Services 账户页面的 Amazon Organizations 控制台。
2. 选择复选框

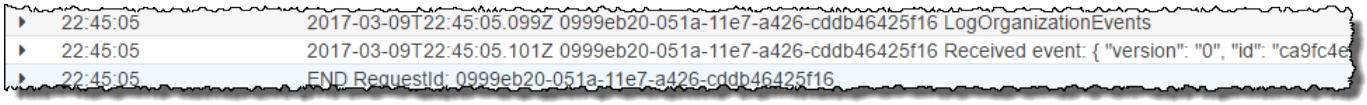
   ☑

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

查看 EventBridge 日志条目

1. 打开 CloudWatch 控制台，网址为https://console.amazonaws.cn/cloudwatch/。

2. 在导航窗格中，选择 Logs (日志)。
3. 在日志组下，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。选择该存储桶。
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中是否有来自组织的一封邮件CWEvnt（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，您应删除在本教程中创建的所有不想保留的 Amazon 资源。

清理您的 Amazon 环境

1. 使用CloudTrail 控制台删除您在步骤 1 中创建**My-Test-Trail**的名为的跟踪。
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 控制台删除您在步骤 4 中创建**OrgsMonitorRule**的名为的 EventBridge 规则。
6. 使用 Organizations 控制台删除您通过步骤 5 创建的、名为 **TestCWEOU** 的 OU。

就是这样。在本教程中，您已配置 EventBridge 为监控组织是否有更改。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 与 Amazon SDK 一起使用

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

SDK 文档
Amazon CLI

SDK 文档
适用于 Java 的 Amazon SDK
适用于 JavaScript 的 Amazon SDK
适用于 .NET 的 Amazon SDK
适用于 PHP 的 Amazon SDK
Amazon Tools for PowerShell
适用于 Python (Boto3) 的 Amazon SDK
适用于 Ruby 的 Amazon SDK
适用于 SAP ABAP 的 Amazon SDK

使用管理组织 Amazon Organizations

组织是您可以集中管理的组织集合 Amazon Web Services 账户 ，并将其组织成一个分层的树状结构，根位于顶部，组织单元嵌套在根目录下。每个账户可以直接位于根目录中，也可以放置在层次结构 OUs 中的一个中。

每个组织都包括：

- 一个管理账户
- 零个或多个成员账户
- 零个或多个组织单位 (OUs)
- 零个或多个策略。

一个组织的功能由您启用的功能集决定。

主题

使用 Amazon Organizations 创建组织

您可以将您的 Amazon Web Services 账户作为管理账户来创建组织。创建组织时，您可以选择组织是支持所有功能（推荐），还是只支持整合账单功能。默认情况下，您创建的组织会支持所有功能。

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

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

   如果您意外选择了错误的选项，您可以立即转到 Settings (设置) 页面，然后选择 Delete organization (删除组织) 并重新开始。
3. 组织已创建，并且会显示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）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 Amazon Organizations 的电子邮件地址验证。您可以在不验证管理账户电子邮件地址的情况下创建账户以添加到组织中。但是，要邀请现有账户，您必须先完成电子邮件验证。

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

Amazon CLI 与 Amazon SDK

以下代码示例演示如何使用 `CreateOrganization`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 在 GitHub 上查看更多内容。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Creates an organization in AWS Organizations.
    /// </summary>
    public class CreateOrganization
    {
        /// <summary>
        /// Creates an Organizations client object and then uses it to create
        /// a new organization with the default user as the administrator, and
        /// then displays information about the new organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
            {
                FeatureSet = "ALL",
            });

            Organization newOrg = response.Organization;

            Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
{newOrg.MasterAccountId}");
```

```
        }
    }
```

- 有关 API 的详细信息，请参阅《适用于 .NET 的 Amazon SDK API 参考》中的 CreateOrganization。

CLI

Amazon CLI

示例 1：创建新组织

Bill 想使用账户 111111111111 中的凭证创建一个组织。以下示例显示该账户成为新组织中的主账户。由于他没有指定功能集，因此，新组织默认为在根上启用所有功能并启用服务控制策略。

```
aws organizations create-organization
```

输出包括一个组织对象，其中包含有关新组织的详细信息：

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

示例 2：创建仅启用整合账单功能的新组织

以下示例创建仅支持整合账单功能的组织：

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

输出包括一个组织对象，其中包含有关新组织的详细信息：

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

有关更多信息，请参阅《Amazon Organizations 用户指南》中的“创建组织”。

- 有关 API 详细信息，请参阅《Amazon CLI 命令参考》中的 CreateOrganization。

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。
- 验证您的电子邮件地址后，邀请现有的 Amazon Web Services 账户作为会员账户加入您的组织。

Amazon Organizations 的电子邮件地址验证

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。

验证您的电子邮件地址

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。如果已超过 24 小时，请参阅重新发送验证电子邮件。

使用 Amazon Organizations 重新发送验证电子邮件

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

- 要查看与您的管理账户关联的电子邮件地址是什么，请参阅从管理账户查看组织的详细信息。
- 若要更改与管理账户关联的电子邮件地址，请参阅《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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 导航到 Settings (设置) 页面，然后选择 Send verification request (发送验证请求)。只有在未验证管理账户时才存在该选项。
3. 在 24 小时内验证您的电子邮件地址。

验证您的电子邮件地址后，您可以邀请其他Amazon Web Services 账户加入您的组织。有关更多信息，请参阅 使用管理账户邀请 Amazon Organizations。

使用 Amazon Organizations 更改组织的电子邮件地址

要更改与管理账户关联的电子邮件地址，请参阅《Amazon 账户管理 参考指南》中的 Update the Amazon Web Services 账户 name, email address, or password for the root user。

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。您必须首先重新发送验证请求。通过回复电子邮件完成此过程后，您邀请的账户可以接受邀请。

通过以下方式为组织启用所有功能 Amazon Organizations

Amazon Organizations 有两个可用的功能集：

- 所有功能-此功能集是首选的默认使用方式 Amazon Organizations，它包括合并账单的所有功能。在创建组织时，默认情况下将启用所有功能。启用所有功能后，您可以使用 Organizations 中提供的高级账户管理功能，例如与支持的 Amazon 服务和组织政策的集成。
- 整合账单功能 – 此功能集仅限于在整个组织中生成单一的账单。整合账单不提供其他管理功能。

如果创建启用整合账单功能集的组织，可以稍后启用所有功能。但是，启用所有功能后，您无法从所有功能迁移到整合账单功能。

标准迁移和辅助迁移

迁移到所有功能有两种方法，一是标准迁移，二是辅助迁移。

标准迁移是所有 Amazon Organizations 客户都可以使用的自助服务流程，用于启用所有功能模式。

辅助迁移是 Enterprise Support 计划客户可以代表您请求将其组织 Amazon 迁移到所有功能模式的流程。

> **Note**
>
> 单向过程和回滚过程
>
> - 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。
> - 辅助迁移过程开始执行后，将无法回滚。如果您想改用标准流程，则需要等待 90 天，直到此过程到期。

主题

注意事项

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：

受邀账户必须批准迁移

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。

系统会通知受邀账户当前启用的是哪种功能集

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。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。

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。

在组织中创建账户的过程不受迁移的影响

您可以继续在组织中创建账户。该过程不受此更改的影响。

必须使用服务相关角色 **`AWSServiceRoleForOrganizations`**

Amazon Organizations 验证每个成员账户是否都有一个名为的服务相关角色。`AWSServiceRoleForOrganizations`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。如果您在使用创建的账户中删除了该角色 Amazon Organizations，则该账户将收到专门重新创建该角色的邀请。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。

使用标准迁移过程启用所有 Organizations 功能

本主题介绍如何使用标准迁移过程启用所有功能。

第 1 步：请求受邀账户批准迁移（管理账户）

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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在设置页面上，选择开始流程以启用所有功能。
3. 在启用所有功能页面上，确认您了解在选择开始流程以启用所有功能进行切换之后便无法再恢复到仅整合账单功能。

   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

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

组织中的所有受邀账户批准请求之后，您可以完成流程并启用所有功能。如果您的组织中没有任何受邀成员账户，也可以立即完成流程。要最终完成该过程，请继续根据第 3 步：完成迁移过程以启用所有功能（管理账户）中的内容操作。

第 2 步：批准该请求以启用所有功能或重新创建服务相关角色（受邀账户）

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

> **最小权限**
>
> 要批准请求以为成员账户启用所有功能，该成员账户必须拥有以下权限：
>
> - `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 用户身份登录，担任 IAM 角色；或以组织成员账户中的根用户身份登录（不推荐）。

2. 阅读以了解接受在组织中启用所有功能的请求对您的账户意味着什么，然后选择 Accept。在组织中的所有账户接受请求并且管理账户管理员完成流程之前，此页面一直将该流程显示为未完成。

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

第 3 步：完成迁移过程以启用所有功能（管理账户）

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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Settings (设置) 页面上，如果所有受邀账户接受启用所有功能的请求，则页面顶部将显示一个绿色框以通知您。在绿色框中，选择 Go to finalize (转到最终确定)。

3. 在 Enable all features (启用所有功能) 页面上，选择 Finalize (最终确定)，然后在确认对话框中再次选择 Finalize (最终确定)。
4. 组织现已启用所有功能。

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：
  - ListHandshakesForOrganization
  - AcceptHandshake

使用辅助迁移过程启用所有 Organizations 功能

如果您是企业客户，由于可能要管理大量账户，可能难以完成标准迁移过程。例如，在大型组织中迁移所有受邀账户时，您可能难以获得批准。

使用辅助迁移时，拥有 Enterprise Support 计划的客户可以请求 Amazon 代您将其组织迁移到所有功能，从而有助于您完成此过程。此过程要求您签署一份协议合同，确认您拥有所有账户，然后需要等待 14 天。这一等待期为希望在所有功能迁移生效之前退出组织的账户提供了时间，以退出组织。

Amazon Web Services Management Console

使用辅助迁移功能迁移到所有功能

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在设置页面上，选择启用所有功能，然后选择辅助迁移。
3. 阅读协议的条款和条件，选择接受，然后选择开始流程以启用所有功能，从而开始迁移。

> **Note**
>
> 开始辅助迁移过程会优先于标准迁移过程
> 如果您当前正在使用标准迁移过程启用所有功能，则该过程将被取消，然后辅助迁移过程将会启动。
> 辅助迁移过程是单向的，无法回滚
> 辅助迁移过程开始执行后，将无法回滚。如果您想改用标准流程，则需要等待 90 天，直到此过程到期。

如果您使用辅助迁移，则无需以根用户身份访问受邀账户以接受向所有功能迁移。

您可以联系您的技术客户经理（TAM），了解辅助迁移的确切详情、进度和时间表。

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

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

使用删除组织 Amazon Organizations

当您不再需要组织时，可将其删除。删除组织不会导致管理账户被注销，而只是将管理账户从组织中移除，然后再删除组织本身。

以前的管理账户变为独立账户 Amazon Web Services 账户 ，不再由管理 Amazon Organizations。这时您有三种选项：

- 您可以将其作为独立账户继续使用
- 您可以用其来创建其他组织
- 您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。

主题

注意事项

无法恢复已删除的组织

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。

只有在移除了所有成员账户之后，才能删除组织

必须先删除组织中的所有成员账户，然后才能删除组织。如果您使用创建了某些成员帐户 Amazon Organizations，则可能无法删除这些帐户。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，请参阅使用成员账户退出组织 Amazon Organizations。

处于“已暂停”状态的成员账户无法从组织中移除

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。

如果通过删除组织来从组织中移除管理账户，则会在以下方面影响该账户：

- 该账户只负责支付自己的费用，不再负责支付其他任何账户产生的费用。

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

组织的管理账户永远不会受到服务控制策略 (SCPs) 的影响，因此在权限不再可用之后 SCPs ，权限不会发生变化。

备份所有报告

请务必从管理账户导出或备份报告，尤其是账单报告。删除组织时不会存储组织级别的报告和历史记录。所有成本数据（例如 Cost Explorer 数据集）都将被删除。建议您完整导出所有账单历史记录。

有关更多信息，请参阅成本和使用情况报告、Cost Explorer 报告、节省计划报告以及预留实例（RI）利用率和覆盖范围。

删除组织

使用以下步骤删除将以前的管理账户恢复为不再由 Amazon Organizations管理 Amazon Web Services 账户 的独立账户的组织。

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

Amazon Web Services Management Console

删除组织

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

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

Amazon CLI & Amazon SDKs

以下代码示例演示如何使用 `DeleteOrganization`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing organization using the AWS
/// Organizations Service.
/// </summary>
public class DeleteOrganization
{
    /// <summary>
    /// Initializes the Organizations client and then calls
    /// DeleteOrganizationAsync to delete the organization.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();
```

```
            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考DeleteOrganization中的。

CLI

Amazon CLI

删除组织

以下示例演示如何删除组织。要执行此操作，您必须是组织中主账户的管理员。该示例假设您之前已从组织中删除了所有成员账户和政策： OUs

```
aws organizations delete-organization
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DeleteOrganization中的。

使用管理组织中的账户 Amazon Organizations

Amazon Web Services 账户是您的 Amazon 资源的容器。您可以在中创建和管理您的 Amazon 资源 Amazon Web Services 账户。

本主题介绍如何管理的帐户 Amazon Organizations。

主题

使用管理账户 Amazon Organizations

管理账户是 Amazon Web Services 账户 您用来创建组织的。

管理账户是组织的最终所有者，对组织的安全、基础设施和财务策略拥有最终控制权。此账户具有付款人账户的角色，并负责支付其组织中账户产生的所有费用。

本主题介绍如何使用管理账户 Amazon Organizations。

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。这些建议假定您还遵守仅将根用户用于真正需要它的任务的最佳实践。

主题

限制谁有权访问管理账户

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

检查并跟踪谁有访问权限

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

仅将管理账户用于需要管理账户的任务

我们建议您将管理账户及其用户和角色仅用于必须由该账户执行的任务。将所有 Amazon 资源存储在组织 Amazon Web Services 账户 中的其他资源中，并防止它们进入管理账户。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 (SCPs) 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。

有关必须从管理账户调用的任务列表，请参阅只能从组织的管理账户调用的操作。

避免将工作负载部署到组织的管理账户中

特权操作可以在组织的管理账户中执行，但 SCPs 不适用于管理账户。因此，管理账户中包含的云资源和数据应仅限必须在管理账户中管理的云资源和数据。

将责任委托给非管理账户以实现去中心化

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

有关更多信息，请参阅安全参考架构、使用多个账户组织您的 Amazon 环境，以及Amazon Web Services 服务 你可以和它一起使用 Amazon Organizations有关将成员账户注册为各种 Amazon 服务的委托管理员的建议。

有关设置委托管理员的更多信息，请参阅 为 Amazon 账户管理启用委托管理员账户 和 的委派管理员 Amazon Organizations。

注销组织的管理账户

要注销组织的管理账户，必须首先注销或移除该组织中的所有成员账户。注销管理账户的行为还会在注销后期限届满后，删除 Amazon Organizations 实例以及您在该组织内创建的任何策略。

注销管理账户

请使用以下过程注销管理账户。

> **Important**
>
> 在注销管理账户之前，我们强烈建议您查看注意事项并了解注销账户的影响。有关更多信息，请参阅《Amazon 账户管理指南》中的 What you need to know before closing your account 和 What to expect after you close your account。

Amazon Management Console

从“账户”页面注销管理账户

> **Note**
>
> 您无法直接从 Amazon Organizations 控制台注销管理账户。

1. 在要注销的管理账户中，以具有所需最低权限 `portal:ModifyAccount` 的用户或角色身份登录。
2. 确认组织中没有剩余的活跃成员账户。为此，请转到Amazon Organizations 控制台。如果您的会员账户仍处于活动状态，则需要从组织中移除成员账户先按照中提供的指导关闭组织中的成员账户 Amazon Organizations进行操作，然后才能进入下一步操作。
3. 在右上角的导航栏中，选择账户名称或账号，然后选择账户。

4. 在账户页面上，选择关闭账户按钮。阅读并确保理解账户关闭指南。
5. 选择关闭账户按钮，启动账户关闭流程。
6. 几分钟后，您应该会收到一封确认账户已注销的电子邮件。

Amazon CLI & Amazon SDKs

Amazon CLI 或其中一个 API 操作不支持此任务 Amazon SDKs。只有使用才能执行此任务 Amazon Web Services Management Console。

使用管理成员账户 Amazon Organizations

除管理账户外 Amazon Web Services 账户，成员账户是组织的一部分。

本主题介绍如何使用管理成员账户 Amazon Organizations。

主题

- 成员账户的最佳实践
- 使用在组织中创建成员账户 Amazon Organizations
- 使用访问组织中的成员账户 Amazon Organizations
- 关闭组织中的成员账户 Amazon Organizations
- 使用 Amazon Organizations 阻止成员账户注销
- 使用 Amazon Organizations 从组织中移除成员账户
- 使用成员账户退出组织 Amazon Organizations
- 更新成员账户的 Amazon Web Services 电子邮件地址 Amazon Organizations

成员账户的最佳实践

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

主题

- 定义账户名称和属性
- 高效扩展环境和使用账户

- 启用 root 访问权限管理以简化成员账户的 root 用户凭证的管理

定义账户名称和属性

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

高效扩展环境和使用账户

在扩大规模时，在创建新账户之前，请确保尚不存在满足类似需求的账户，以避免不必要的重复。Amazon Web Services 账户 应基于共同的访问要求。如果您计划回收利用某些账户（例如沙盒账户或等效账户），我们建议您清理账户中不需要的资源或工作负载，但保存这些账户以备将来使用。

在注销账户之前，请注意账户注销限额限制。有关更多信息，请参阅 的配额和服务限制 Amazon Organizations。考虑实施清理流程以回收利用账户，而不是尽可能注销账户和创建新账户。这样，您就可以避免因运行资源和达到 CloseAccount API 限制而产生成本。

启用 root 访问权限管理以简化成员账户的 root 用户凭证的管理

我们建议您启用 root 访问权限管理，以帮助您监控和删除成员账户的 root 用户证书。根访问权限管理可防止根用户凭证的恢复，从而提高组织中的账户安全性。

- 删除成员账户的 root 用户凭证，以防止登录 root 用户。这还会阻止恢复成员帐户的根用户。
- 假设特权会话对成员账户执行以下任务：
  - 删除一项配置错误的存储桶策略，此策略拒绝所有主体访问 Amazon S3 存储桶策略。
  - 删除将会拒绝所有主体访问 Amazon SQS 队列的 Amazon Simple Queue Service 基于资源的策略。
  - 允许成员账户恢复其根用户证书。有权访问该成员账户的根用户电子邮件收件箱的人可以重置 root 用户密码并以成员账户 root 用户身份登录。

启用根访问管理后，新创建的成员账户将没有根用户证书，这样就无需在配置后提供额外的安全保护，例如MFA。 secure-by-default

有关更多信息，请参阅《用户指南》中的 “集中管理成员账户的根Amazon Identity and Access Management 用户证书”。

使用 SCP 限制成员账户中的根用户可以执行的操作

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

除必须在成员账户中执行的特定仅限根操作外，您可以拒绝所有根操作。例如，以下 SCP 可防止任何成员账户中的根用户进行任何 Amazon 服务 API 调用，但“更新配置错误的 S3 存储桶策略并拒绝所有委托人访问权限”（需要根凭证的操作之一）除外。有关更多信息，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

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

    "Statement": [

        {

            "Effect": "Deny",

            "NotAction":[

            "s3:GetBucketPolicy",

            "s3:PutBucketPolicy",

            "s3:DeleteBucketPolicy"

                 ],

            "Resource": "*",

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

            }

        }

    ]
 }
```

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

使用在组织中创建成员账户 Amazon Organizations

本主题介绍如何在您的组织 Amazon Web Services 账户 中创建 Amazon Organizations。有关创建单曲的信息 Amazon Web Services 账户，请参阅入门资源中心。

创建成员账户前的注意事项

Organizations 会自动**`OrganizationAccountAccessRole`**为成员账户创建IAM角色

当您在组织中创建成员账户时，Organizations 会自动`OrganizationAccountAccessRole`在成员账户中创建角色，使管理账户中的用户和角色能够对成员账户行使完全的管理控制。IAM每次策略更新时，附加到同一托管式策略的任何其他账户都会自动更新。此角色受适用于成员账户的任何服务控制策略 (SCPs) 的约束。

Organizations 会自动**`AWSServiceRoleForOrganizations`**为成员账户创建服务相关角色

当您在组织中创建成员账户时，Organizations 会自动在成员账户中创建服务相关角色`AWSServiceRoleForOrganizations`，以确保能与选定的 Amazon 服务集成。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。

成员账户可能需要额外的信息才能作为独立账户运行

Amazon 不会自动收集成员账户作为独立账户运行所需的所有信息。如果您需要从组织中删除成员账户并使其成为独立账户，则您必须先提供账户的信息，然后才能删除账户。有关更多信息，请参阅 使用成员账户退出组织 Amazon Organizations。

只能在组织的根中创建成员账户

组织中的成员帐户只能在组织的根目录中创建，不能在任何其他组织单位中创建 (OUs)。在创建组织的成员账户根目录后，您可以将其移动OUs。有关更多信息，请参阅 使用 Amazon Organizations 将账户移动到 OU 或者在根和 OU 之间移动。

附加到根的策略会立即生效

如果您在根上附加了任何策略，这些策略会立即应用于所创建账户中的所有用户和角色。

如果您为组织中的其他服务启用了 Amazon 服务信任，则该可信服务可以在组织中的任何成员帐户（包括您创建的帐户）中创建服务相关角色或执行操作。

Amazon Control Tower 应在以下位置创建由管理的组织的成员帐户 Amazon Control Tower

如果您的组织由管理 Amazon Control Tower，则使用 Amazon Control Tower 控制台中的 Amazon Control Tower 账户工厂或使用创建您的成员账户 Amazon Control Tower APIs。如果您在组织由管理的 Organizations 中创建成员帐户 Amazon Control Tower，则该帐户将无法注册到该帐户 Amazon Control Tower。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。

成员账户必须选择启用才能接收营销电子邮件

您作为组织的一员创建的成员帐户不会自动订阅 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。

创建成员账户

登录到组织的管理账户后，您可以创建属于组织的成员账户。

使用以下步骤创建账户时， Amazon Organizations 会自动将以下主要联系人信息从管理账户复制到新成员账户：

- 电话号码
- 公司名称
- 网站 URL
- 地址

Organizations 还会从管理账户中复制通信语言和 Marketplace 信息（在某些情况下是账户的供应商 Amazon Web Services 区域）。

> **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

创建自动成为您组织一部分的 Amazon Web Services 账户

1. 登录 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
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)（默认情况下选择该选项）。
4. 在 Create an Amazon Web Services 账户(创建亚马逊云科技账户) 页面上，为 Amazon Web Services 账户 name (亚马逊云科技账户名称) 输入要分配给账户的名称。此名称将帮助您区分该账户与组织中的所有其他账户，并且独立于 IAM 别名或拥有者的电子邮件名称。

   > **Important**
   >
   > 请务必验证 Amazon Web Services 账户 名称是否正确。一旦成功创建账户，就无法修改账户名称。

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。此电子邮件地址已无法与其他电子邮件地址关联， Amazon Web Services 账户 因为它已成为该账户根用户的用户名凭证。
6. （可选）指定分配给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。如果未指定名称，则 Amazon Organizations 为角色指定默认名称`OrganizationAccountAccessRole`。建议您对您的所有账户使用默认名称以实现一致性。

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

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

   - 如果您收到错误，指明您超出了组织的账户配额，请参阅尝试向组织中添加账户时，我收到“quota exceeded (超出限额)”消息。

- 如果您收到错误，指明由于您的组织仍在进行初始化，所以您无法添加账户，请等待一小时，然后重试。
- 您也可以查看日 Amazon CloudTrail 志，了解账户创建是否成功的信息。有关更多信息，请参阅 登录和监控 Amazon Organizations。
- 如果错误仍然存在，请联系 Amazon Web Services 支持。

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，该账户已存在，并且具有向管理账户中的用户授予管理员访问权限的IAM角色，您可以按照中的步骤访问该账户使用访问组织中的成员账户 Amazon Organizations。

Amazon CLI & Amazon SDKs

以下代码示例演示如何使用 `CreateAccount`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
    /// the new account with the name specified in accountName.
    /// </summary>
    public static async Task Main()
```

```
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var accountName = "ExampleAccount";
            var email = "someone@example.com";

            var request = new CreateAccountRequest
            {
                AccountName = accountName,
                Email = email,
            };

            var response = await client.CreateAccountAsync(request);
            var status = response.CreateAccountStatus;

            Console.WriteLine($"The staus of {status.AccountName} is
 {status.State}.");
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 CreateAccount” 中的。

CLI

Amazon CLI

创建自动属于组织的成员账户

以下示例演示如何创建组织的成员账户。为成员账户配置的名称为 Production Account，电子邮件地址为 susan@example.com。 OrganizationAccountAccessRole 由于未指定 roleName 参数，Organizations 会使用默认名称自动创建IAM角色。此外，ALLOW由于未指定 IamUserAccessToBilling 参数，因此允许具有足够权限的IAM用户或角色访问账户账单数据的设置被设置为默认值。Organiations 会自动向 Susan 发送一封 “欢迎来到 Amazon” 电子邮件：

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

输出包括一个请求对象，以显示状态目前为 IN_PROGRESS：

```
{
```

```
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

稍后，您可以通过向 describe-create-account-status命令提供 Id 响应值作为 create-account-request-id参数值来查询请求的当前状态。

有关更多信息，请参阅《Organi Amazon zations 用户指南》中的在Amazon 组织中创建帐户。

- 有关API详细信息，请参阅 “CreateAccount Amazon CLI命令参考”。

使用访问组织中的成员账户 Amazon Organizations

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。您可以在创建时指定不同的名称，但我们建议您在所有账户中使用一致的名称。 Amazon Organizations 不会创建任何其他用户或角色。

要访问组织中的账户，您必须使用以下方法之一：

您可以集中成员账户的 root 访问权限，以删除组织中现有成员账户的 root 用户证书。删除根用户证书会删除根用户密码、访问密钥、签名证书，并停用多因素身份验证 (MFA)。这些成员账户没有根用户凭证，无法以根用户身份登录，并且无法恢复根用户密码。默认情况下，您在 Organizations 中创建的新账户不具有根用户证书。

- 除非创建权限更有限的其他用户和角色，否则请勿使用 root 用户访问您的账户。然后以这些用户或角色之一的身份登录。
- 在根用户@@ 上启用多重身份验证 (MFA)。重置密码，然后向根用户分配 MFA 设备。

使用 IAM Identity Center 的可信访问

使用Amazon IAM Identity Center并启用 IAM 身份中心的可信访问权限 Amazon Organizations。这允许用户使用其公司凭据登录 Amazon 访问门户，并访问其分配的管理账户或成员账户中的资源。

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

使用 IAM 角色 **`OrganizationAccountAccessRole`**

如果您使用中提供的工具创建账户 Amazon Organizations，则可以使用以这种方式创建的所有新账户中都存在的名`OrganizationAccountAccessRole`为的预配置角色来访问该账户。有关更多信息，请参阅 使用 Amazon Organizations 访问具有 OrganizationAccountAccessRole 的成员账户。

如果您邀请现有账户加入您的组织，并且该账户接受邀请，则您可以选择创建 IAM 角色来允许管理账户访问受邀成员账户。此角色应该与自动添加到使用 Amazon Organizations创建的账户中的角色相同。

如需创建此角色，请参阅使用 Amazon Organizations 为受邀账户创建 OrganizationAccountAccessRole。

创建角色之后，您可以使用使用 Amazon Organizations 访问具有 OrganizationAccountAccessRole 的成员账户中的步骤访问它。

> **最小权限**
>
> 要 Amazon Web Services 账户 从组织中的任何其他账户访问的，您必须具有以下权限：
>
> - `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。

主题

- 使用 Amazon Organizations 为受邀账户创建 OrganizationAccountAccessRole
- 使用 Amazon Organizations 访问具有 OrganizationAccountAccessRole 的成员账户

使用 Amazon Organizations 为受邀账户创建 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 使用 Amazon Organizations 访问具有 OrganizationAccountAccessRole 的成员账户。

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

Amazon Web Services Management Console

在成员账户中创建 Amazon Organizations 管理员角色

1. 通过 https://console.aws.amazon.com/iam/ 登录到 IAM 控制台。您必须以 IAM 用户身份登录，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 管理员用户。
2. 在 IAM 控制台中，导航至角色，然后选择创建角色。
3. 依次选择 Amazon Web Services 账户，然后选择其他 Amazon Web Services 账户。
4. 输入您希望向其授予管理员访问权限的管理账户的 12 位账户 ID 编号。在选项下，请注意以下方面：
   - 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？。
   - 如果您启用了 MFA 并进行了配置，则可以选择要求使用 MFA 设备进行身份验证。有关 MFA 的更多信息，请参阅《IAM 用户指南》中的在 Amazon 中使用多重身份验证（MFA）。
5. 选择下一步。
6. 在附加权限页面上，选择名为 `AdministratorAccess` 的 Amazon 托管式策略，然后选择下一步。
7. 在命名、检查和创建页面上，指定一个角色名称和可选的描述。我们建议您使用 `OrganizationAccountAccessRole`，以便与分配给新账户中角色的默认名称保持一致。要提交您的更改，请选择 Create role (创建角色)。
8. 您的新角色将显示在可用角色列表上。选择新角色的名称以查看详细信息，特别注意提供的链接 URL。向成员账户中需要访问该角色的用户提供此 URL。此外，记下 Role ARN (角色 ARN)，因为您在步骤 15 中需要它。
9. 通过 https://console.aws.amazon.com/iam/ 登录到 IAM 控制台。此时，以管理账户中有权创建策略和将策略分配给用户或组的用户身份登录。
10. 导航到策略，然后选择创建策略。
11. 对于 Service，选择 STS。
12. 对于 Actions (操作)，在 Filter (筛选器) 框中开始键入 **`AssumeRole`**，然后在该角色显示后选中其旁边的复选框。
13. 选择资源，确保已选择特定，然后选择添加 ARN。
14. 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。选择添加 ARN。

15. 如果您正授予在多个成员账户中代入该角色的权限，请为每个账户重复步骤 14 和 15。
16. 选择下一步。
17. 在检查并创建页面上，输入新策略的名称，然后选择创建策略以保存您的更改。
18. 导航窗格中选择用户组，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）。
19. 选择权限选项卡。
20. 选择添加策略，选择附加策略，然后选择您在步骤 11–18 中创建的策略。

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

使用 Amazon Organizations 访问具有 OrganizationAccountAccessRole 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。

您可以按照使用 Amazon Organizations 为受邀账户创建 OrganizationAccountAccessRole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???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，选择选择服务，在搜索框中输入 **STS** 以筛选列表，然后选择 STS 选项。

4. 在操作部分中的搜索框中输入 **assume** 以筛选列表，然后选择 AssumeRole 选项。
5. 在资源部分中，选择特定，然后选择添加 ARN
6. 在指定 ARN 部分中，对于资源位置选择其他账户。
7. 输入您刚刚创建的成员账户的 ID
8. 对于资源角色名称及路径，请输入您在上一节中创建的角色的名称（我们建议将其命名为 `OrganizationAccountAccessRole`）。
9. 当对话框显示正确的 ARN 时，选择添加 ARN。
10. （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。
11. 选择下一步。
12. 在检查并创建页面上，输入新策略的名称。例如：**`GrantAccessToOrganizationAccountAccessRole`**。您还可以添加可选的说明。
13. 选择 Create policy (创建策略) 以保存新的托管策略。
14. 现在，您已有策略可用，您可以将其附加到组。

    在导航窗格中选择用户组，然后选择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。
15. 请选择权限选项卡，选择添加权限，然后选择附加策略。
16. （可选）在 Search (搜索) 框中，您可以开始键入策略的名称以筛选列表，直到您可以看到刚刚在Step 2到Step 13中创建的策略的名称。还可以通过选择所有类型，然后选择客户管理，从而筛选出所有 Amazon 托管式策略。
17. 选中策略旁边的复选框，然后选择附加策略。

现在，作为组成员的 IAM 用户有权使用以下过程在 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)。

关闭组织中的成员账户 Amazon Organizations

如果您不再需要组织中的某个成员账户，则可以遵循本主题中的说明从 Amazon Organizations 控制台将其注销。只有当您的组织处于 “所有功能” 模式时，您才能使用 Amazon Organizations 控制台关闭成员账户。

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

要注销管理账户，请参阅注销组织的管理账户。

注销成员账户

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

> **Important**
>
> 在注销会员账户之前，我们强烈建议您查看注意事项并了解注销账户的影响。有关更多信息，请参阅《Amazon 账户管理指南》中的 What you need to know before closing your account 和 What to expect after you close your account。

Amazon Management Console

通过 Amazon Organizations 控制台关闭成员账户

1.
2. 在 Amazon Web Services 账户 页面上，找到并选择您想要关闭的成员账户的名称。您可以导航 OU 层次结构，或查看没有 OU 结构的账户的平面列表。

3. 选择页面顶部的账户名称旁边的 Close（关闭）。只有当 Amazon 组织处于 “所有功能” 模式时，此选项才可用。

> **Note**
>
> 如果您的组织使用整合账单模式，您将无法在控制台中看到 “关闭” 按钮。要在整合账单模式下关闭账户，请以 root 用户身份登录要关闭的账户。在 “账户” 页面上，选择 “关闭账户” 按钮，输入您的账户 ID，然后选择 “关闭账户” 按钮。

4. 阅读并确保理解账户关闭指南。
5. 输入成员账户 ID，然后选择注销账户。

> **Note**
>
> 您注销的任何成员账户将在 Amazon Organizations 控制台中的账户名称旁边显示一个 SUSPENDED 标签，自原始注销日期起最长持续 90 天。90 天后， Amazon Organizations 中将不再显示该成员账户。

从“账户”页面关闭成员账户

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

Amazon CLI & Amazon SDKs

要关闭 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 SDKs: CloseAccount

使用 Amazon Organizations 阻止成员账户注销

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

您可以通过以下两种方式之一创建拒绝关闭账户的 IAM policy：

- 通过在 `Resource` 元素中包含 `arn`，在策略中明确列出您要保护的每个账户。要查看示例，请参阅防止本策略中列出的成员账户关闭。
- 标记个人账户以防止其被关闭。在您的策略中使用 `aws:ResourceTag` 标记全局条件键，以防任何带有该标签的账户被关闭。要了解如何标记账户，请参阅 标记 Organizations 资源。要查看示例，请参阅 防止带标签的成员账户关闭 。

防止成员账户关闭的 IAM policy 示例

以下代码示例展示了两种可用来限制成员账户注销账户的不同功能方法。

防止带标签的成员账户关闭

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

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

防止本策略中列出的成员账户关闭

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
    ]
}
```

使用 Amazon Organizations 从组织中移除成员账户

移除成员账户不会导致该账户被注销，而只是将成员账户从组织中移除。以前的成员账户将成为不再由 Amazon Organizations 管理的独立 Amazon Web Services 账户。

移除账户后，该账户不再受任何策略约束，并自行支付账单。从组织中移除账户后，该账户应计的任何费用将不再计入该组织的管理账户。

注意事项

管理账户创建的 IAM 访问角色不会被自动删除

当您从组织中移除成员账户时，为允许该组织的管理账户访问而创建的任何 IAM 角色都不会自动删除。如果要终止以前组织的管理账户的此访问权限，则必须手动删除 IAM 角色。有关如何删除角色的信息，请参阅《IAM 用户指南》中的删除角色或实例配置文件。

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

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。要移除还没有此信息的账户，请按照 使用成员账户退出组织 Amazon Organizations 中的步骤操作。

您必须等到账户创建后至少满七天

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。

退出组织的账户的所有者将负责所有产生的新成本

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。

该账户不能是为组织启用的任何 Amazon 服务的委派管理员账户

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。要详细了解如何禁用或更改 Amazon 服务的委托管理员账户，请参阅该服务的文档。

该账户不再能够访问成本和使用情况数据

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。

该账户上附加的标签将被删除

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。

该账户中的主体不再受任何组织策略的影响

该账户中的委托人不再受组织内应用的任何策略影响。这意味着，SCP 施加的限制将不复存在，该账户中的用户和角色将比之前拥有更多权限。其他组织策略类型不能再强制执行或处理。

该账户不再属于组织协议的管辖范围

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。

与其他服务的集成可能被禁用

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。

从组织中移除成员账户

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

最小权限

要从您的组织中移除一个或多个成员账户，您必须以管理账户中的用户或角色身份登录并且必须拥有以下权限：

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

如果您选择在第 5 步中以成员账户中的用户或角色身份登录，则该用户或角色必须拥有以下权限：

- `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要。
- `organizations:LeaveOrganization` – 请注意，组织管理员可以将删除此权限的策略应用到您的账户，从而阻止您从组织中删除自己的账户。
- 如果您以 IAM 用户身份登录并且账户缺少付款信息，则用户必须具有 `aws-portal:ModifyBilling` 和 `aws-portal:ModifyPaymentMethods` 权限（如果账户尚未迁移到精细权限）或 `payments:CreatePaymentInstrument` 和 `payments:UpdatePaymentPreferences` 权限（如果账户已迁移到精细权限）。此外，成员账户必须已启用对账单的 IAM 用户访问权限。如果尚未启用此权限，请参阅《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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在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。如果您没有看到复制链接，请使用此链接进入注册 Amazon 页面，完成缺少的注册步骤。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。

   d. 从组织中删除授予访问您账户的权限的 IAM 角色。

      Important

      如果您的账户是在组织中创建的，Organizations 会在该账户中自动创建一个 IAM 角色，以允许组织的管理账户进行访问。如果该账户被邀请加入，则 Organizations 不会自动创建此类角色，但您或其他管理员可能已经创建了一个角

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

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

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

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

成员账户也可以使用 leave-organization 来移除自己。有关更多信息，请参阅 使用成员账户退出组织 Amazon Organizations。

使用成员账户退出组织 Amazon Organizations

登录成员账户后，您可以退出组织。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。

注意事项

组织的账户状态会影响可见的成本和使用情况数据

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。

该账户不再属于代表其接受的组织协议的管辖范围

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 “组织协议” 页面上查看这些Amazon Artifact 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。

作为成员账户退出组织

要退出组织，请完成以下过程。

> **最小权限**
>
> 要退出组织，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用户身份登录但账户缺少付款信息，则该用户必须拥有`aws-portal:ModifyBilling`和`aws-portal:ModifyPaymentMethods`权限（如果账户尚未迁移到细粒度权限）
>
> 或`payments:CreatePaymentInstrument`和`payments:UpdatePaymentPreferences`权

限（如果账户已迁移到细粒度权限）。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

成员账户离开组织

1. 在 Amazon Organizations 主机上登录主Amazon Organizations 机。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在成员账户中登录。

   默认情况下，您无权访问使用创建的成员账户中的 root 用户密码 Amazon Organizations。如果需要，请按照中使用 root 用户（不建议用于日常任务）中的步骤恢复 root 用户密码使用访问组织中的成员账户 Amazon Organizations。
2. 在 Organizations 控制面板页面上，选择退出组织。
3. 在是否要退出组织？对话框中，选择退出组织。当系统提示进行确认时，确认您选择删除账户。确认后，您将被重定向到 Amazon Organizations 控制台的 “入门” 页面，您可以在其中查看您的账户加入其他组织的所有待处理邀请。

   如果显示当前无法退出组织消息，则表示您的账户尚不具备作为独立账户运行所需的所有信息。如果是这样，请继续下一步。
4. 如果是否要退出组织？对话框显示当前无法退出组织消息，选择完成账户注册步骤链接。

   如果您没有看到完成账户注册步骤链接，请使用此链接进入注册 Amazon 页面，完成缺少的注册步骤。
5. 在注册 Amazon 页面上，输入成为独立账户所需的所有信息。可能涉及以下类型的信息：

   - 联系人姓名和地址
   - 有效付款方式
   - 电话号码验证
   - 支持计划选项
6. 在出现一个指明注册过程已完成的对话框时，请选择 Leave organization。

   您将看到确认对话框。确认您选择删除账户。您将被重定向到 Amazon Organizations 控制台的 “入门” 页面，您可以在其中查看您的账户加入其他组织的所有待处理邀请。
7. 从组织中删除授予访问您账户的权限的 IAM 角色。

> **Important**
>
> 如果您的账户是在组织中创建的，则 Organizations 会自动在账户中创建一个允许组织管理账户访问的IAM角色。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。如果您想终止来自前组织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 SDKs: LeaveOrganization

成员账户离开组织后，请务必从组织中移除授予您账户访问权限的IAM角色。

> **Important**
>
> 如果您的账户是在组织中创建的，则 Organizations 会自动在账户中创建一个允许组织管理账户访问的IAM角色。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。如果您想终止来自前组织管理账户的此访问权限，则必须手动删除此IAM角色。有关如何删除角色的信息，请参阅IAM用户指南中的删除角色或实例配置文件。

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

更新成员账户的 Amazon Web Services 电子邮件地址 Amazon Organizations

为了提高安全性和管理弹性，管理账户中的IAM委托人（具有必要IAM权限）可以集中更新其任何成员账户的 Amazon Web Services 电子邮件地址（也称为主电子邮件地址），而无需单独登录每个账户。这让管理账户中的管理员（或委派管理员账户）能够更好地控制其成员账户。它还可确保您的 Amazon Organizations 任何成员账户的 Amazon Web Services 电子邮件地址保持最新，即使您可能无法访问原始的亚马逊云科技电子邮件地址或管理凭证。

当管理账户管理员集中更改 Amazon Web Services 电子邮件地址时，密码和MFA配置都将与更改前相同。请注意，控制账户的 Amazon Web Services 电子邮件地址和主要联系电话号码的用户MFA可以绕过该设置。

要更新组织中成员账户的 Amazon Web Services 电子邮件地址，您的组织必须事先启用所有功能模式。 Amazon Organizations 在整合账单模式下或不属于组织的账户中，无法集中更新其 Amazon Web Services 电子邮件地址。想要更改不受支持的账户的 Amazon Web Services 电子邮件地址的用户API应继续使用账单控制台来管理其亚马逊云科技电子邮件地址。

更新成员账户的 Amazon Web Services 电子邮件地址

使用以下步骤更新亚马逊 Web Services 的电子邮件地址。

Amazon Management Console

> **注意**
>
> - 要通过管理账户或组织中的委派管理员账户对成员账户执行此过程，必须为账户管理服务启用可信访问。
> - 如果账户所在组织与您用来调用此操作的组织不同，则不能使用此过程访问该账户。

使用 Amazon Organizations 控制台更新成员账户的 Amazon Web Services 电子邮件地址

1. 在要注销的管理账户中，以具有所需最低权限 `portal:ModifyAccount` 的用户或角色身份登录。

2. 在该Amazon Web Services 账户页面上，选择您要为其更新 Amazon Web Services 电子邮件地址的成员账户。
3. 在账户详细信息部分中选择操作按钮，然后选择更新电子邮件地址。
4. 在 “电子邮件” 下，输入成员帐户的新电子邮件地址，然后选择 “保存”。这会向新的电子邮件地址发送一次性密码 (OTP)。

> **Note**
>
> 如果您在等待代码时需要在 Organizations 控制台中关闭此页面，则可以在代码发送后的 24 小时内返回并完成该OTP过程。要执行此操作，请在账户详细信息页面上，选择操作按钮，然后选择完成电子邮件更新。

5. 在验证码下，输入在上一步中发送到新电子邮件地址的验证码，然后选择确认。这会将更新提交到账户的 Amazon Web Services 电子邮件地址。

Amazon CLI & Amazon SDKs

您可以使用以下 Amazon CLI 命令或其 Amazon SDK等效操作来检索或更新 Amazon Web Services 的电子邮件地址：

- GetPrimaryEmail
- StartPrimaryEmailUpdate
- AcceptPrimaryEmailUpdate

> **注意**
>
> - 要通过管理账户或组织中的委派管理员账户对成员账户执行这些操作，必须为账户管理服务启用可信访问。
> - 如果账户所在组织与您用来调用此操作的组织不同，则访问该账户。

> **最小权限**
>
> 对于各个操作，您必须具有映射到此操作的权限：
>
> - `account:GetPrimaryEmail`

- account:StartPrimaryEmailUpdate
- account:AcceptPrimaryEmailUpdate

如果您使用这些个人权限，则可以授予某些用户仅读取 Amazon Web Services 电子邮件地址信息的权限，而授予其他用户同时读取和写入的权限。

要完成 Amazon Web Services 电子邮件更新流程，您必须按照以下示例中显示的顺序APIs一起使用主电子邮件。

Example **GetPrimaryEmail**

以下示例从组织中的指定成员账户检索 Amazon Web Services 电子邮件地址。所用凭证必须来自组织管理账户或账户管理委托管理员账户。

```
$ aws account get-primary-email --account-id 123456789012
```

Example **StartPrimaryEmailUpdate**

以下示例启动 Amazon Web Services 电子邮件地址更新流程，识别新的电子邮件地址，并向组织中指定成员账户的新电子邮件地址发送一次性密码 (OTP)。所用凭证必须来自组织管理账户或账户管理委托管理员账户。

```
$ aws account start-primary-email-update --account-id 123456789012 --primary-email
 john@examplecorp.com
```

Example **AcceptPrimaryEmailUpdate**

以下示例接受OTP代码并将新的电子邮件地址设置为组织中的指定成员账户。所用凭证必须来自组织管理账户或账户管理委托管理员账户。

```
$ aws account accept-primary-email-update --account-id 123456789012 --otp 12345678
 --primary-email john@examplecorp.com
```

使用管理账户邀请 Amazon Organizations

创建组织并确认自己拥有与管理账户关联的电子邮件地址后，您可以邀请现有人员 Amazon Web Services 账户 加入您的组织。使用 Amazon Organizations 控制台发起和管理您向其他账户发送的邀请。您只能从组织的管理账户向其他账户发送邀请。

当你邀请一个账户时， Amazon Organizations 会向账户所有者发送邀请，账户所有者可以决定接受还是拒绝邀请。

如果您是的管理员 Amazon Web Services 账户，也可以接受或拒绝来自组织的邀请。如果接受，您的账户将成为该组织的成员之一。

要创建自动属于组织的账户，请参阅使用在组织中创建成员账户 Amazon Organizations。

> **Important**
>
> 组织中的所有账户都必须与管理账户来自同一个 Amazon 分区。商业 Amazon Web Services 区域 分区中的账户不能位于拥有来自中国区域分区的账户或位于区域分区的账户 Amazon GovCloud (US) 的组织中。

主题

注意事项

每天可以发送的邀请数量限制

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

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

一个账户只能加入一个组织

一个账户只能加入一个组织。如果您收到多个邀请，则只能接受一个邀请。

账单历史记录和报告保留在管理账户中

所有账户的账单历史记录和报告都保存在组织中的管理账户中。在将账户移动到新的组织之前，请导出或备份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、Cost Explorer 报告、节省计划报告以及预留实例（RI）利用率和覆盖范围。

管理账户负责支付成员账户产生的所有费用

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产生的所有费用。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。

Organizations 会自动创建服务相关角色 **`AWSServiceRoleForOrganizations`**

Amazon Organizations 创建名为的服务关联角色`AWSServiceRoleForOrganizations`，以支持与其他 Amazon 服务 Amazon Organizations 之间的集成。有关更多信息，请参阅 Amazon Organizations 和服务相关角色。如果您的组织支持所有功能，则受邀账户必须具有此角色。如果组织仅支持整合账单功能集，则可以删除该角色。如果您删除了此角色，之后又启用了组织中的所有功能，则会为该账户 Amazon Organizations 重新创建此角色。

Organizations 不会自动创建 IAM 角色 **`OrganizationAccountAccessRole`**

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

> **Note**
>
> 当您在组织中创建账户而不是邀请现有账户加入时，`OrganizationAccountAccessRole`默认情况下 Amazon Organizations 会自动创建 IAM 角色。

附加到根或包含该账户的 OU 的策略会立即生效

如果您将任何策略附加到根或包含受邀账户的组织单位（OU），这些策略会立即应用于受邀账户中的所有用户和角色。

您可以为组织中的其他服务启用 Amazon 服务信任。在您这样做时，该可信服务可以在组织的任何成员账户（包括受邀账户）中创建服务相关角色或执行操作。

只有整合账单功能集的组织仍然可以邀请账户

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。

使用发送账户邀请 Amazon Organizations

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 Amazon Organizations 的电子邮件地址验证。验证电子邮件地址后，请完成以下步骤来邀请账户加入您的组织。

> 最小权限
>
> Amazon Web Services 账户 要邀请加入您的组织，您必须具有以下权限：
>
> - `organizations:DescribeOrganization`（仅限控制台）
> - `organizations:InviteAccountToOrganization`

Amazon Web Services Management Console

邀请其他账户加入组织

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

   如果您的电子邮件地址还未验证，请在创建组织后的 24 小时内按照验证电子邮件中的说明进行验证。在您接收到验证电子邮件消息之前可能会有一段延迟。未完成电子邮件地址验证前，您无法邀请其他账户加入您的组织。
3. 导航到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. 在邀请现有 Amazon页面上，在要邀请的电子邮件地址或账户 ID 中，输入与 Amazon Web Services 账户 要邀请的账户关联的电子邮件地址或其账户 ID 号。
6. （可选）对于 Message to include in the invitation email message (要包含在邀请电子邮件中的消息)，输入您要包括在发送受邀请账户拥有者的电子邮件邀请中的任意文本。

7. （可选）在 Add tags (添加标签) 部分中，指定在账户管理员接受邀请后自动应用到账户的一个或多个标签。为此，请选择 Add tag (添加标签)，然后输入键和可选值。将值留空，设置为空字符串；它并非 null。您最多可以将 50 个标签附加到 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 支持。

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

   对此账户的邀请立即计入组织的最大账户数； 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 SDKs: InviteAccountToOrganization

使用管理待处理账户邀请 Amazon Organizations

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

   此页面显示从您的组织发送的所有邀请及其当前状态。

   如果您看不到邀请，请检查受邀账号是否是其他组织的管理账号。只有成员账户和独立账户才能收到邀请。管理账户无法收到邀请。

   如果您想邀请属于其他组织的管理账户的账户，建议您将该账户设为独立账户。

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

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，取消握手
- 以下示例显示了此组织向其他账户发送的邀请。

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

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

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

以下示例说明如何取消对账户的邀请。

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

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

- Amazon SDKs: ListHandshakesForOrganization, CancelHandshake

接受或拒绝账户邀请 Amazon Organizations

如果您收到加入某个组织的邀请，可以接受或拒绝该邀请。

注意事项

组织的账户状态会影响可见的成本和使用情况数据

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。

只有成员账户和独立账户可以接受或拒绝邀请

只有成员账户和独立账户可以接受或拒绝加入组织的邀请。如果向成员账户发送了邀请，则该账户应该在接受邀请之前离开当前组织。如果向已属于某个组织的管理账户发送邀请，则该账户在从其组织中移除所有成员账户并删除该组织后才能查看邀请。

接受或拒绝账户邀请

要接受或拒绝邀请，请完成以下步骤。

> 最小权限
>
> 要接受或拒绝加入 组织的邀请，您必须拥有以下权限：
>
> - `organizations:ListHandshakesForAccount`— 需要在 Amazon Organizations 控制台中查看邀请列表。
> - `organizations:AcceptHandshake`.
> - `organizations:DeclineHandshake`.
> - `iam:CreateServiceLinkedRole` – 仅在接受邀请需要在成员账户中创建服务相关角色，以支持与其他 Amazon Web Services 服务的集成时为必填项。有关更多信息，请参阅 Amazon Organizations 和服务相关角色。

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 用户的身份登录受邀账户，担任 IAM 角色；或作为该账户的根用户登录（不推荐）。
3. member account's Invitation (成员账户的邀请) 页面显示您的账户加入组织的待接受邀请。

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

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

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

     Amazon Organizations 在新成员账户中自动创建与服务相关的角色，以支持与其他 Amazon Web Services 服务成员 Amazon Organizations 之间的集成。有关更多信息，请参阅 Amazon Organizations 和服务相关角色。

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

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

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

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 SDKs: AcceptHandshake, DeclineHandshake

使用以下方式将账户迁移到其他组织 Amazon Organizations

您可以随时将一个组织 Amazon Web Services 账户 从另一个组织迁移到另一个组织。例如，当您需要将多个组织中的一个或多个 Amazon Web Services 账户 组织合并为一个组织时，在合并和收购的情况下，迁移账户可能会很有帮助。

无论是哪种应用场景，在组织之间迁移账户都需要您从旧组织中移除账户，使该账户成为独立账户，并且该账户必须接受新组织的邀请以加入新组织。在迁移过程中，工作负载和服务将继续按照您的规范运行。但要注意组织中可能存在的任何依赖项，这一点十分重要。

> **Note**
>
> 无法迁移已注销或暂停的账户
> 您无法迁移已注销或暂停的账户。要重新激活账户，请联系 Amazon Web Services 支持。
> 七天龄期要求

在组织中创建账户后，必须至少要满七天才能迁移该账户。邀请的账户不受此等待期限的限制。

在账户之间复制数据

以下 Amazon 规范性指南提供了有关在以下位置之间复制数据的策略的信息 Amazon Web Services 账户：资源复制或在资源之间迁移。 Amazon Web Services 账户

迁移账户之前需要完成的操作

在将您的组织 Amazon Web Services 账户 从一个组织迁移到另一个组织之前，请确保您已完成以下步骤。

第 1 步：检查您是否拥有迁移账户所需的IAM权限

步骤 1

确保您已应用了将账户迁移到相关组织所需的权限。

要退出组织，您必须拥有以下权限：

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

有关更多信息，请参阅从成员账户退出组织。

Amazon Web Services 账户 要邀请加入组织，您必须具有以下权限：

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

有关更多信息，请参阅邀请 Amazon Web Services 账户 加入您的组织。

要迁移账户，您不能有阻止迁移的IAM策略或服务控制策略

如果您是管理账户或委托管理员，则可以通过为组织内的IAM身份（用户、群组和角色）附加权限策略来控制对 Amazon 资源的访问权限。有关更多信息，请参阅IAM政策 Amazon Organizations。

迁移账户之前的准备：

- 检查是否存在阻止您迁移账户的IAM策略或服务控制策略 (SCPs)。

- 确定需要在迁移账户的组织中复制的现有IAM策略和服务控制策略 (SCPs)。
- 确定指定您的组织 ID 的现有IAM政策。例如，`aws:PrincipalOrgID`。

有关更多信息，请参阅《IAM用户指南》中的管理IAM策略和服务控制策略（SCPs）。

第 2 步：检查您是否已删除允许访问旧管理账户的IAM权限

步骤 2

确保您已删除允许访问旧管理账户的IAM权限，例如`OrganizationAccountAccessRole`。

当您从组织中删除成员账户时，任何为允许该组织的管理账户访问而创建的IAM角色都不会自动删除。如果您想终止来自前组织管理账户的此访问权限，则必须手动删除该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。

步骤 3：检查手机验证和付款方式

步骤 3

要迁移的账户必须作为独立账户运行一段时间后才能迁移到新组织。

要允许账户作为独立账户运行，请检查以下项目：

- 确保您的电话验证为 up-to-date。
- 确保为账户添加了有效的付款方式，以用于支付账户迁移期间产生的任何费用。
- 如果您使用发票作为付款方式，请确保您的发票是 up-to-date。

步骤 4：备份所有报告

步骤 4

请务必从管理账户导出或备份报告，尤其是账单报告。迁移账户时不会存储组织级别的报告和历史记录。建议您完整导出所有账单历史记录。您仍然可以访问成员账户的报告，例如 Amazon CloudTrail 活动历史记录和账户账单历史记录。

> **Important**
>
> 将账户从组织中移除后，所有组织级别的报告和历史记录（例如管理账户中的组织账单信息）都将被删除。

有关更多信息，请参阅成本和使用情况报告、Cost Explorer 报告、节省计划报告以及预留实例（RI）利用率和覆盖范围。

步骤 5：检查组织依赖项

步骤 5

确保要迁移的账户不存在任何与组织相关的依赖项。

要检查的依赖项：

- 如果该账户是委派管理员，则必须先将委派管理员权限取消注册，然后才能迁移账户。有关更多信息，请参阅可与之配合使用的服务 Amazon Organizations。
- 如果该账户是管理账户，则迁移前必须从组织中移除所有成员账户并删除组织。删除组织后，您的管理账户将作为独立账户运行。迁移后，管理账户将成为新组织的成员账户。有关更多信息，请参阅删除组织。
- 如果任何IAM权限取决于账户，则需要在将账户迁移到新组织后调整旧组织的权限，这样旧组织才能像以前一样运作。有关更多信息，请参阅管理组织的访问权限。
- 如果您使用任何账户或组织单位（OU）标签，则需要在新组织中重新创建这些标签。

（可选）步骤 6：如果您使用，请查看指南 Amazon Control Tower

（可选）步骤 6

如果您要将账户迁入或迁出由管理的组织 Amazon Control Tower，请查看以下 Amazon 规范性指南：将 Amazon 成员账户从 Amazon Organizations 迁移到。 Amazon Control Tower

迁移账户时需要完成的操作

迁移过程需要新组织向迁移账户发送邀请，旧组织需要移除要迁移的账户，并且要迁移的账户需要接受新组织发出的加入新组织的邀请。

迁移账户

1. 从新组织的管理账户向要迁移的账户发送邀请。您应在该账户退出旧组织之前向其发送邀请。这有助于尽可能降低要迁移的账户临时作为独立账户运行时产生的成本。有关邀请账户的信息，请参阅邀请 Amazon Web Services 账户 加入您的组织。
2. 从旧组织中移除要迁移的账户。您可以使用管理账户将成员账户从组织中移除，也可以成员账户身份退出组织。

3. 接受加入新组织的邀请。有关更多信息，请参阅接受来自组织的邀请。从一个组织迁移到另一个组织的账户将自动添加到新组织的根目录中。在将账户移至新组织中的组织单位 (OU) 之前，建议您检查要迁移的账户是否具有相应的组织策略和 OU 权限。
4. 要迁移管理账户，必须首先从组织中移除所有成员账户并删除组织，然后才能将管理账户迁移到新组织。删除旧组织后，您的管理账户将作为独立账户运行，并且可以接受新组织发出的加入新组织的邀请。如果您接受邀请，该管理账户将成为新组织的成员账户。

迁移账户之后需要完成的操作

在将账户从一个组织迁移到另一个组织之后，务必要完成以下步骤。

迁移后检查

1. 评估迁移后账户的所有账单工具配置，例如成本类别、预算和账单警报等。
2. 对于您从一个组织迁移到另一个组织的所有账户，检查并更新以下货币信息：
   a. 必要时更新账户的税务设置。
   b. 确保要迁移的账户的 Amazon Web Services 支持 计划与新组织的付款人账户相匹配。
   c. 检查您可能想应用到迁移后账户的任何可能免税待遇。
3. 验证并确认已迁移账户的现有IAM策略和服务控制策略 (SCPs)。例如，您可能需要更新某些IAM策略的组织 ID 以反映新组织。
4. 更新您迁移了账户的新组织的成本分配标签。您需要更新您迁移的账户之前收集的所有成本分配标签。
5. 任何预留实例和节省计划都将随账户一起迁移，而不会保留在旧组织中。 Amazon Web Services 支持 如果需要将这些文件转移到旧组织，请联系。

使用 Amazon Organizations 查看组织中账户的详细信息

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

使用 Amazon Organizations 导出组织中账户的详细信息

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。

> **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 或 CREATED。

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

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

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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择 Actions（操作），然后对于 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！）选择下载 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。

使用 Amazon Organizations 更新组织中账户的备用联系人

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。

使用 Amazon Organizations 更新组织中账户的主要联系人信息

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主要联系人信息。要了解如何更新主要联系人信息，请参阅《Amazon 账户管理参考》中的访问或更新主要账户联系人。

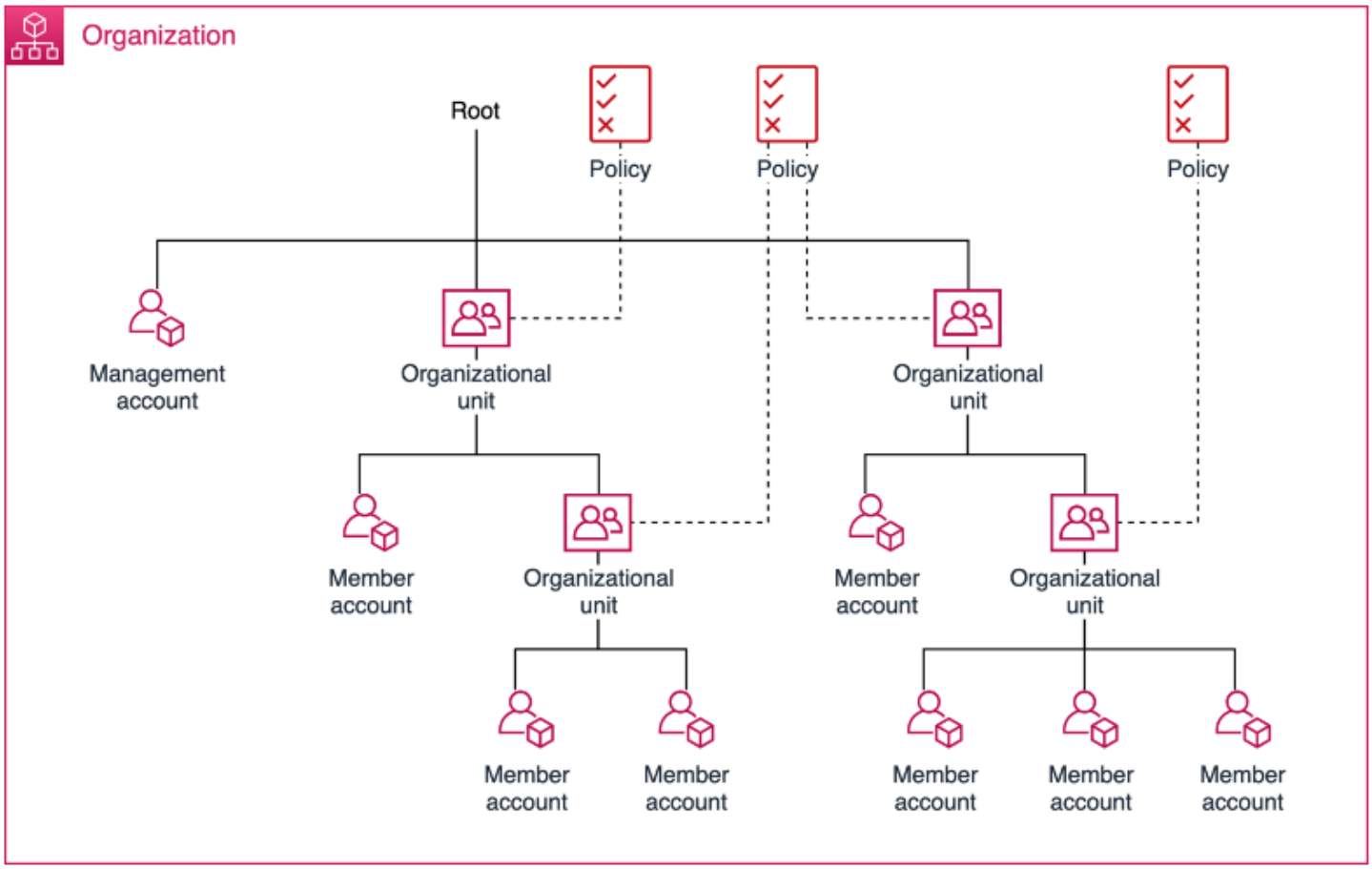
使用 Amazon Organizations 更新为组织中账户启用的 Amazon Web Services 区域

您可以通过 Amazon Organizations 控制台为组织内的账户更新已启用 Amazon Web Services 区域。要了解如何更新已启用的 Amazon Web Services 区域，请参阅《Amazon 账户管理参考》中的 Specifying which Amazon Web Services 区域 your account can use。

使用管理组织单位 (OUs) Amazon Organizations

您可以使用组织单位 (OUs) 将账户组合在一起，作为一个单元进行管理。这将极大简化您的账户管理。例如，您可以将基于策略的控制附加到 OU，该 OU 中的所有账户将自动继承策略。你可以在一个组织 OUs 内创建多个组织，也可以在其他组织 OUs 中创建 OUs。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。

下图显示了一个由七个账户组成的组织，这些账户在根目录 OUs 下分为四个账户。该组织还有一些政策适用于 OUs。



> **Note**
>
> 组织中有一个根，它 Amazon Organizations 会在你第一次建立组织时为你创建。

主题

- 管理组织单位 (OUs) 的最佳实践 Amazon Organizations

- 使用 Amazon Organizations 浏览根和组织单位（OU）层次结构
- 使用 Amazon Organizations 查看组织单位（OU）的详细信息
- 使用 Amazon Organizations 创建组织单位（OU）
- 使用 Amazon Organizations 重命名组织单位（OU）
- 使用 Amazon Organizations 标记组织单位（OU）
- 使用 Amazon Organizations 将账户移动到 OU 或者在根和 OU 之间移动
- 使用 Amazon Organizations 查看根的详细信息
- 使用 Amazon Organizations 删除组织单位（OU）

管理组织单位 (OUs) 的最佳实践 Amazon Organizations

请遵循以下建议，以帮助您完成 Amazon Organizations 使用组织单位管理多账户环境的过程（OUs）。

主题

- 理解 Amazon Organizations
- 推荐的基础组织单位 () OUs
- 建议增设组织单位 (OUs)
- 结论

理解 Amazon Organizations

架构完善的多账户 Amazon 环境的基础是 Amazon Organizations，它使您能够集中管理和管理多个账户。组织单位 (OU) 是组织中账户的逻辑分组。 OUs 使您能够将帐户组织成层次结构，并帮助您应用管理控制。Or ganizations 策略定义了您可以应用于一组的控制措施 Amazon Web Services 账户。例如，服务控制策略 (SCP) 是一种策略，用于定义组织中的账户可以执行的 Amazon Web Services 服务操作，例如 Amazon EC2 Run Instance。

虽然您可以从一个账户开始您的 Amazon 旅程，但 Amazon 建议您随着工作负载规模和复杂性的增加而设置多个帐户。使用多账户环境是一种 Amazon 最佳实践，它可以带来以下好处：

- 满足各种要求的快速创新：您可以将资源分配 Amazon Web Services 账户 给公司内的不同团队、项目或产品，以帮助确保他们每个人都能快速创新，同时满足自己的安全需求。
- 简化计费：使用倍数 Amazon Web Services 账户 可以帮助确定哪个产品或服务系列负责 Amazon 收费，从而简化 Amazon 成本分摊方式。

- 灵活的安全控制：您可以使用多个 Amazon Web Services 账户 来隔离具有特定安全要求或需要满足严格合规性准则（例如 HIPAA 或 PCI）的工作负载或应用程序。
- 适应业务流程：您可以以最能反映公司业务流程的不同需求的方式组织多个 Amazon Web Services 账户 业务流程，这些业务流程具有不同的运营、监管和预算要求。

推荐的基础组织单位 () OUs

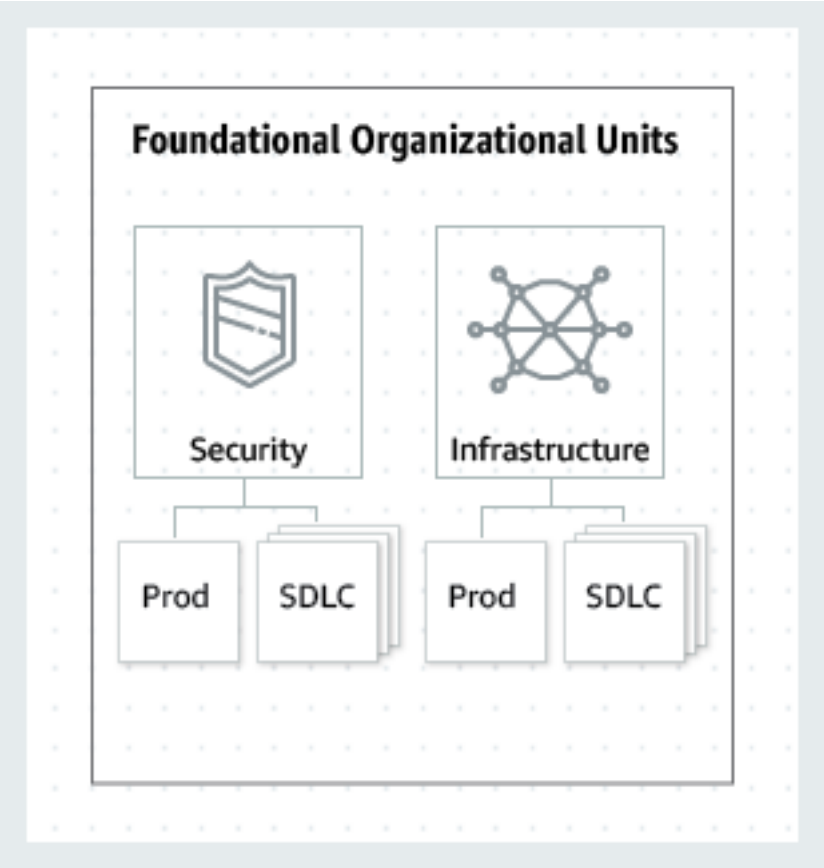
您的组织单位 (OUs) 应基于职能或常用控件集，而不是反映公司的报告结构。 Amazon 建议您从安全性和基础架构入手。大多数企业都有集中式的团队来满足这些需求，为整个组织提供服务。我们建议 OUs 为这些特定功能创建一组基础知识：

- 安全性：用于安全服务。为日志存档、安全只读访问、安全工具和“打碎玻璃”程序分别创建账户。
- 基础设施：用于共享的基础设施服务，例如联网和 IT 服务。为您需要的每种基础设施服务分别创建账户。

鉴于大多数公司对生产工作负载有不同的策略要求，因此基础设施和安全性可以嵌套 OUs 于非生产 (SDLC) 和生产 (Prod)。SDLC OU 中的账户用于承载非生产工作负载，不应存在来自其他账户的生产依赖项。如果生命周期阶段之间的 OU 策略存在差异，则 SDLC 可以分为多个阶段 OUs（例如，开发阶段和预生产阶段）。Prod OU 中的账户用于承载生产工作负载。

根据您的要求在 OU 级别应用策略来管理 Prod 和 SDLC 环境。通常，在 OU 级别应用策略比在单个账户级别应用策略更好，因为这可以简化策略管理以及任何可能的问题排查。

下图显示了安全和基础架构的基础 OUs（Prod 和 SDLC）：



建议增设组织单位 (OUs)

中央服务到位后，我们建议您创建 OUs 与构建或运行您的产品或服务直接相关的服务。许多 Amazon 客户在建立基础 OUs 后构建了以下内容：

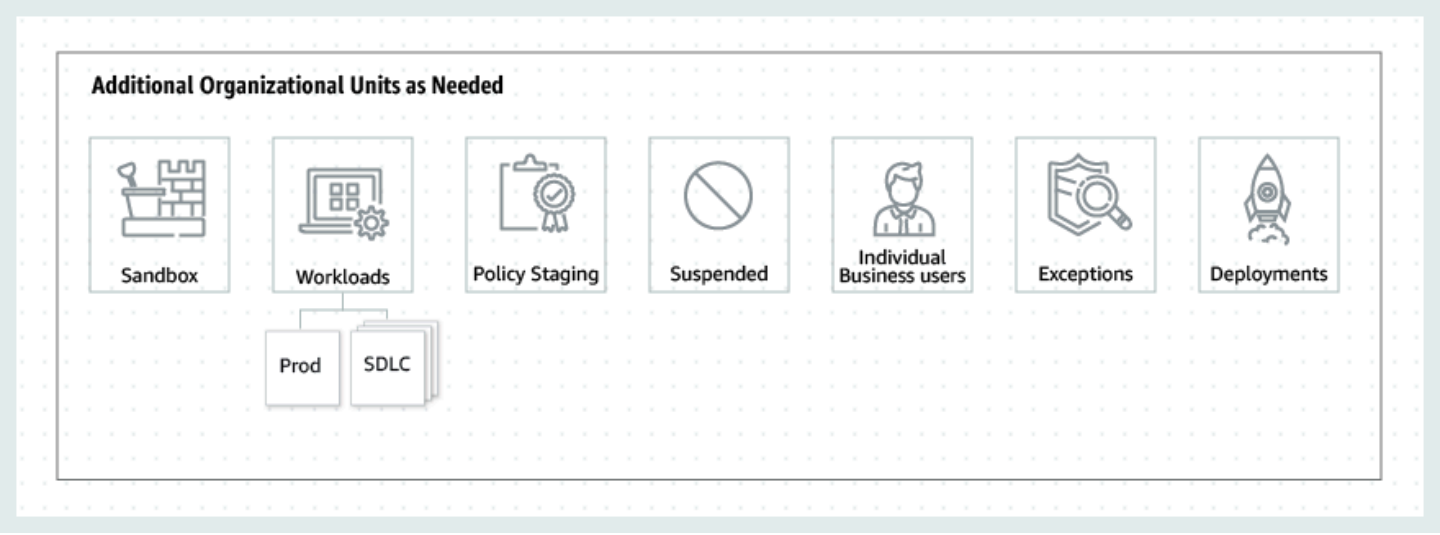
- 沙盒：个人开发者可以用来进行实验的 Amazon Web Services 服务沙盒。 Amazon Web Services 账户 确保这些账户可以与内部网络分离。
- 工作负载： Amazon Web Services 账户 包含托管面向外部的应用程序服务的工作负载。您应该 OUs 在 SDLC 和 Prod 环境（类似于基础环境 OUs）下进行构建，以便隔离和严格控制生产工作负载。

我们还建议根据您的具体需求添加额外的 OUs 维护和持续扩展。以下是基于现有 Amazon 客户实践的一些常见主题：

- P@@ olicy St aging：持有 Amazon 账户，您可以在其中测试提议的政策变更，然后将其广泛应用于组织。首先在计划的 OU 中实施账户级别的变更，然后慢慢地将变更应用到其他账户以及整个组织的其他部门。 OUs

- 已@@ 暂停： Amazon Web Services 账户 已关闭并等待从组织中删除的内容。将某个会拒绝所有操作的 SCP 附加到此 OU。如果需要还原，请务必在账户上标记详细信息以实现可追溯性。
- 个人企业用户：一种受限访问的 OU，包含 Amazon Web Services 账户 可能需要创建与业务生产力相关的应用程序的业务用户（非开发人员），例如设置 S3 存储桶以与合作伙伴共享报告或文件。
- 例外：暂挂 Amazon Web Services 账户 用于具有高度定制的安全或审计要求的业务用例，这些要求与工作负载组织单位中定义的要求不同。例如， Amazon Web Services 账户 专门为机密的新应用程序或功能设置一个。在账户 SCPs 级别使用，以满足定制需求。考虑使用 Amazon 和Amazon Config 规则设置检测 EventBridge和反应系统。
- 部署：包含 Amazon Web Services 账户 用于工作负载组织单元中应用程序delivery/deployment (CI/CD deployments). You can create this OU if you have a different governance and operational model for CI/CD deployments as compared to accounts in the Workloads OUs (Prod and SDLC). Distribution of CI/CD helps reduce the organizational dependency on a shared CI/CD environment operated by a central team. For each set of SDLC/Prod Amazon Web Services 账户 的持续集成和持续运行，在部署组织单元下创建 CI/CD 帐户。
- 过渡：在将现有账户和工作负载转移到临时暂存区域，然后再移动到组织的标准区域。这可能是因为账户是收购的一部分，以前由第三方管理，或者是旧组织结构中的旧账户。

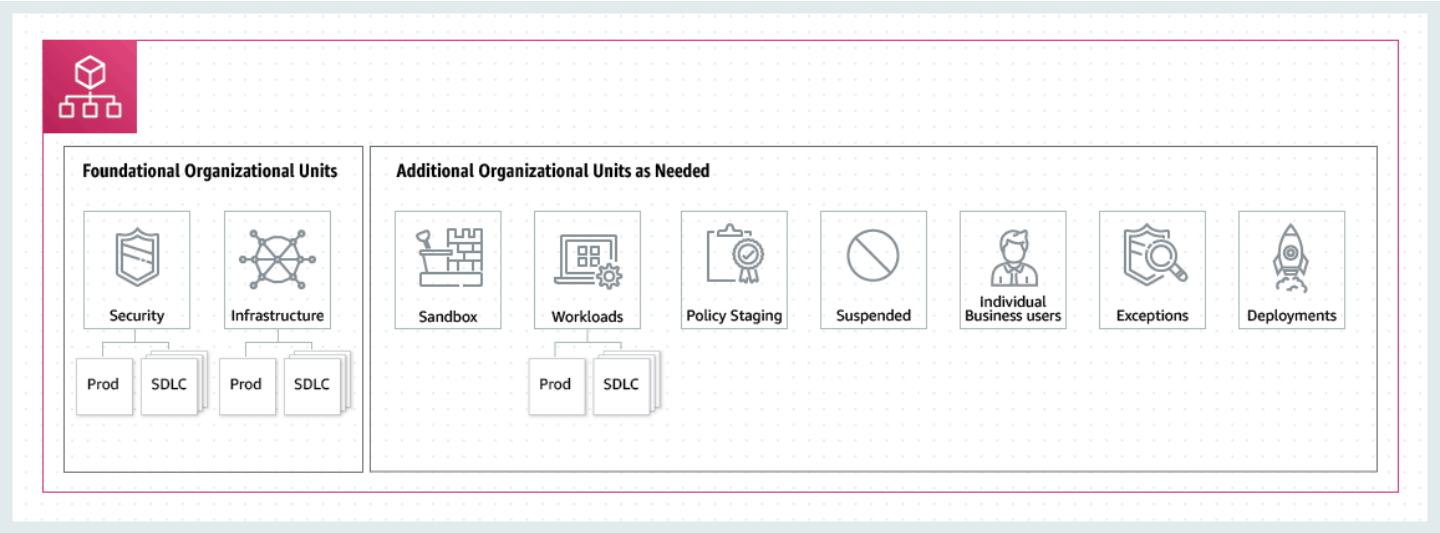
下图显示了沙箱、工作负载、策略暂存、暂停、个人业务用户、异常、部署和过渡账户的其他 OUs 内容：



结论

精心设计的多账户策略可以帮助您进行创新 Amazon，同时有助于确保满足您的安全性和可扩展性需求。本主题中描述的框架代表了 Amazon 最佳实践，您应该将其用作 Amazon 旅程的起点。

下图显示了推荐的基础知识 OUs 和其他 OUs内容：



使用 Amazon Organizations 浏览根和组织单位（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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 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的展开图标（ ）。
   要减少视觉混乱和折叠树结构的分支，请选择展开的父实体旁边的折叠图标（ ）。
4. 选择 OU 或根的名称以查看其详细信息并执行某些操作。或者，您可以选择名称旁的单选按钮，然后在 Actions (操作) 菜单中的实体上执行某些操作。

您还可以使用表格形式查看仅在您组织中的账户列表，而无需先导航到 OU 来找到它们。在此视图中，您无法看到任何 OU，也无法操纵附加到它们的策略。

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

使用 Amazon Organizations 查看组织单位（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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在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

使用 Amazon Organizations 创建组织单位（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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 导航到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，在您看到所需内容后，请选择其名称。
4. 在层次结构中选择了正确的父 OU 后，在 Actions (操作) 菜单上的 Organizational Unit (组织部门) 下，选择 Create new (新建)
5. 在 Create organizational unit (创建组织部门) 对话框中，键入要创建的 OU 的名称。
6. （可选）添加一个或多个标签，方法是选择 Add tag (添加标签)，然后输入一个键和可选的值。将值留空，设置为空字符串；它并非 `null`。您最多可以向 OU 附加 50 个标签。
7. 最后，选择 Create organizational unit (创建组织部门)。

您的新 OU 显示在父级内部。现在，您可以将账户移动到此 OU 或者为其附加策略。

Amazon CLI 与 Amazon SDK

创建 OU

以下代码示例演示如何使用 `CreateOrganizationalUnit`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 在 GitHub 上查看更多内容。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitName = "ProductDevelopmentUnit";

        var request = new CreateOrganizationalUnitRequest
        {
            Name = orgUnitName,
            ParentId = "r-0000",
        };

        var response = await client.CreateOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
```

```
                Console.WriteLine($"Successfully created organizational unit:
 {orgUnitName}.");
                Console.WriteLine($"Organizational unit {orgUnitName} Details");
                Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
 {response.OrganizationalUnit.Id}");
            }
            else
            {
                Console.WriteLine("Could not create new organizational unit.");
            }
        }
    }
```

- 有关 API 的详细信息，请参阅《适用于 .NET 的 Amazon SDK API 参考》中的 CreateOrganizationalUnit。

CLI

Amazon CLI

在根 OU 或父 OU 中创建 OU

以下示例演示如何创建名为 AccountingOU 的 OU：

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

输出包括一个 organizationalUnit 对象，其中包含有关新 OU 的详细信息：

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- 有关 API 详细信息，请参阅《Amazon CLI 命令参考》中的 CreateOrganizationalUnit。

使用 Amazon Organizations 重命名组织单位（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 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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Amazon Web Services 账户 页面，导航到要重命名的 OU，然后执行下面的一种步骤：
   - 选择要重命名的 OU 旁边的单选按钮
     然后，在 Actions (操作) 菜单中的 Organizational unit (组织部门) 下，选择 Rename (重命名)。
   - 选择 OU 的名称，以访问 OU 的详细信息页面。然后再页面的顶部选择 Rename (重命名)。
3. 在 Rename organizational unit (重命名组织部门) 对话框中，输入新名称，然后选择 Save changes (保存更改)。

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

使用 Amazon Organizations 标记组织单位（OU）

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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Amazon Web Services 账户 页面上，导航到要编辑其标签的 OU 并选择其名称。
3. 在 OU 的详细信息页面上，选择 Tags (标签) 选项卡，然后选择 Manage tags (管理标签)。
4. 您可以在此选项卡上执行以下操作：

- 编辑任何标签的值，方法是在旧标签上输入新值。您不能修改标签键。要更改键，您必须删除带有旧键的标签，然后添加使用新键的标签。
- 删除现有标签，方法是选择要重命名的标签旁边的 Remove (删除)。
- 添加新的标签键和值对。选择 Add tag (添加标签)，然后在提供的框中输入新的键名称和可选值。如果您将 Value (值) 框留空，则值是空字符串；它并非 null。

5. 在完成所有要进行的添加、删除和编辑操作之后，选择 Save changes (保存更改)。

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

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

使用 Amazon Organizations 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，您可以查看管理根的详细信息。

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

使用 Amazon Organizations 删除组织单位（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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在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 与 Amazon SDK

删除 OU

以下代码示例演示如何使用 `DeleteOrganizationalUnit`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 在 GitHub 上查看更多内容。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
```

```
    {
        /// <summary>
        /// Initializes the Organizations client object and calls
        /// DeleteOrganizationalUnitAsync to delete the organizational unit
        /// with the selected ID.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var orgUnitId = "ou-0000-00000000";

            var request = new DeleteOrganizationalUnitRequest
            {
                OrganizationalUnitId = orgUnitId,
            };

            var response = await client.DeleteOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- 有关 API 的详细信息，请参阅《适用于 .NET 的 Amazon SDK API 参考》中的 DeleteOrganizationalUnit。

CLI

Amazon CLI

删除 OU

以下示例说明如何删除 OU。该示例假设您之前已从 OU 中删除所有账户和其他 OU：

```
aws organizations delete-organizational-unit --organizational-unit-id ou-examplerootid111-exampleouid111
```

- 有关 API 详细信息，请参阅《Amazon CLI 命令参考》中的 DeleteOrganizationalUnit。

使用管理组织政策 Amazon Organizations

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

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

主题

策略类型

Organizations 提供了以下两大类的策略类型：

授权策略

授权策略可帮助您集中管理 Amazon Web Services 账户 整个组织的安全性。

- 服务控制策略 (SCPs) 提供对组织中 IAM 用户和 IAM 角色的最大可用权限的集中控制。

- 资源控制策略 (RCPs) 提供对组织中资源的最大可用权限的集中控制。

管理策略

管理策略可帮助您在整个组织中集中配置 Amazon Web Services 服务 和管理其功能。

- 声明式策略允许您在整个组织中大规模集中声明和强制执行给 Amazon Web Services 服务 定配置所需的配置。连接后，当服务添加新功能或时，配置将始终保持不变 APIs。
- Backup 策略允许您集中管理备份计划并将其应用于组织账户中的 Amazon 资源。
- 标签策略允许您标准化附加到组织账户中 Amazon 资源的标签。
- 聊天机器人策略允许你控制聊天应用程序（例如 Slack 和 Microsoft Teams）对组织账户的访问权限。
- AI 服务选择退出策略允许您控制组织中所有账户的 Amazon AI 服务数据收集。

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

策略类型	策略类别	影响管理账户	可附加到根、OU 或账户的最大数量	最大大小	支持查看 OU 或账户的有效策略
SCP	授权	否	5	5120 个字符	否
RCP	授权	否	5	5120 个字符	否
声明性政策	管理	是	10	10,000 个字符	是

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

中的授权策略 Amazon Organizations

中的授权策略 Amazon Organizations 使您可以集中配置和管理成员账户中委托人和资源的访问权限。这些策略如何影响您应用这些策略的组织单位 (OUs) 和账户取决于您所应用的授权策略的类型。

中有两种不同类型的授权策略 Amazon Organizations：服务控制策略 (SCPs) 和资源控制策略 (RCPs)。

主题

- SCPs 和之间的区别 RCPs
- 使用 SCPs 和 RCPs
- 服务控制策略 (SCPs)

- 资源控制策略 (RCPs)

SCPs 和之间的区别 RCPs

SCPs 是以校长为中心的控件。 SCPs 针对成员账户中委托人可用的最大权限创建权限护栏或设置限制。当您想要对组织中的委托人集中实施一致的访问控制时，可以使用 SCP。这可能包括指定您的 IAM 用户和 IAM 角色可以访问哪些服务，他们可以访问哪些资源，或者他们可以在什么条件下提出请求（例如，来自特定区域或网络）。

RCPs 是以资源为中心的控制措施。 RCPs 为成员账户中的资源的最大可用权限创建权限护栏或设置限制。如果要对组织中的资源集中实施一致的访问控制，则可以使用 RCP。这可以限制对您的资源的访问权限，使它们只能由属于您的组织的身份进行访问，或者指定组织外部身份可以访问您的资源的条件。

有些控件可以通过 SCPs 和以类似的方式应用 RCPs。例如，您可能希望阻止用户将未加密的对象上传到 S3，这些对象可以写成 SCP，以强制控制您的委托人可以对您的 S3 存储桶执行的操作。此控件也可以写成 RCP，以便在任何委托人将对象上传到您的 S3 存储桶时都需要加密。如果您的存储桶允许组织外部的委托人（例如第三方供应商）将对象上传到您的 S3 存储桶，则第二种选择可能是首选。但是，有些控件只能在 RCP 中实现，有些控制只能在 SCP 中实现。有关更多信息，请参阅 和的一般用 SCPs 例 RCPs。

使用 SCPs 和 RCPs

SCPs 并且 RCPs 是独立的控制机构。您可以选择仅启用 SCPs 或 RCPs，或者同时使用这两种策略类型。通过同时使用 SCPs 和 RCPs，您可以围绕您的身份和资源创建数据边界。

SCPs 提供控制您的身份可以访问哪些资源的功能。例如，您可能希望允许您的身份访问 Amazon 组织中的资源。但是，您可能需要防止自己的身份访问组织外部的资源。您可以使用强制执行此控制 SCPs。

RCPs 提供控制哪些身份可以访问您的资源的功能。例如，您可能希望允许组织中的身份访问组织中的资源。但是，您可能需要防止组织外部的身份访问您的资源。您可以使用强制执行此控制 RCPs。RCPs 提供影响组织外部委托人访问您的资源的有效权限的能力。 SCPs 只能影响 Amazon 组织内委托人的有效权限。

和的一般用 SCPs 例 RCPs

下表详细介绍了使用 SCP 的一般用例以及 RCPs

使用案例	策略类型	影响 你的身份	外部身份	你的资源	外部资源（请求的目标）
限制您的身份可以使用的服务或操作	SCP	X 形		X 形	X 形
限制您的身份可以访问哪些资源	SCP	X 形		X 形	X 形
强制要求您的身份如何访问资源	SCP	X 形		X 形	X 形
限制哪些身份可以访问您的资源	RCP	X 形	X 形	X 形	
保护组织中的敏感资源	RCP	X 形	X 形	X 形	
强制要求如何访问您的资源	RCP	X 形	X 形	X 形	

服务控制策略 (SCPs)

服务控制策略 (SCPs) 是一种组织策略，可用于管理组织中的权限。 SCPs为组织中的IAM用户和IAM角色提供对最大可用权限的集中控制。 SCPs帮助您确保您的帐户符合组织的访问控制准则。 SCPs仅在启用了所有功能的组织中可用。 SCPs如果您的组织仅启用了整合账单功能，则不可用。有关启用 SCPs 的说明，请参阅启用策略类型。

SCPs不要向组织中的IAM用户和IAM角色授予权限。不授予任何权限SCP。对组织中的IAM用户和IAM角色可以执行的操作SCP定义权限护栏或设置限制。要授予权限，管理员必须附加策略来控制访问权限，例如附加到IAM用户和IAM角色的基于身份的策略，以及附加到您账户中资源的基于资源的策略。有关更多信息，请参阅《用户指南》中的基于身份的策略和基于资源的策略。IAM

有效权限是SCP和资源控制策略 (RCPs) 所允许的权限与基于身份和基于资源的策略所允许的权限之间的逻辑交集。

> **⚠ SCPs不影响管理账户中的用户或角色**
>
> SCPs不要影响管理账户中的用户或角色。它们仅影响组织中的成员账户。这也意味着这SCPs适用于被指定为授权管理员的成员账户。

本页面上的主题

的测试效果 SCPs

Amazon 强烈建议您在未彻底测试该政策对账户的影响之前，不要将其附加SCPs到组织的根目录上。您可以改为创建一个 OU，并将您的账户一次移入一个，或至少每次以少量移入，以确保您不会无意中阻止用户使用关键服务。确定账户是否使用服务的一种方法是检查服务上次访问的 IAM 数据。另一种方法是Amazon CloudTrail 使用记录API级别的服务使用情况。

> **Note**
>
> 除非您修改 F ullAWSAccess 策略或将其替换为具有允许操作的单独策略，否则成员账户的所有操作都将失败，否则成员账户的所有 Amazon 操作都将失败。

最大大小为 SCPs

你中的所有字符都按其最大大小进行SCP计数。本指南中的示例显示了带有额外空格以提高其可读性的SCPs格式化内容。但是，在您的策略大小接近最大大小时，可以删除任何空格（例如，引号之外的空格字符和换行符）来节省空间。

> **Tip**
>
> 使用可视化编辑器来构建你的SCP. 它会自动删除额外的空格。

隶SCPs属于组织中的不同级别

有关SCPs工作原理的详细说明，请参阅SCP 评估。

SCP对权限的影响

SCPs与 Amazon Identity and Access Management 权限策略类似，使用几乎相同的语法。但是，SCP从不授予权限。取而代之SCPs的是为组织中的IAM用户和IAM角色指定最大可用权限的访问控制。有关更多信息，请参阅《IAM用户指南》中的策略评估逻辑。

- SCPs仅影响由属于组织的账户管理的IAM用户和角色。 SCPs不要直接影响基于资源的策略。也不会影响组织外的账户的用户或角色。例如，请考虑一个 Amazon S3 存储桶，它由组织中的账户“A”所有。存储桶策略（一种基于资源的策略）会向来自组织外账户 B 的用户授予访问权限。账户 A 已SCP附加。这SCP不适用于账户 B 中的外部用户，仅SCP适用于组织中由账户 A 管理的用户。
- SCP限制成员账户中IAM用户和角色的权限，包括成员账户的根用户。任何账户都只有上方的每个父级允许的那些权限。如果某个权限在账户以上的任何级别被隐式（未包含在`Allow`策略声明中）或明确阻止（包含在`Deny`策略声明中），则受影响账户中的用户或角色将无法使用该权限，即使账户管理员向该用户附加了具有*/*权限的`AdministratorAccess`IAM策略。
- SCPs仅影响组织中的成员帐户。它们对管理账户中的用户或角色没有任何影响。这也意味着这SCPs适用于被指定为授权管理员的成员账户。有关更多信息，请参阅 管理账户的最佳实践。
- 仍然必须通过适当的 IAM 权限策略将权限授予用户和角色。没有任何IAM权限策略的用户没有访问权限，即使适用的SCPs允许所有服务和所有操作。
- 如果用户或角色的IAM权限策略授予对相应用户也允许的操作的访问权限SCPs，则该用户或角色可以执行该操作。
- 如果用户或角色的IAM权限策略允许访问相应用户不允许或明确拒绝的操作SCPs，则该用户或角色将无法执行该操作。

- SCPs影响关联账户中的所有用户和角色，包括 root 用户。唯一例外在 不受限制的任务和实体 SCPs中介绍。
- SCPs不影响任何服务相关角色。服务相关角色允许其他角色与 Amazon Web Services 服务 之集成 Amazon Organizations ，并且不能受其限制。SCPs
- 当您在根目录中禁用SCP策略类型时，所有策略SCPs类型将自动与该根目录中的所有 Amazon Organizations 实体分离。 Amazon Organizations 实体包括组织单位、组织和账户。如果您在根目录SCPs中重新启用，则该根目录将恢复为仅自动附加到根目录中所有实体的默认`FullAWSAccess`策略。之前SCPs被禁用的 Amazon Organizations 实体的所有附件都将丢失且无法自动恢复，但您可以手动重新连接它们。SCPs
- 如果同时存在权限边界（高级IAM功能）和权限，则边界SCP、和基于身份的策略都必须允许该操作。SCP

使用访问数据进行改进 SCPs

使用管理账户凭据登录后，您可以在IAM控制台Amazon Organizations部分查看 Amazon Organizations 实体或策略的上次访问服务数据。您也可以使用 Amazon Command Line Interface (Amazon CLI) 或 Amazon API in IAM 来检索上次访问服务的数据。这些数据包括 Amazon Organizations 账户中的IAM用户和角色上次尝试访问哪些允许的服务以及何时访问的信息。您可以使用此信息来识别未使用的权限，以便可以完善您的权限，SCPs以更好地遵守最低权限原则。

例如，您可能有一个拒绝列表 SCP，禁止访问三个 Amazon Web Services 服务。`Deny`声明中未列出的所有服务均被允许。SCP中的服务上次访问的数据会IAM告诉您 Amazon Web Services 服务 哪些数据是允许的，SCP但从未使用过。有了这些信息，您可以更新SCP以拒绝访问不需要的服务。

有关更多信息，请参阅《IAM 用户指南》中的以下主题：

- 查看 Organizations 的 Organizations 服务上次的访问数据
- 使用数据来细化组织部门的权限

不受限制的任务和实体 SCPs

您不能使用SCPs来限制以下任务：

- 管理账户执行的任何操作
- 使用附加到服务相关角色的权限执行的任何操作
- 以根用户身份注册企业支持计划

- 为 CloudFront 私有内容提供可信签名者功能
- 以根用户身份DNS为 Amazon Lightsail 电子邮件服务器和亚马逊EC2实例进行反向配置
- 一些 Amazon相关服务的任务：
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - 亚马逊产品营销 API

SCP 评估

> **Note**
>
> 本节中的信息不适用于管理策略类型，包括备份策略、标签策略、聊天机器人策略或 AI 服务选择退出策略。有关更多信息，请参阅 了解管理策略继承。

由于您可以在中附加不同级别的多个服务控制策略 (SCPs) Amazon Organizations，因此了解评估 SCPs 方式可以帮助您编写 SCPs 得出正确结果的内容。

主题

- 如何 SCPs 使用 “允许”
- 如何 SCPs 使用 “拒绝”
- 使用策略 SCPs

如何 SCPs 使用 “允许”

要允许特定账户获得权限，在从根到账户直接路径中的每个 OU（包括目标账户本身），每个级别都必须有显式**`Allow`**语句。这就是为什么在启用 SCPs时会 Amazon Organizations 附加名为 F ull 的 Amazon 托管 SCP 策略AWSAccess，该策略允许所有服务和操作。如果该政策在组织的任何级别被删除且未被替换，则该级别下的所有 OUs和账户都将被禁止采取任何行动。

例如，我们来看一下图 1 和图 2 所示的场景。要允许账户 B 获得权限或服务，应将允许该权限或服务的 SCP 附加到根、生产 OU 和账户 B 本身。

SCP 评估遵循 deny-by-default模型，这意味着任何未明确允许的权限 SCPs 都将被拒绝。如果 SCPs 在任何级别（例如根、生产 OU 或账户 B）中都没有允许声明，则访问将被拒绝。

备注

- SCP 中的 `Allow` 语句允许 `Resource` 元素仅包含一个 `"*"` 条目。
- SCP 中的 `Allow` 语句完全不能有 `Condition` 元素。

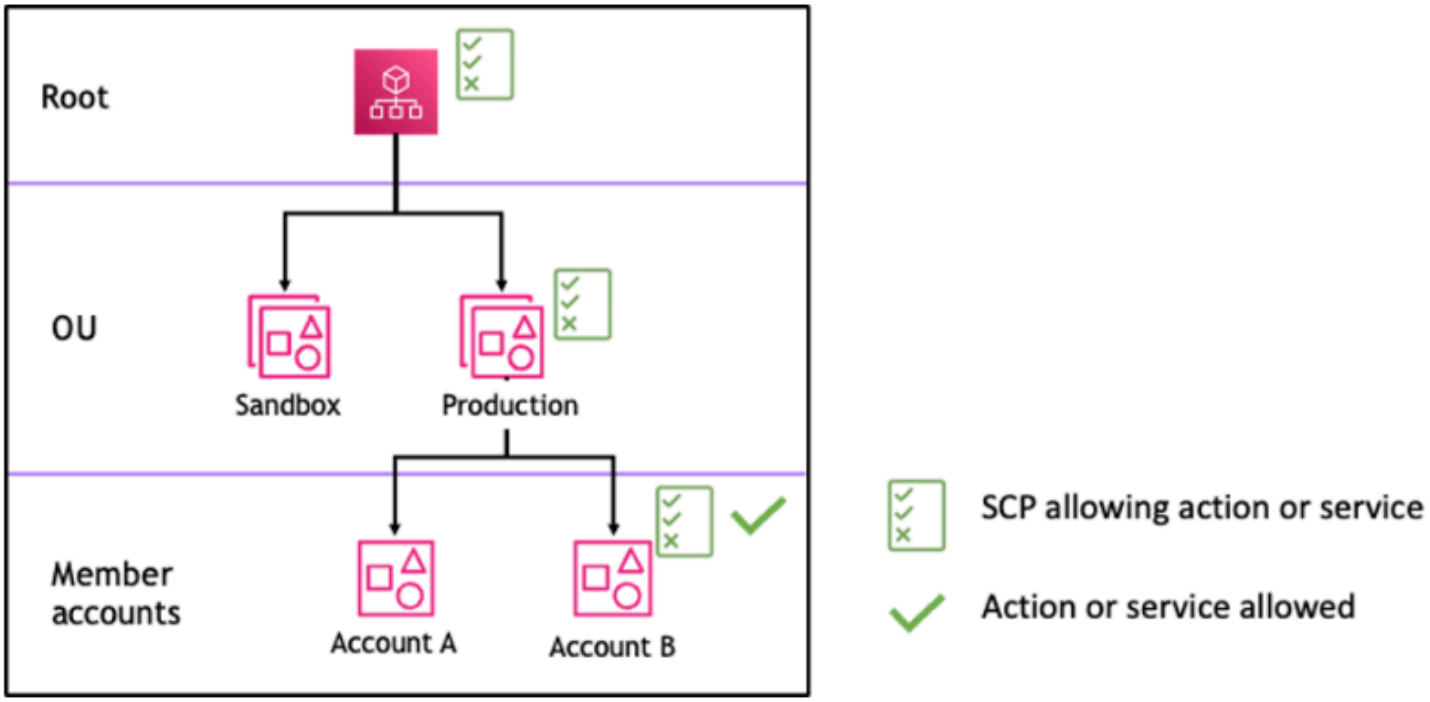


图 1：在根、生产 OU 和账户 B 处附加 *Allow* 语句的组织结构示例

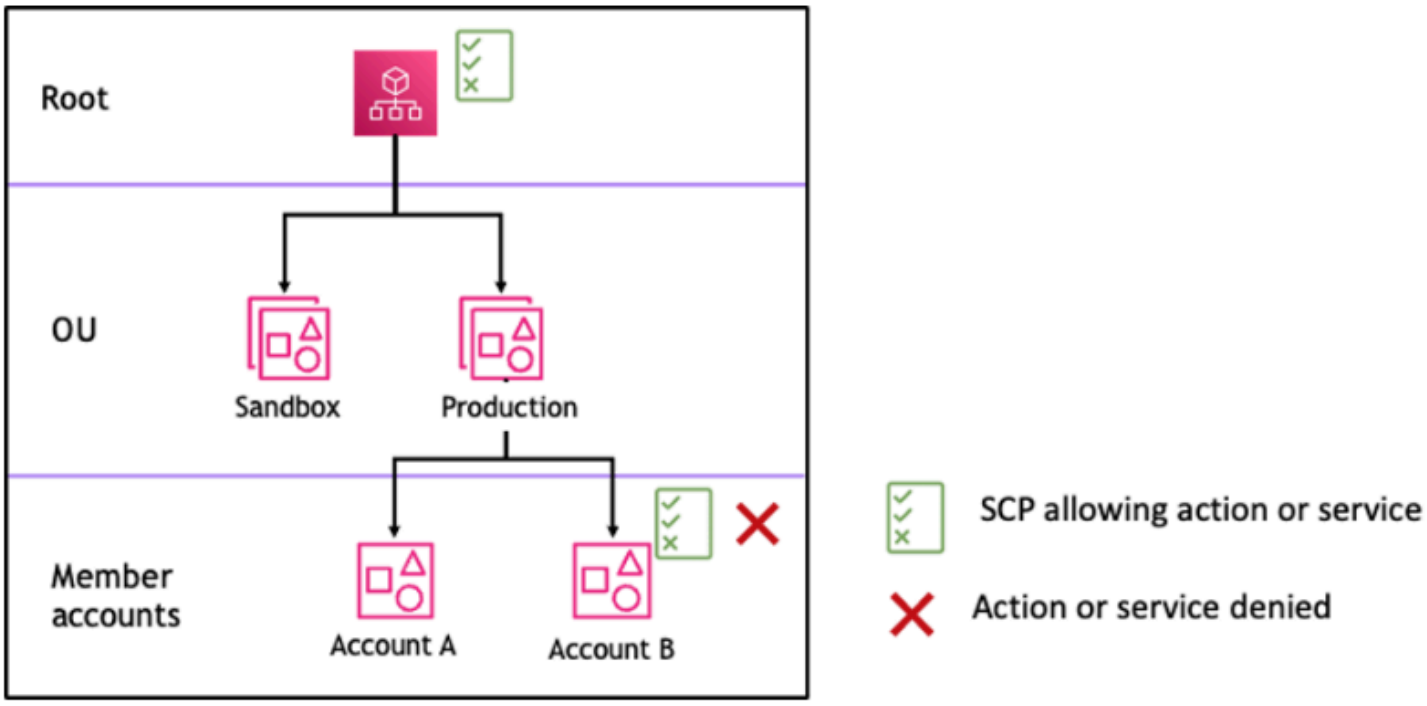


图 2：生产 OU 中缺少 *Allow* 语句的组织结构示例及其对账户 B 的影响

如何 SCPs 使用 “拒绝”

要拒绝特定账户获得权限，在从根到账户直接路径中的每个 OU（包括目标账户本身），任何 SCP 都可以拒绝该权限。

例如，假设有一个 SCP 附加到生产 OU，它为给定服务指定了显式 Deny 语句。碰巧还有另一个 SCP 附加到根和账户 B，它显式允许访问相同的服务，如图 3 所示。因此，账户 A 和账户 B 都将被拒绝访问该服务，因为将针对组织下的所有账户 OUs 和成员账户评估附加到组织中任何级别的拒绝策略。

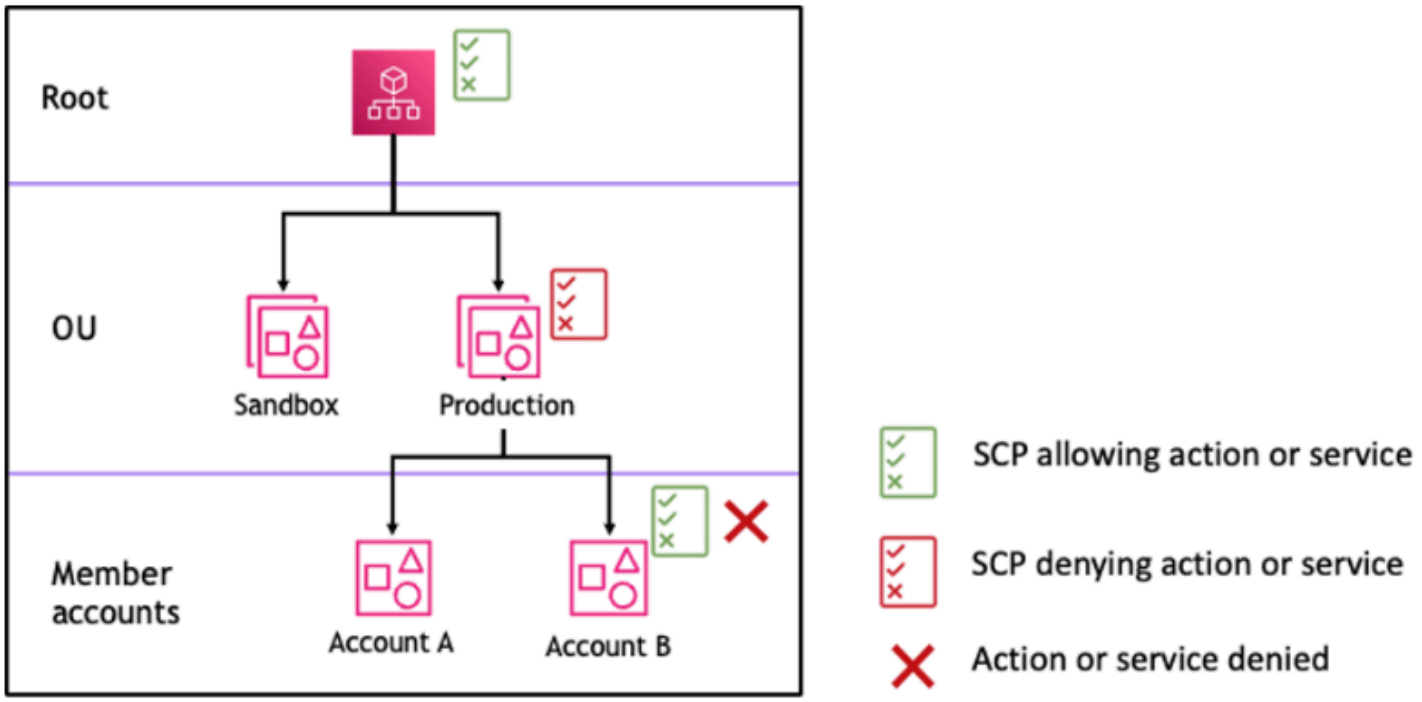


图 3：生产 OU 中附加了 *Deny* 语句的组织结构示例及其对账户 B 的影响

使用策略 SCPs

在撰写时， SCPs 您可以结合使用`Allow`和`Deny`语句来允许在组织中执行预期的操作和服务。`Deny`对账单是实施限制的有力方法，这些限制应该适用于组织中的更广泛部分，或者 OUs 因为当它们应用于根级或 OU 级别时，它们会影响其下的所有帐户。

例如，您可以在根级别为 阻止成员账户退出组织 实施使用 Deny 语句的策略，该策略将对组织中的所有账户有效。拒绝语句还支持条件元素，这有助于创建例外情况。

> **Tip**
>
> 您可以在 IAM 中使用服务上次访问的数据来更新您的 SCPs ，将访问权限限制为仅您需要 Amazon Web Services 服务 的内容。有关更多信息，请参阅《IAM 用户指南》中的查看 Organizations 的 Organizations 服务上次访问的数据。

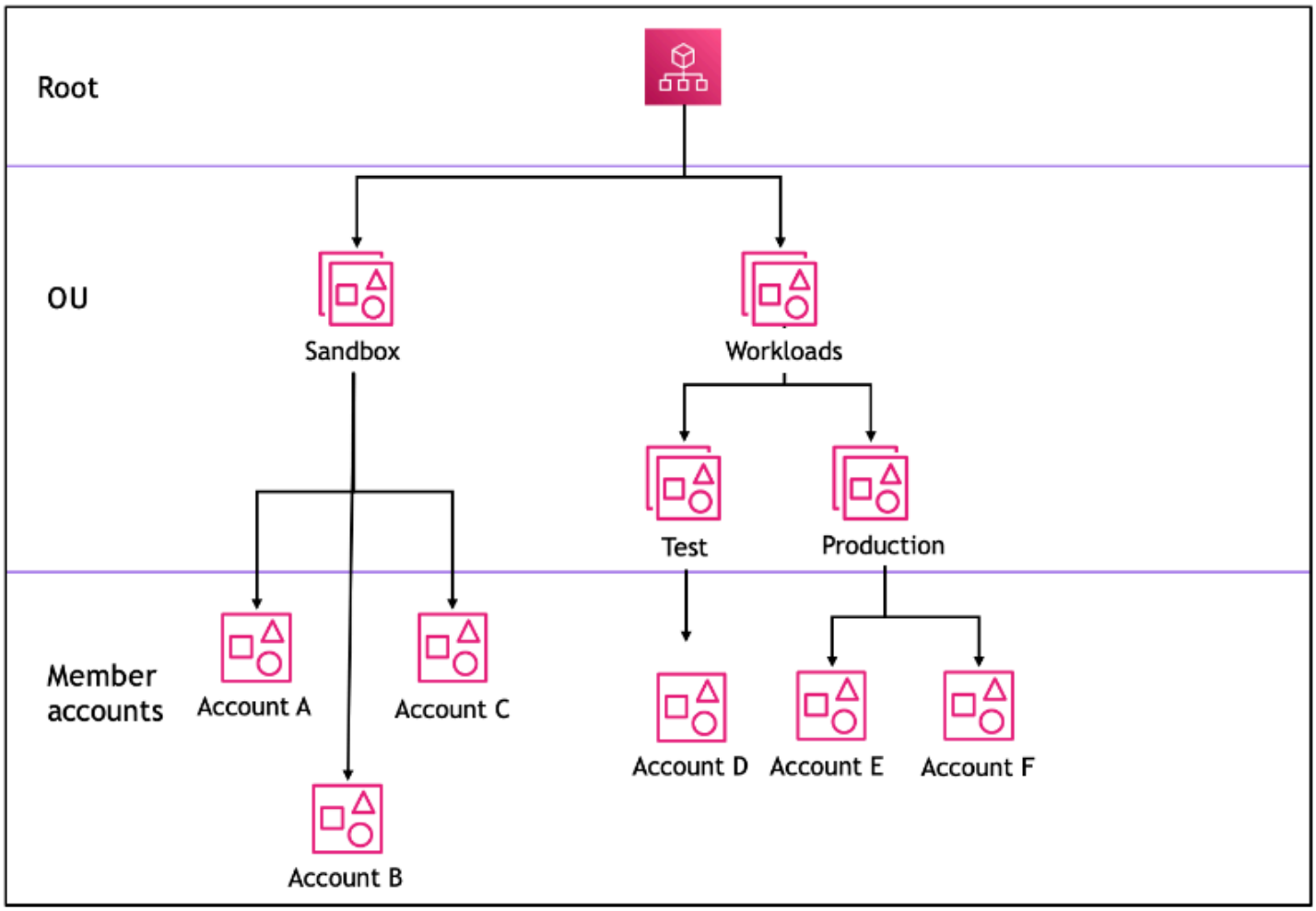
Amazon Organizations 创建后，将名为 F ull 的 Amazon 托管 SCP 附加`AWSAccess`到每个根、OU 和账户。此策略允许所有服务和操作。您可以将 F ull AWSAccess 替换为仅允许一组服务的策略，这样除非通过更新明确允许新 Amazon Web Services 服务 服务，否则不允许使用新服务 SCPs。例如，如果您的组织只想允许在您的环境中使用部分服务，则可以使用 `Allow` 语句来仅允许特定服务。

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

将两个语句组合在一起的策略可能与以下示例类似，它阻止成员账户离开组织并允许使用所需的 Amazon 服务。组织管理员可以分离完整AWSAccess策略，改为附加此策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

现在，考虑以下示例组织结构，以了解如何在组织中的不同 SCPs 级别上应用多个组织结构。



下表显示了沙盒 OU 中的有效策略。

场景	根处的 SCP	沙盒 OU 处的 SCP	账户 A 处的 SCP	账户 A 处生成的策略	账户 B 和账户 C 处生成的策略
1	完全 Amazon 访问权限	完全 Amazon 访问权限 + 拒绝 S3 访问权限	完全 Amazon 访问权限 + 拒绝 EC2 访问	没有 S3，没有 EC2 访问权限	没有 S3 访问
2	完全 Amazon 访问权限	允许 EC2 访问	允许 EC2 访问	允许 EC2 访问	允许 EC2 访问

场景	根处的 SCP	沙盒 OU 处的 SCP	账户 A 处的 SCP	账户 A 处生成的策略	账户 B 和账户 C 处生成的策略
3	拒绝 S3 访问	允许 S3 访问	完全 Amazon 访问权限	无服务访问	无服务访问

下表显示了工作负载 OU 中的有效策略。

场景	根处的 SCP	工作负载 OU 处的 SCP	测试 OU 处的 SCP	账户 D 处生成的策略	生产 OU、账户 E 和账户 F 处生成的策略
1	完全 Amazon 访问权限	完全 Amazon 访问权限	完全 Amazon 访问权限 + 拒绝 EC2 访问	无法 EC2 访问	完全 Amazon 访问权限
2	完全 Amazon 访问权限	完全 Amazon 访问权限	允许 EC2 访问	允许 EC2 访问	完全 Amazon 访问权限
3	拒绝 S3 访问	完全 Amazon 访问权限	允许 S3 访问	无服务访问	没有 S3 访问

SCP 语法

服务控制策略 (SCPs) 使用的语法与 (IAM) 权限策略和基于资源的策略 Amazon Identity and Access Management （ 如 Amazon S3 存储桶策略 ）使用的语法类似。有关 IAM 策略及其语法的更多信息，请参阅《IAM 用户指南》https://docs.amazonaws.cn/IAM/latest/UserGuide/access_policies.html中的 IAM 策略概述。

SCP 是一个纯文本文件，根据 JSON 的规则设置结构。它使用本主题中所述的元素。

> **Note**
>
> SCP 中的所有字符将计入其最大大小。本指南中的示例显示了带有额外空格以提高其可读性的 SCPs 格式化内容。但是，在您的策略大小接近最大大小时，可以删除任何空格（例如，引号之外的空格字符和换行符）来节省空间。

有关的一般信息 SCPs，请参见服务控制策略 (SCPs)。

元素摘要

下表汇总了您可以在中使用的策略元素 SCPs。某些策略元素仅 SCPs 在该拒绝操作中可用。支持的效果列列出了您可以与中的每个策略元素一起使用的效果类型 SCPs。

元素	用途	支持的效果
操作	指定 SCP 允许或拒绝的 Amazon 服务和操作。	`Allow, Deny`
效果	定义 SCP 语句是允许还是拒绝账户中的 IAM 用户和角色访问权限。	`Allow, Deny`
Statement	充当策略元素的容器。中可以有多个语句 SCPs。	`Allow, Deny`

元素	用途	支持的效果
Statement ID (Sid)	（可选）提供语句的友好名称。	Allow, Deny
版本	指定要用于处理策略的语言语法规则。	Allow, Deny
Condition	指定语句何时生效的条件。	Deny
NotAction	指定免受 SCP 限制的 Amazon 服务和操作。用来代替 Action 元素。	Deny
资源	指定 SCP 适用的 Amazon 资源。	Deny

以下各节提供了有关如何在中使用策略元素的更多信息和示例 SCPs。

主题

- Action 和 NotAction 元素
- Condition 元素

- Effect 元素
- Resource 元素
- Statement 元素
- Statement ID (Sid) 元素
- Version 元素
- 不支持的元素

Action 和 **NotAction** 元素

每个语句必须包含下列项目之一：

- 在允许和拒绝语句中，为 Action 元素。
- 仅在拒绝语句中（其中，Effect 元素的值为 Deny），为 Action 或 NotAction 语句。

Action或NotAction元素的值是一个字符串列表（JSON 数组），用于标识语句允许或拒绝的 Amazon 服务和操作。

所有字符串均包含服务简写（例如“s3”、“ec2”、“iam”或“organizations”），全小写，后跟冒号，然后是该服务的操作。操作和注释不区分大小写。通常，输入时每个单词都以大写字母开头，其余单词以小写字母开头。例如："s3:ListAllMyBuckets"。

您也可以在 SCP 中使用星号（*）或问号（？）等通配符：

- 使用星号（*）通配符以匹配名称中包含相同部分的多个操作。值 "s3:*" 表示 Amazon S3 服务中的所有操作。该值仅"ec2:Describe*"匹配以 “描述” 开头的 EC2 操作。
- 使用问号（？）通配符来匹配单个字符。

> **Note**
>
> 在 SCP 中，Action 或 NotAction 参数中的通配符（*）和（？）只能单独使用或放在字符串结尾处。它不能出现在字符串的开头或中间部分。因此，"servicename:action*"有效，但"servicename:*action"和在中"servicename:some*action"均无效 SCPs。

有关所有服务及其在两者 Amazon Organizations SCPs和 IAM 权限策略中支持的操作的列表，请参阅 IA M 用户指南中的Amazon 服务操作、资源和条件密钥。

有关更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素： NotAction操作和 I AM JSON 策略元素：。

`Action` 元素的示例

以下示例显示了一个 SCP，其语句允许账户管理员为账户中的 EC2实例委派描述、启动、停止和终止权限。这是另一个允许列表示例，这在未附加默认 `Allow *` 策略时非常有用，因此，在默认情况下，权限将被隐式拒绝。如果默认 `Allow *` 策略仍附加到以下策略所附加到的根、OU 或账户，则以下策略没有任何效果。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
    }
}
```

以下示例演示如何通过拒绝访问您不希望用于所附加账户中的服务。它假设默认值"`Allow *`" SCPs 仍然附加到 all OUs 和 root 上。此示例策略禁止关联账户中的账户管理员委派对 IAM、Amazon 和 Amazon EC2 RDS 服务的任何权限。只要没有其他已附加策略拒绝，就可以委派来自其他服务的任何操作。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
}
```

`NotAction` 元素的示例

以下示例说明如何使用`NotAction`元素将 Amazon 服务排除在策略的影响之外。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
         }
       }
     }
   ]
}
```

使用此声明，除非使用 IAM 操作 Amazon Web Services 区域，否则受影响的账户只能在指定范围内执行操作。

Condition 元素

您可以在 SCP 中的拒绝语句中指定 Condition 元素。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
```

```
                }
            }
        }
    ]
}
```

此 SCP 拒绝对 eu-central-1 和 eu-west-1 区域之外的任何操作的访问，但列出的服务中的操作除外。

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

Effect 元素

每个语句必须包含一个 Effect 元素。该值可以是 Allow 或 Deny。它会影响在同一个语句中列出的任意操作。

有关更多信息，请参阅《IAM 用户指南》https://docs.amazonaws.cn/IAM/latest/UserGuide/reference_policies_elements_effect.html中的 IAM JSON 策略元素：效果。

"Effect": "Allow"

以下示例演示带有一条语句的 SCP，该语句包含一个 Effect 元素，其值为 Allow，表示允许账户用户执行 Amazon S3 服务的操作。对于使用允许列表策略（已经分离了所有默认 FullAWSAccess 策略使得默认情况下默示拒绝权限）的组织，此示例非常有用。结果是语句允许任何附加账户的 Amazon S3 权限：

```
{
    "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "*"
    }
}
```

即使它使用与 IAM 权限策略相同的 Allow 值关键字，在 SCP 中它也不会实际授予用户执行任何操作的权限。相反，可以 SCPs 充当筛选器，为组织、组织单位 (OU) 或账户中的账户指定最大权限。在前面的示例中，即使账户中的用户已经附加了 AdministratorAccess 托管式策略，SCP 也会将受影响账户中的所有用户限制为只能执行 Amazon S3 操作。

"Effect": "Deny"

在Effect元素值为的语句中Deny，您还可以限制对特定资源的访问权限或定义何时生效 SCPs 的条件。

以下显示了有关如何在拒绝语句中使用条件密钥的示例。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

EC2 如果 Amazon EC2 实例未设置为，SCP 中的此声明设置了保护措施，防止受影响的账户（其中 SCP 附加到账户本身或包含该账户的组织根目录或 OU）启动亚马逊实例。t2.micro即使将允许此操作的 IAM 策略附加到账户，SCP 所创建的防护机制也会阻止它。

Resource 元素

在 Effect 元素具有值 Allow 的语句中，您只能在 SCP 的 Resource 元素中指定“*”。您不能指定单个资源 Amazon 资源名称 (ARNs)。

您也可以在 resource 参数中使用星号（*）或问号（？）等通配符：

- 使用星号（*）通配符以匹配名称中包含相同部分的多个操作。
- 使用问号（？）通配符来匹配单个字符。

在Effect元素值为的语句中Deny，您可以指定个人 ARNs，如以下示例所示。

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

```
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

此 SCP 阻止受影响账户中的 IAM 用户和角色对在组织的所有账户中创建的常见管理 IAM 角色进行更改。

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：资源。

`Statement` 元素

一个 SCP 可包含一个或多个 `Statement` 元素。一条策略中只能有一个 `Statement` 关键字，但其值可以是 JSON 语句数组 (使用 [ ] 字符括起)。

以下示例演示包含单个 `Effect`、`Action` 和 `Resource` 元素的语句。

```
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
```

以下示例包括作为一个 `Statement` 元素中的数组列表的两个语句。第一个语句允许所有操作，而第二个语句拒绝任何 EC2 操作。结果是，账户管理员可以委派除亚马逊弹性计算云 (Amazon EC2) 以外的任何权限。

```
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
```

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：语句。

Statement ID (**Sid**) 元素

Sid 是您针对策略语句提供的可选标识符。您可以为语句数组中的每个语句指定 Sid 值。以下示例 SCP 显示了一个示例 Sid 语句。

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
}
```

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：ID。

Version 元素

每个 SCP 必须包含 Version 元素，其值为 "2012-10-17"。此版本值与 IAM 权限策略的最新版本相同。

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

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：版本。

不支持的元素

中不支持以下元素 SCPs：

- `Principal`
- `NotPrincipal`
- `NotResource`

服务控制策略示例

本主题中显示的示例服务控制策略 (SCP) 仅供参考。

> **在使用这些示例之前**
>
> 在组织中使用这些示例 SCP 之前，请执行以下操作：
>
> - 仔细检查并根据您的独特需求定制 SCP。
> - 利用您使用的 Amazon Web Services 服务全面测试您环境中的 SCP。
>
> 本部分中的示例策略演示 SCP 的实施和使用。这些示例策略并不是要完全按照所示实施的官方Amazon建议或最佳实践。您有责任仔细测试任何基于拒绝的策略，以确定其是否适合解决环境的业务需求。基于拒绝的服务控制策略可能会无意中限制或阻止您使用 Amazon Web Services 服务，除非您在策略中添加了必要的例外情况。有关此类例外情况的示例，请参阅第一个示例，该示例从阻止访问不需要的Amazon Web Services 区域规则中将全球服务豁免。
> - 请记住，SCP 影响所附加到的每个账户中的每个用户和角色以及根用户。
> - 请记住，SCP 不影响服务相关角色。服务相关角色让其他 Amazon Web Services 服务能够与 Amazon Organizations 集成且不受 SCP 的限制。

> **Tip**
>
> 您可以使用 IAM 中的服务上次访问数据来更新您的 SCP，从而仅允许访问您需要的 Amazon Web Services 服务。有关更多信息，请参阅《IAM 用户指南》中的查看 Organizations 的 Organizations 服务上次访问的数据。

以下每个策略是拒绝列表策略战略的示例。附加拒绝列表策略时还必须附加在受影响账户中允许已批准的操作的其他策略。例如，默认 `FullAWSAccess` 策略允许在账户中使用所有服务。此策略默认附加到根、所有组织部门 (OU) 和所有账户。它实际上不授予权限；SCP 也不授予权限。相反，它使该账户中的管理员能够委派对这些操作的访问权限，方法是将标准 Amazon Identity and Access

Management（IAM）权限策略附加到账户中的用户、角色或组。然后，其中每个拒绝列表策略通过阻止访问指定服务或操作来覆盖任何策略。

示例

- 一般示例
  - 根据请求的Amazon Web Services 区域拒绝访问Amazon
  - 阻止 IAM 用户和角色进行某些更改
  - 阻止 IAM 用户和角色进行指定的更改，但指定管理员角色除外
  - 需要 MFA 才能执行 API 操作
  - 阻止根用户的服务访问
  - 阻止成员账户退出组织
- SCPs 的示例 聊天应用程序中的 Amazon Q 开发者版
  - 拒绝所有 IAM 操作
  - 拒绝来自指定 Slack 频道的 S3 存储桶放置请求
- Amazon CloudWatch 的示例 SCP
  - 阻止用户禁用 CloudWatch 或更改其配置
- Amazon Config 的示例 SCP
  - 阻止用户禁用 Amazon Config 或更改其规则
- 亚马逊弹性计算云 (Amazon EC2) 示例 SCPs
  - 要求 Amazon EC2 实例使用特定类型
  - 防止在没有的情况下启动 EC2 实例 IMDSv2
  - 防止禁用默认 Amazon EBS 加密
  - 防止创建和连接非 gp3 卷
- Amazon GuardDuty 的示例 SCP
  - 阻止用户禁用 GuardDuty 或修改其配置
- Amazon Resource Access Manager 的示例 SCP
  - 阻止外部共享
  - 允许特定账户仅共享指定的资源类型
  - 阻止与组织或组织部门（OU）共享
  - 仅允许与指定的 IAM 用户和角色共享
- Amazon 应用程序恢复控制器（ARC）示例 SCP

  - 阻止用户更新 ARC 路由控制状态
- 适用于 Amazon S3 的 SCP 示例
  - 防止上传 Amazon S3 未加密对象
- 标记资源的示例 SCP
  - 需要在指定的已创建资源上使用标签
  - 阻止标记被修改，除非由授权委托人修改
- Amazon Virtual Private Cloud（Amazon VPC）的示例 SCP
  - 阻止用户删除 Amazon VPC 流日志
  - 阻止还没有 Internet 访问权的任何 VPC 获取它

一般示例

根据请求的Amazon Web Services 区域拒绝访问Amazon

此 SCP 拒绝对特定区域之外的任何操作的访问。使用您要使用的Amazon Web Services 区域替换 `eu-central-1` 和 `eu-west-1`。它为已批准的全局服务中的操作提供了豁免。此示例还说明如何豁免由两个指定管理员角色中的任何一个发出的请求。

> **Note**
>
> 要将区域拒绝 SCP 与 Amazon Control Tower 结合使用，请参阅《Amazon Control Tower 控制参考指南》中的 Deny access to Amazon based on the requested Amazon Web Services 区域。

此策略使用 `Deny` 效果来拒绝访问不是针对两个批准区域（`eu-central-1` 和 `eu-west-1`）之一的操作的所有请求。通过 NotAction 元素，您可以列出其操作（或单个操作）不受此限制约束的服务。由于全球服务具有由 `us-east-1` 区域物理托管的终端节点，因此必须以这种方式豁免它们。借助以这种方式构建的 SCP，如果所请求的服务包含在 `NotAction` 元素中，则允许对 `us-east-1` 区域中的全局服务发出的请求。此示例策略拒绝对 `us-east-1` 区域中的服务的任何其他请求。

> **Note**
>
> 此示例可能未包含所有最新的全局 Amazon Web Services 服务或操作。将服务和操作列表替换为由组织中的账户使用的全球服务。

提示

您可以在 IAM 控制台中查看服务上次访问的数据，以确定您的组织使用哪些全球服务。IAM 用户、组或角色的详细信息页面上的 Access Advisor (访问顾问) 选项卡显示该实体已使用的Amazon服务，并按最近的访问顺序进行排序。

注意事项

- Amazon KMS 和 Amazon Certificate Manager 支持区域终端节点。但是，如果您想将它们与 Amazon CloudFront 等全球服务一起使用，则必须将它们包含在以下示例 SCP 的全球服务排除列表中。像 Amazon CloudFront 这样的全球服务通常需要访问位于同一区域的 Amazon KMS 和 ACM，对于全球服务来说，这是美国东部（弗吉尼亚北部）区域（`us-east-1`）。
- 默认情况下，Amazon STS 是全球服务，必须包含在全球服务排除列表中。不过，您可以启用 Amazon STS 来使用区域终端节点而不是单个全局终端节点。如果执行此操作，则可以从以下示例 SCP 中的全球服务豁免列表中删除 STS。有关更多信息，请参阅在Amazon Web Services 区域中管理 Amazon STS。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
```

```
            "cur:*",
            "directconnect:*",
            "ec2:DescribeRegions",
            "ec2:DescribeTransitGateways",
            "ec2:DescribeVpnGateways",
            "fms:*",
            "globalaccelerator:*",
            "health:*",
            "iam:*",
            "importexport:*",
            "kms:*",
            "mobileanalytics:*",
            "networkmanager:*",
            "organizations:*",
            "pricing:*",
            "route53:*",
            "route53domains:*",
            "route53-recovery-cluster:*",
            "route53-recovery-control-config:*",
            "route53-recovery-readiness:*",
            "s3:GetAccountPublic*",
            "s3:ListAllMyBuckets",
            "s3:ListMultiRegionAccessPoints",
            "s3:PutAccountPublic*",
            "shield:*",
            "sts:*",
            "support:*",
            "trustedadvisor:*",
            "waf-regional:*",
            "waf:*",
            "wafv2:*",
            "wellarchitected:*"
        ],
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "aws:RequestedRegion": [
                    "eu-central-1",
                    "eu-west-1"
                ]
            },
            "ArnNotLike": {
                "aws:PrincipalARN": [
                    "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
```

```
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

阻止 IAM 用户和角色进行某些更改

此 SCP 阻止 IAM 用户和角色对在组织的所有账户中创建的特定 IAM 角色进行更改。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}
```

阻止 IAM 用户和角色进行指定的更改，但指定管理员角色除外

此 SCP 基于前面的示例为管理员创建例外。它阻止受影响账户中的 IAM 用户和角色对在组织的所有账户中创建的常见管理 IAM 角色进行更改，但使用指定角色的管理员除外。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessWithException",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

需要 MFA 才能执行 API 操作

使用如下所示的 SCP，要求先启用多重身份验证（MFA），之后 IAM 用户和角色才能执行操作。在此示例中，操作是停止 Amazon EC2 实例。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
```

```
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

阻止根用户的服务访问

以下策略限制对成员账户中根用户指定操作的所有访问权限。如果要阻止您的账户以特定方式使用根凭证，请将您自己的操作添加到此策略中。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

阻止成员账户退出组织

以下策略阻止使用 LeaveOrganization API 操作，以便成员账户的管理员无法从组织中删除其账户。

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

```
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:LeaveOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

SCPs 的示例 聊天应用程序中的 Amazon Q 开发者版

此类别中的示例

- 拒绝所有 IAM 操作
- 拒绝来自指定 Slack 频道的 S3 存储桶放置请求

拒绝所有 IAM 操作

以下 SCP 拒绝通过所有 聊天应用程序中的 Amazon Q 开发者版 配置调用的所有 IAM 操作。

```
{
    "Effect": "Deny",
    "Action": "iam:*",
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:ChatbotSourceArn": "arn:aws:chatbot::*:*"
        }
    }
}
```

拒绝来自指定 Slack 频道的 S3 存储桶放置请求

以下策略会拒绝 S3 将所有来自某个 Slack 频道的请求放入指定存储桶。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExampleS3Deny",
```

```
            "Effect": "Deny",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringLike": {
                      "aws:ChatbotSourceArn": "arn:aws:chatbot::*:chat-configuration/
slack-channel/*"
                }
            }
        }
    ]
}
```

Amazon CloudWatch 的示例 SCP

此类别中的示例

- 阻止用户禁用 CloudWatch 或更改其配置

阻止用户禁用 CloudWatch 或更改其配置

低级 CloudWatch 操作员需要监控控制面板和警报。但不得删除或更改高级人员可能设置的任何控制面板或警报。此 SCP 阻止任何受影响账户中的用户或角色运行可删除或更改您的控制面板或警报的任何 CloudWatch 命令。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon Config 的示例 SCP

此类别中的示例

- 阻止用户禁用 Amazon Config 或更改其规则

阻止用户禁用 Amazon Config 或更改其规则

此 SCP 阻止任何受影响账户中的用户或角色运行可禁用 Amazon Config 或更改其规则或触发器的 Amazon Config 操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

亚马逊弹性计算云 (Amazon EC2) 示例 SCPs

此类别中的示例

- 要求 Amazon EC2 实例使用特定类型
- 防止在没有的情况下启动 EC2 实例 IMDSv2
- 防止禁用默认 Amazon EBS 加密
- 防止创建和连接非 gp3 卷

要求 Amazon EC2 实例使用特定类型

借助此 SCP，任何不使用 `t2.micro` 实例类型启动的实例都将被拒绝。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
    }
  ]
}
```

防止在没有的情况下启动 EC2 实例 IMDSv2

以下政策限制所有用户在没有的情况下 IMDSv2启动 EC2 实例。

```
[
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "StringNotEquals":{
            "ec2:MetadataHttpTokens":"required"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "NumericGreaterThan":{
            "ec2:MetadataHttpPutResponseHopLimit":"3"
         }
      }
   },
   {
```

```
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
]
```

以下政策限制所有用户在没有 EC2 实例的情况下启动实例，IMDSv2但允许特定 IAM 身份修改实例元数据选项。

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
```

```
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "ArnNotLike": {
        "aws:PrincipalARN": [
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
      }
    }
  }
]
```

防止禁用默认 Amazon EBS 加密

以下策略限制所有用户禁用默认 Amazon EBS 加密。

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

防止创建和连接非 gp3 卷

以下政策限制所有用户创建或附加任何非 gp3 卷类型的 Amazon EBS 卷。有关更多信息，请参阅 Amazon EBS 卷类型。

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

```
      "Sid": "DenyCreationAndAttachmentOfNonGP3Volumes",
      "Effect": "Deny",
      "Action": [
        "ec2:AttachVolume",
        "ec2:CreateVolume",
        "ec2:RunInstances"
      ],
      "Resource": "arn:aws:ec2:*:*:volume/*",
      "Condition": {
        "StringNotEquals": {
          "ec2:VolumeType": "gp3"
        }
      }
    }
  ]
}
```

这有助于在整个组织中强制执行标准化的卷配置。

> **不会阻止修改卷类型**
>
> 您不能使用限制将现有 gp3 卷修改为其他类型的 Amazon EBS 卷的操作。 SCPs例如，此 SCP 不会阻止您将现有的 gp3 卷修改为 gp2 卷。这是因为条件键`ec2:VolumeType`会在修改卷类型之前对其进行检查。

Amazon GuardDuty 的示例 SCP

此类别中的示例

- 阻止用户禁用 GuardDuty 或修改其配置

阻止用户禁用 GuardDuty 或修改其配置

此 SCP 阻止任何受影响账户中的用户或角色直接以命令形式或通过控制台禁用 GuardDuty 或更改其配置。它有效地允许对 GuardDuty 信息和资源进行只读访问。

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

```
            "Action": [
                "guardduty:AcceptInvitation",
                "guardduty:ArchiveFindings",
                "guardduty:CreateDetector",
                "guardduty:CreateFilter",
                "guardduty:CreateIPSet",
                "guardduty:CreateMembers",
                "guardduty:CreatePublishingDestination",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteDetector",
                "guardduty:DeleteFilter",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeletePublishingDestination",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
                "guardduty:UpdatePublishingDestination",
                "guardduty:UpdateThreatIntelSet"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon Resource Access Manager 的示例 SCP

此类别中的示例

- 阻止外部共享
- 允许特定账户仅共享指定的资源类型

- 阻止与组织或组织部门（OU）共享
- 仅允许与指定的 IAM 用户和角色共享

阻止外部共享

以下示例 SCP 阻止用户创建允许与不属于组织的 IAM 用户和角色共享的资源共享。

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

允许特定账户仅共享指定的资源类型

以下 SCP 允许账户 111111111111 和 222222222222 创建共享前缀列表的资源共享，并将前缀列表与现有资源共享相关联。

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

```
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEquals": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

阻止与组织或组织部门（OU）共享

以下 SCP 会阻止用户创建与组织或 OU 共享资源的资源共享。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

仅允许与指定的 IAM 用户和角色共享

以下示例 SCP 允许用户仅与组织 o-12345abcdef、组织部门 ou-98765fedcba 和账户 111111111111 共享资源。

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

Amazon 应用程序恢复控制器（ARC）示例 SCP

此类别中的示例

- 阻止用户更新 ARC 路由控制状态

阻止用户更新 ARC 路由控制状态

低级别 ARC 操作员需要监控控制面板并查看 ARC 信息。但是，操作员不得更新路由控制以将应用程序从一个 Amazon Web Services 区域 故障转移到另一个，而高级操作员可能允许进行此操作。此 SCP 会阻止任何受影响账户中的用户或角色运行可更新 ARC 路由控制的 ARC 操作。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAll",
            "Effect": "Deny",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

适用于 Amazon S3 的 SCP 示例

> **Note**
>
> Amazon Simple Storage Service（Amazon S3）会自动对每个新对象应用服务器端加密（SSE-S3），除非您指定了其他加密选项。有关更多信息，请参阅《Amazon S3 用户指南中的 Amazon S3 现在会自动加密所有新对象。

此类别中的示例

- 防止上传 Amazon S3 未加密对象

防止上传 Amazon S3 未加密对象

以下策略限制所有用户将未加密的对象上传到 S3 存储桶。

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
```

```
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

以下策略限制所有用户将未加密的对象上传到 S3 存储桶，并且对其存储桶中的对象上传强制执行指定的加密类型（AES256 或 aws:kms）。

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

标记资源的示例 SCP

此类别中的示例

- 需要在指定的已创建资源上使用标签
- 阻止标记被修改，除非由授权委托人修改

需要在指定的已创建资源上使用标签

如果请求不包含指定的标签，以下 SCP 将阻止受影响账户中的 IAM 用户和角色创建特定资源类型。

> **Important**
>
> 请务必使用您在环境中使用的服务测试基于拒绝的策略。以下示例是创建未标记的密钥或运行未标记的 Amazon EC2 实例的简单块，不包括任何例外。
> 以下示例策略与 Amazon CloudFormation 不兼容，因为该服务会创建一密钥，然后将其标记为两个单独的步骤。此示例策略有效地阻止 Amazon CloudFormation 将密钥作为堆栈的一部分创建，因为这样的操作会导致出现没有按要求被标记的密钥。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
```

```
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
  ]
}
```

有关在 Amazon Organizations SCP 和 IAM 权限策略中均支持的所有服务和操作列表，请参阅《IAM 用户指南》中的 Actions, Resources, and Condition Keys for Amazon Web Services 服务。

阻止标记被修改，除非由授权委托人修改

以下 SCP 显示策略如何仅允许授权委托人修改附加到资源的标签。这是将基于属性的访问控制（ABAC）作为Amazon云安全策略的一个重要部分。该策略允许调用者仅修改授权标签（在此示例中为 `access-project`）与附加到发出请求的用户或角色的相同授权标签完全匹配的资源上的标签。该策略还可以阻止授权用户更改用于授权的标签的值。调用委托人必须具有授权标签才能进行任何更改。

此策略仅阻止未经授权的用户更改标签。未被此策略阻止的授权用户必须仍具有单独的 IAM 策略，该策略明确授予相关标记 API 的 `Allow` 权限。例如，如果您的用户具有使用 `Allow */*` 的管理员策略（允许所有服务和所有操作），则组合将导致允许管理员用户仅能更改那些授权标签值与附加到用户委托人的授权标签值匹配的标签。这是因为该策略中的显式 `Deny` 将覆盖管理员策略中的显式 `Allow`。

> **Important**
>
> 这不是一个完整的策略解决方案，不应按如下所示使用。此示例仅用于演示 ABAC 策略的一部分，需要针对生产环境进行定制和测试。
> 有关完整策略及其工作原理的详细分析，请参阅使用 Amazon Organizations 中的服务控制策略保护用于授权的资源标签
> 请务必使用您在环境中使用的服务测试基于拒绝的策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
```

```
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "access-project"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

Amazon Virtual Private Cloud（Amazon VPC）的示例 SCP

此类别中的示例

- 阻止用户删除 Amazon VPC 流日志

- 阻止还没有 Internet 访问权的任何 VPC 获取它

阻止用户删除 Amazon VPC 流日志

此 SCP 阻止任何受影响账户中的用户或角色删除 Amazon Elastic Compute Cloud（Amazon EC2）流日志或者 CloudWatch 日志组或日志流。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
 }
```

阻止还没有 Internet 访问权的任何 VPC 获取它

此 SCP 阻止任何受影响账户中的用户或角色更改 Amazon EC2 Virtual Private Cloud（VPC）的配置以允许他们直接访问 Internet。它不会阻止现有直接访问或通过您的本地网络环境路由的任何访问。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

排查 Amazon Organizations 服务控制策略（SCP）问题

此处的信息有助您诊断和修复服务控制策略（SCP）中的常见错误。

Amazon Organizations 中的服务控制策略（SCP）与 IAM 策略类似并有共用的语法。此语法以 JavaScript 对象表示法 (JSON) 的规则开头。JSON 描述对象 以及组成对象的名称和值对。IAM 策略语法通过定义名称和值的含义，并让使用策略授予权限的 Amazon Web Services 服务可以理解这些名称和值来进行构建。

Amazon Organizations 使用部分 IAM 句法和语法。有关详细信息，请参阅SCP 语法。

常见策略错误

- 多个策略对象
- 多个 Statement 元素
- 策略文档超出最大大小

多个策略对象

一个 SCP 必须包含一个并且只能包含一个 JSON 对象。可通过在两旁放置 { } 括号来表示对象。虽然您可以通过在外部对中嵌入额外 { } 括号在 JSON 对象中嵌套其他对象，但是一个策略只能包含一个最外层的 { } 括号对。以下示例不正确，因为它在顶层包含两个对象 (以##标示)：

```
{
  "Version": "2012-10-17",
  "Statement":
  {
     "Effect":"Allow",
     "Action":"ec2:Describe*",
     "Resource":"*"
  }
}
{
  "Statement": {
     "Effect": "Deny",
     "Action": "s3:*",
     "Resource": "*"
```

```
  }
}
```

不过，您可以使用正确的策略语法来实现上面示例的意图。可以将两个数据块合并到单个 Statement 元素中，而不是包含两个完整的策略对象 (每个都有自己的 Statement 元素)。Statement 元素将两个对象组成的数组作为其值，如以下示例所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":" *"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

无法将此示例进一步压缩到带一个元素的 Statement 中，因为两个元素具有不同的作用。通常，您只能在每个语句中的 Effect 和 Resource 元素相同时组合语句。

多个 Statement 元素

此错误乍一看似乎是由上一部分中的错误变化而来的。但是，它在句法上是不同类型的错误。在以下示例中，顶层只有一个策略对象，由单个 { } 括号对表示。但是，该对象包含两个 Statement 元素。

一个 SCP 策略只能包含一个 Statement 元素，名称 (Statement) 在冒号左侧，它的值在冒号右侧。Statement 元素的值必须是对象，以 { } 括号表示，其中包含一个 Effect 元素、一个 Action 元素和一个 Resource 元素。以下示例不正确，因为它在策略对象中包含两个 Statement 元素：

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
```

```
  },
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

因为值对象可以是多个值对象组成的数组，所以您可以通过将两个 Statement 元素合并为一个对象数组元素来解决此问题，如以下示例所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
 ]
}
```

Statement 元素的值是对象数组。此示例中的数组包含两个对象，每个对象是 Statement 元素的正确值。数组中的每个对象之间用逗号隔开。

策略文档超出最大大小

SCP 文档的最大大小为 5,120 个字符。此最大大小包括所有字符，含空格。要减小 SCP 的大小，您可以删除引号之外的所有空格字符（如空格和换行符）。

> **Note**
>
> 如果您使用 Amazon Web Services Management Console保存策略，JSON 元素之间和引号之外的额外白色空格（如空格和换行符）不计算在内。如果您使用 SDK 操作或 Amazon CLI 保存策略，则策略将完全按照您提供的方式保存，并且不会自动删除字符。

资源控制策略 (RCPs)

资源控制策略 (RCPs) 是一种组织策略，可用于管理组织中的权限。 RCPs提供对组织中资源的最大可用权限的集中控制。 RCPs帮助您确保账户中的资源符合组织的访问控制准则。 RCPs仅在启用了所有功能的组织中可用。 RCPs如果您的组织仅启用了整合账单功能，则不可用。有关启用 RCPs 的说明，请参阅启用策略类型。

RCPs仅凭对组织中的资源授予权限是不够的。不授予任何权限RCP。对身份可以对组织中的资源执行的操作RCP定义权限护栏或设置限制。管理员仍必须将基于身份的策略附加到IAM用户或角色，或者将基于资源的策略附加到您账户中的资源才能实际授予权限。有关更多信息，请参阅《用户指南》中的基于身份的策略和基于资源的策略。IAM

有效权限是RCPs和服务控制策略 (SCPs) 所允许的权限与基于身份和基于资源的策略所允许的权限之间的逻辑交集。

> **⚠ RCPs不要影响管理账户中的资源**
>
> RCPs不要影响管理账户中的资源。它们仅影响组织内成员账户中的资源。这也意味着这RCPs适用于被指定为授权管理员的成员账户。

本页面上的主题

Amazon Web Services 服务 该支持清单 RCPs

RCPs适用于以下资源 Amazon Web Services 服务：

- Amazon S3

- Amazon Security Token Service
- Amazon Key Management Service
- Amazon SQS
- Amazon Secrets Manager

的测试效果 RCPs

Amazon 强烈建议您在未彻底测试该政策对您账户中资源的影响之前，不要将其附加RCPs到组织的根目录。首先，您可以附加RCPs到单个测试账户，将它们向上移动到层次结构的OUs下层，然后根据需要在组织结构中向上移动。确定影响的一种方法是查看 Amazon CloudTrail 日志中是否存在拒绝访问的错误。

最大大小为 RCPs

你中的所有字符都按其最大大小进行RCP计数。本指南中的示例显示了带有额外空格以提高其可读性的RCPs格式化内容。但是，在您的策略大小接近最大大小时，可以删除任何空格（例如，引号之外的空格字符和换行符）来节省空间。

> **Tip**
>
> 使用可视化编辑器来构建你的RCP. 它会自动删除额外的空格。

隶RCPs属于组织中的不同级别

您可以RCPs直接关联到个人账户或组织根帐户。OUs有关RCPs工作原理的详细说明，请参阅RCP评估。

RCP对权限的影响

RCPs是一种 Amazon Identity and Access Management (IAM) 策略。它们与基于资源的政策关系最为密切。但是，RCP从不授予权限。取而代之RCPs的是访问控制，用于指定组织中资源的最大可用权限。有关更多信息，请参阅《IAM 用户指南》中的策略评估逻辑。

- RCPs适用于其子集的资源 Amazon Web Services 服务。有关更多信息，请参阅 Amazon Web Services 服务 该支持清单 RCPs。
- RCPs仅影响由关联的组织中的账户管理的资源RCPs。它们不会影响来自组织外部账户的资源。例如，假设组织中的账户 A 拥有的 Amazon S3 存储桶。存储桶策略（基于资源的策略）向来自组织外

部账户 B 的用户授予访问权限。账户 A 已RCP附加。这RCP适用于账户 A 中的 S3 存储桶，即使账户 B 中的用户访问也是如此。但是，当账户 A 中的用户访问时，这RCP不适用于账户 B 中的资源。

- RCP限制成员账户中资源的权限。账户中的任何资源都只能拥有该账户上每个家长所允许的权限。如果某个权限在账户以上的任何级别被阻止，则受影响账户中的资源没有该权限，即使资源所有者附加了允许任何用户完全访问权限的基于资源的策略。
- RCPs适用于作为操作请求的一部分获得授权的资源。这些资源可以在《服务授权参考》的 “操作” 表的 “资源类型” 列中找到。如果在 “资源类型” 列中未指定任何资源，则应用调用主账户RCPs的资源。例如，对对象资源`s3:GetObject`进行授权。每当`GetObject`提出请求时，都RCP将适用一个适用条款来确定提出请求的委托人是否可以调用该`GetObject`操作。适用的RCPRCP是指已附加到帐户、组织单位 (OU) 或拥有所访问资源的组织根目录的。
- RCPs仅影响组织中成员账户中的资源。它们对管理账户中的资源没有影响。这也意味着这RCPs适用于被指定为授权管理员的成员账户。有关更多信息，请参阅 管理账户的最佳实践。
- 当委托人请求访问已关联的账户RCP（带有适用的资源RCP）中的资源时，策略评估逻辑中将包含该资源，以确定是允许还是拒绝委托人访问。RCP
- RCPs无论委托人是否属于同一个组织RCP，都会影响委托人尝试使用适用的成员账户访问资源的有效权限。这包括根用户。唯一的例外情况是委托人是服务相关角色，因为RCPs不适用于服务相关角色发出的呼叫。服务相关角色可以代表您执行必要的操作，并且不受RCPs限制。 Amazon Web Services 服务
- 用户和角色仍必须通过适当的IAM权限策略获得权限，包括基于身份的策略和基于资源的策略。没有任何IAM权限策略的用户或角色没有访问权限，即使适用的权限策略RCP允许所有服务、所有操作和所有资源。

不受限制的资源和实体 RCPs

您不能使用RCPs来限制以下内容：

- 对管理账户中的资源的任何操作。
- RCPs不影响任何服务相关角色的有效权限。服务相关角色是一种独特的IAM角色类型，直接链接到 Amazon 服务，包括该服务代表您调用其他 Amazon 服务所需的所有权限。服务相关角色的权限不能受限制。RCPs RCPs也不会影响 Amazon 服务担任服务相关角色的能力；也就是说，服务相关角色的信任策略也不会受到影响。RCPs
- RCPs不适用Amazon 托管式密钥 于 Amazon Key Management Service。 Amazon 托管式密钥 由一个人代表您创建、管理和使用 Amazon Web Services 服务。您无法更改或管理他们的权限。
- RCPs不要影响以下权限：

服务	API	未经授权的资源 RCPs
Amazon Key Management Service	`kms:RetireGrant`	RCPs不要影响`kms:RetireGrant` 权限。有关如何确定权限的更多信息，请参阅《Amazon KMS 开发者指南》中的停用和撤销授权。`kms:RetireGrant`

RCP评估

> **Note**
>
> 本节中的信息不适用于管理策略类型，包括备份策略、标签策略、聊天机器人策略或 AI 服务选择退出策略。有关更多信息，请参阅 了解管理策略继承。

由于您可以在中附加不同级别的多个资源控制策略 (RCPs) Amazon Organizations，因此了解评估RCPs方式可以帮助您编写RCPs得出正确结果的文章。

使用策略 RCPs

该`RCPFullAWSAccess`策略是一个 Amazon 托管策略。启用资源控制策略后，它会自动附加到组织根目录、每个 OU 和组织中的每个账户 (RCPs)。您无法分离此政策。此默认设置RCP允许所有委托人和操作访问权限通过RCP评估，这意味着在您开始创建和附加之前RCPs，您的所有现有IAM权限将继续按原样运行。此 Amazon 托管策略不授予访问权限。

您可以使用`Deny`语句来阻止对组织中资源的访问。要拒绝特定账户中资源的权限，RCP从根目录到账户直接路径中的每个 OU（包括目标账户本身）都可以拒绝该权限。

`Deny`声明是实施限制的有力方法，对于组织的更广泛部分来说，这些限制应该是正确的。例如，您可以附加一个策略来帮助防止组织外部的身份访问您的资源根级别，该策略将对组织中的所有账户都生效。 Amazon 强烈建议您在未彻底测试该政策对您账户中资源的影响之前，不要将其附加RCPs到组织的根目录。有关更多信息，请参阅 的测试效果 RCPs。

在图 1 中，生产OU中有一个RCP附件，其中为给定服务指定了明确的Deny语句。因此，账户 A 和账户 B 都将被拒绝访问该服务，因为将针对组织下的所有账户OUs和成员账户评估附加到组织中任何级别的拒绝策略。

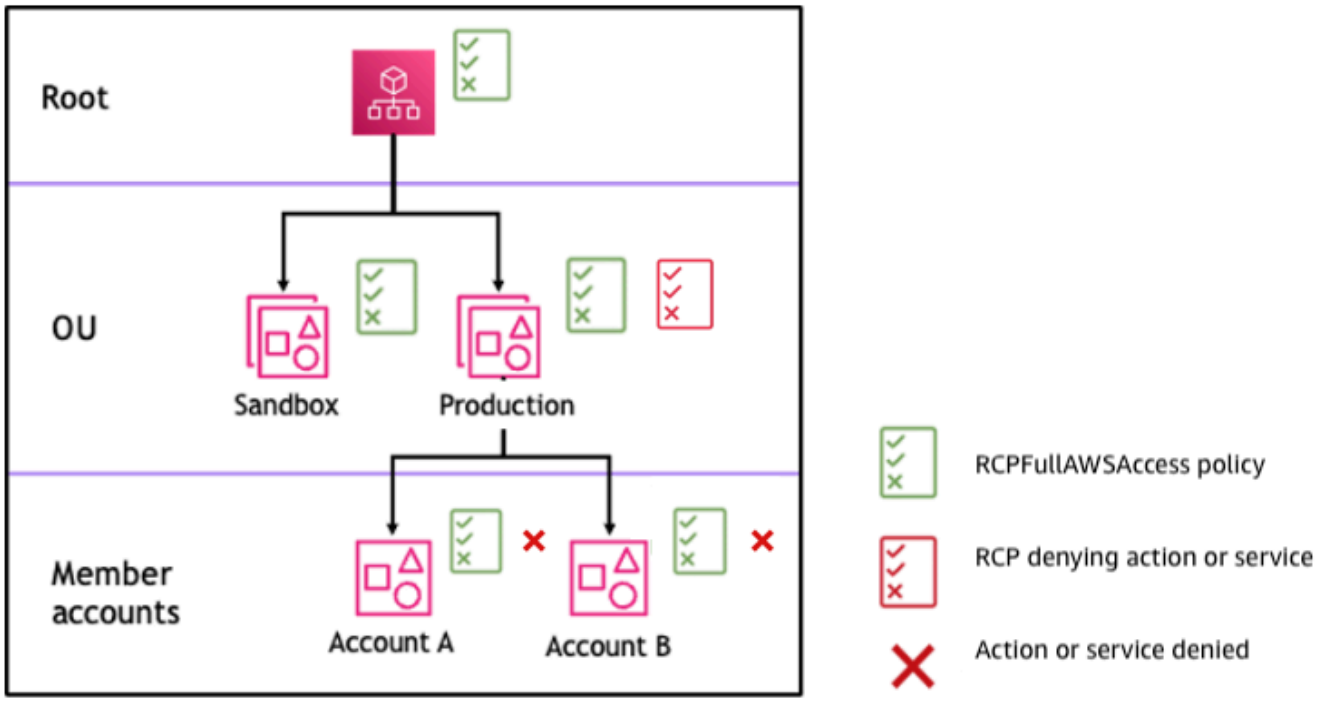


图 1：示例组织结构及其对账户 A 和账户 B 的影响 *Deny*

RCP 语法

资源控制策略 (RCPs) 使用的语法与基于资源的策略使用的语法类似。有关 IAM 策略及其语法的更多信息，请参阅《IAM 用户指南》https://docs.amazonaws.cn/IAM/latest/UserGuide/access_policies.html中的 IAM 策略概述。

RCP 是根据 JSON 的规则进行结构化的。它使用本主题中所述的元素。

> **Note**
>
> 你的 RCP 中的所有角色都将计入其最大大小。本指南中的示例显示了带有额外空格以提高其可读性的 RCPs 格式化内容。但是，在您的策略大小接近最大大小时，可以删除任何空格（例如，引号之外的空格字符和换行符）来节省空间。

有关的一般信息 RCPs，请参见资源控制策略 (RCPs)。

元素摘要

下表汇总了您可以在中使用的策略元素 RCPs。支持的效果列列出了您可以与中的每个策略元素一起使用的效果类型 RCPs。

> **Note**
>
> 的效果**`Allow`**仅支持**`RCPFullAWSAccess`**策略的效果
> 的效果`Allow`仅支持`RCPFullAWSAccess`策略的效果。启用资源控制策略后，此策略将自动附加到组织根目录、每个 OU 和组织中的每个账户 (RCPs)。您无法分离此政策。此默认 RCP 允许所有委托人和操作访问权限通过 RCP 评估，这意味着在您开始创建和附加之前 RCPs，您的所有现有 IAM 权限将继续按原样运行。这不授予访问权限。

元素	用途
版本	指定要用于处理策略的语言语法规则。
Statement	充当策略元素的容器。中可以有多个语句 RCPs。
Statement ID (Sid)	（可选）提供语句的友好名称。
效果	定义 RCP 语句是否拒绝访问账户中的资源。
主体	指定允许或拒绝访问账户中资源的委托人。
操作	指定 RCP 允许或拒绝的 Amazon 服务和操作。

元素	用途
资源	指定 RCP 适用的 Amazon 资源。
NotResource	指定免受 RCP 限制的 Amazon 资源。用来代替 Resource 元素。
Condition	指定语句何时生效的条件。

主题

- Version 元素
- Statement 元素
- Statement ID (Sid) 元素
- Effect 元素
- Principal 元素
- Action 元素
- Resource 和 NotResource 元素
- Condition 元素
- 不支持的元素

Version 元素

每个 RCP 都必须包含一个值"2012-10-17"为的Version元素。此版本值与 IAM 权限策略的最新版本相同。

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

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：版本。

`Statement` 元素

RCP 由一个或多个`Statement`元素组成。一条策略中只能有一个 `Statement` 关键字，但其值可以是 JSON 语句数组 (使用 [ ] 字符括起)。

以下示例显示了由单个`Effect`、`PrincipalAction`、和`Resource`元素组成的单个语句。

```
 {
    "Statement": {
        "Effect": "Deny",
        "Principal": "*",
        "Action": "*",
        "Resource": "*"
    }
}
```

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：语句。

Statement ID (`Sid`) 元素

`Sid` 是您针对策略语句提供的可选标识符。您可以为语句数组中的每个语句指定 `Sid` 值。以下示例 RCP 显示了一个示例`Sid`语句。

```
{
    "Statement": {
        "Sid": "DenyAllActions",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "*",
        "Resource": "*"
    }
}
```

有关更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素：Sid。

`Effect` 元素

每个语句必须包含一个 `Effect` 元素。使用`Effect`元素`Deny`中的值，您可以限制对特定资源的访问权限或定义何时生效 RCPs 的条件。为 RCPs 此，您创建的值必须是`Deny`。有关更多信息，请参阅 IAM 用户指南中的RCP评估和 IAM JSON 策略元素：影响。

`Principal` 元素

每条语句都必须包含`Principal`元素。只能在 RCP 的`Principal`元素中指定 “*”。使用`Conditions`元素来限制特定的委托人。

有关更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素：委托人。

`Action` 元素

每条语句都必须包含`Action`元素。

`Action`元素的值是一个字符串或字符串列表（JSON 数组），用于标识语句允许或拒绝的 Amazon 服务和操作。

每个字符串都由服务的缩写（例如 “s3”、“sqs” 或 “sts”）组成，全部为小写，后跟一个冒号，然后是来自该服务的操作。通常，输入时每个单词都以大写字母开头，其余单词以小写字母开头。例如：`"s3:ListAllMyBuckets"`。

也可以使用通配符，例如星号 (*) 或问号 (?) 在 RCP 中：

- 使用星号（*）通配符以匹配名称中包含相同部分的多个操作。值 `"s3:*"` 表示 Amazon S3 服务中的所有操作。该值仅`"sts:Get*"`匹配以 “Get” 开头的 Amazon STS 操作。
- 使用问号（？）通配符来匹配单个字符。

> **Note**
>
> 通配符 (*) 和问号 (?) 可以在动作名称中的任何地方使用
> 与不同 SCPs，您可以使用通配符，例如星号 (*) 或问号 (?) 动作名称中的任意位置。

有关支持的服务的列表 RCPs，请参阅Amazon Web Services 服务 该支持清单 RCPs。有关 Amazon Web Services 服务 支持的操作列表，请参阅《服务授权参考》中的 “Amazon 服务操作、资源和条件密钥”。

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：操作。

`Resource` 和 `NotResource` 元素

每个语句都必须包含`Resource`或`NotResource`元素。

您可以使用通配符，例如星号 (*) 或问号 (?) 在资源元素中：

- 使用星号（*）通配符以匹配名称中包含相同部分的多个操作。
- 使用问号（？）通配符来匹配单个字符。

有关更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素： NotResource资源和参阅 I AM JSON 策略元素：。

Condition 元素

您可以在 RCP 的拒绝语句中指定一个Condition元素。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition:": {
                "BoolIfExists": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

除非请求是通过安全传输进行的（请求是通过 TLS 发送的），否则此 RCP 拒绝访问 Amazon S3 的操作和资源。

有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

不支持的元素

中不支持以下元素 RCPs：

- NotPrincipal
- NotAction

资源控制策略示例

本主题中显示的资源控制策略示例 (RCPs) 仅供参考。有关数据边界的示例，请参阅中的数据外围策略示例。 GitHub

> **在使用这些示例之前**
>
> 在组织 RCPs 中使用这些示例之前，请执行以下操作：
>
> - 请仔细查看并根据您的独特要求 RCPs 进行自定义。
> - 使用您使用的 Amazon 服务 RCPs 在您的环境中彻底测试。
>
> 本节中的示例策略演示了的实现和使用 RCPs。这些示例策略并不是要完全按照所示实施的官方 Amazon 建议或最佳实践。您有责任仔细测试任何策略是否适合满足您环境的业务需求。除非您在策略中添加必要的例外情况，否则基于拒绝的资源控制策略可能会无意中限制或阻止您对 Amazon 服务的使用。

一般示例

主题

- RCPFullAWSAccess
- 跨服务混淆了副手保护
- 限制仅通过 HTTPS 连接访问您的资源
- 一致的 Amazon S3 存储桶策略控制

RCPFullAWSAccess

以下策略是 Amazon 托管策略，当您启用资源控制策略（RCPs）时，它会自动附加到组织根目录、每个 OU 和组织中的每个账户。您无法分离此政策。此默认 RCP 允许所有委托人和操作访问您的资源，这意味着在您开始创建和附加之前 RCPs，您的所有现有 IAM 权限将继续按原样运行。您无需测试此策略的效果，因为它允许您的资源继续使用现有的授权行为。

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

```
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

跨服务混淆了副手保护

有些 Amazon Web Services 服务 （呼叫服务）使用其 Amazon Web Services 服务 主体从其他 Amazon Web Services 服务 （称为服务）访问 Amazon 资源。当一个不打算访问 Amazon 资源的行为者试图利用委托人的信任与他们 Amazon Web Services 服务 本来不打算访问的资源进行交互时，这被称为跨服务混乱的副手问题。有关更多信息，请参阅 IAM 用户指南中的混乱副手问题

以下政策要求访问您的资源的 Amazon Web Services 服务 委托人只能代表贵组织发出的请求访问您的资源。此策略仅对`aws:SourceAccount`存在的请求应用控制，这样不需要使用的服务集成就`aws:SourceAccount`不会受到影响。如果请求上下文中存在，`aws:SourceAccount`则`Null`条件的计算结果将为`true`，从而强制执行`aws:SourceOrgID`密钥。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RCPEnforceConfusedDeputyProtection",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:*",
                "sqs:*",
                "secretsmanager:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceOrgID": "my-org-id"
                },
                "Bool": {
                    "aws:PrincipalIsAWSService": "true"
                },
                "Null": {
                    "aws:SourceAccount": "false"
                }
```

```
            }
        }
    ]
}
```

限制仅通过 HTTPS 连接访问您的资源

以下策略要求只有通过 HTTPS (TLS) 的加密连接才能访问您的资源。这可以帮助您防止潜在的攻击者操纵网络流量。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceSecureTransport",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "sts:*",
                "s3:*",
                "sqs:*",
                "secretsmanager:*",
                "kms:*"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

一致的 Amazon S3 存储桶策略控制

以下 RCP 包含多个语句，用于对组织中的 Amazon S3 存储桶实施一致的访问控制。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceS3TlsVersion",
```

```
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "s3:TlsVersion": [
                        "1.2"
                    ]
                }
            }
        },
        {
            "Sid": "EnforceKMSEncryption",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
                }
            }
        }
    ]
}
```

- 语句 ID `EnforceS3TlsVersion` — 要求最低的 TLS 版本为 1.2 才能访问 S3 存储桶。
- 语句 ID `EnforceKMSEncryption`-要求使用 KMS 密钥对对象进行服务器端加密。

中的管理政策 Amazon Organizations

管理策略使您能够集中配置 Amazon Web Services 服务 和管理其功能。这些策略如何影响继承它们的 OUs 和账户取决于您应用的管理策略的类型 Amazon Organizations。查看此部分中的主题，了解有关管理策略的相关术语和概念。

主题

- 的管理策略的先决条件和权限 Amazon Organizations
- 了解管理策略继承
- 查看有效管理策略

- 声明式策略
- 备份策略
- 标签策略
- 聊天机器人策略
- AI 服务选择退出策略

的管理策略的先决条件和权限 Amazon Organizations

本页介绍了 Amazon Organizations管理策略的先决条件和所需权限。

主题

管理策略的先决条件

要使用组织的管理策略，需要满足以下条件：

- 您的组织必须已启用所有功能。
- 您必须登录到组织的管理账户或成为委派管理员。
- 您的 Amazon Identity and Access Management (IAM) 用户或角色必须拥有下一节中列出的权限。

管理策略的权限

以下示例 IAM 策略提供了在组织中使用管理策略的各个方面所需的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageBackupPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
```

```
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

有关 IAM 策略与权限的更多一般信息，请参阅 IAM 用户指南。

了解管理策略继承

> **Important**
>
> 本节中的信息不适用于授权策略：服务控制策略 (SCPs) 和资源控制策略 (RCPs)。有关 Amazon Organizations 层次结构中的 RCPs 工作方式 SCPs 和运作方式的更多信息，请参阅SCP 评估和RCP评估。

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

- 当您将管理策略附加到组织根目录时，组织中的所有 OUs 和账户都将继承该策略。
- 当您将某个管理策略附加到特定 OU 时，直接位于该 OU 下的账户或任何子 OU 都将继承该策略。

- 当您将某个管理策略附加到特定账户时，它仅影响该账户。

由于您可以将管理策略附加到组织中的多个级别，因此账户可以继承多个策略。

本主题介绍如何将父策略和子策略转换为账户的有效策略。

主题

继承术语

本主题在讨论管理策略继承时将使用以下术语。

策略继承

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

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

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

父策略

附加到组织树中的策略，其位置高于附加到树中较低位置实体的策略。

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

子策略

在组织树中附加的级别低于父策略的策略。

有效策略

最后，指定应用于账户的规则的单个策略文档。有效策略是账户继承的任何策略以及直接附加到账户的任何策略的聚合。有关更多信息，请参阅 查看有效管理策略。

继承运算符

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

管理策略类型的策略语法和继承

策略究竟如何影响 OUs 和继承它们的帐户取决于您选择的管理策略的类型。管理策略类型包括：

- 声明式策略
- 备份策略
- 标签策略
- 聊天机器人策略
- AI 服务选择退出策略

管理策略类型的语法包括 继承运算符，这使您可以精细地指定应用父策略中的哪些元素，以及子策略和账户继承时可以覆盖或修改哪些元素。 OUs

有效的策略是从组织根目录继承的一组规则， OUs 以及直接关联到账户的规则。有效策略指定适用于账户的最终规则集。您可以查看账户的有效策略，其中包含所应用策略中所有继承运算符的效果。有关更多信息，请参阅 查看有效管理策略。

继承运算符

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

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

值设置运算符

您可以使用以下值设置运算符来控制策略与其父策略交互的方式：

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

子控制运算符

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

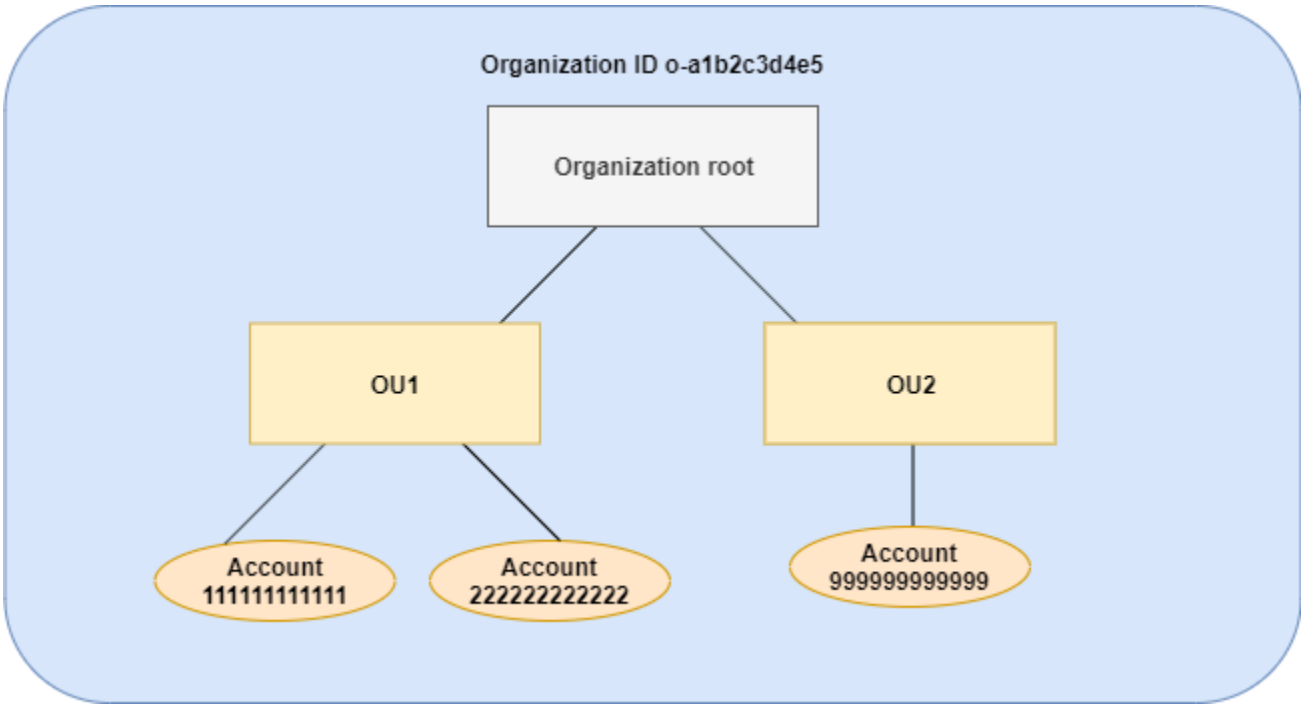
- `"@@operators_allowed_for_child_policies": ["@@all"]` — 儿童 OUs 和账户可以在政策中使用任何运算符。默认情况下，子策略中允许使用所有运算符。
- `"@@operators_allowed_for_child_policies": ["@@assign", "@@append", "@@remove"]` — 子账号 OUs 和账户只能使用子政策中的指定运算符。您可以在此子控制运算符中指定一个或多个值设置运算符。
- `"@@operators_allowed_for_child_policies": ["@@none"]` — 儿童 OUs 和账户不能在策略中使用运算符。可以使用此运算符有效锁定在父策略中定义的值，以使子策略无法添加、追加或删除这些值。

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

继承示例

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

这些示例假定您具有下图所示的组织结构。



示例

- 示例 1：允许子策略仅 覆盖标签值
- 示例 2：将新值附加到继承的标签
- 示例 3：从继承标签中删除值
- 示例 4：限制对子策略的更改
- 示例 5：与子控制运算符的冲突
- 示例 6：在相同层次结构级别附加值的冲突

示例 1：允许子策略仅 覆盖标签值

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

策略 A – 组织根标签策略

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

假设您希望用户 OU1 对密钥使用不同的标签值，并且您想对特定资源类型强制执行标签策略。由于策略 A 没有指定允许使用哪些子控制运算符，因此允许所有运算符。您可以使用@@assign运算符并创建如下所示的标签策略以附加到 OU1。

策略 B — OU1 标签策略

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

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

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

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

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

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

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Sandbox"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

示例 2：将新值附加到继承的标签

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

与示例 1 类似，此示例从用于组织根标签策略的策略 A 开始。

策略 A – 组织根标签策略

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

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

策略 C — 用于附加值的 OU2 标签策略

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

```
}
```

当策略 A 和策略 C 合并形成账户的有效标签策略时，将策略 C 附加到会产生以下影响： OU2

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

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

适用于账户 999999999999 的有效标签策略

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

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

示例 3：从继承标签中删除值

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

与其他示例类似，此示例从用于组织根标签策略的策略 A 开始。

策略 A – 组织根标签策略

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

对于此示例，将策略 D 附加到账户 999999999999。

策略 D – 账户 999999999999 标签策略，用于删除值

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

```
                    ]
                }
            }
        }
    }
}
```

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

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

适用于账户 999999999999 的新有效标签策略

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

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

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

示例 4：限制对子策略的更改

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

此示例从新的组织根标签策略开始，并假定标签策略尚未附加到组织实体。

策略 E – 用于限制子策略中的更改的组织根标签策略

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

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

假定您随后将以下策略 F 附加到 OU。

策略 F – OU 标签策略

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

合并策略 E 和策略 F 会对 OU 的账户产生以下效果：

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

OU 中账户的有效策略

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

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

示例 5：与子控制运算符的冲突

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

假定策略 G 和策略 H 附加到组织根。

策略 G – 组织根标签策略 1

```
{
```

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

策略 H – 组织根标签策略 2

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

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

示例 6：在相同层次结构级别附加值的冲突

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

假定策略 J 第一个附加到组织根，然后将策略 K 附加到组织根。

策略 J – 附加到组织根的第一个标签策略

```
{
    "tags": {
        "project": {
```

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

策略 K – 附加到组织根的第二个标签策略

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

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

策略 JK – 账户的有效标签策略

账户的有效策略如下。

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

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

```
        }
    }
}
```

查看有效管理策略

确定组织中任何账户的有效管理策略。

什么是有效管理策略？

有效策略用于指定对于某个管理策略类型，适用于 Amazon Web Services 账户的最终规则。这是账户所继承的管理策略，加上直接附加到该账户的任何该管理策略类型的策略的聚合。将管理策略附加到组织根时，该策略将适用于组织中的所有账户。将管理策略附加到组织单位（OU）时，该策略将适用于属于该 OU 的所有账户和 OU。将管理策略直接附加到某个账户时，则将仅适用于该具体 Amazon Web Services 账户。

有关如何将策略组合到最终有效策略中的信息，请参阅[了解管理策略继承](#)。

备份策略示例

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

标签策略示例

附加到组织根的标签策略可以定义具有四个合规值的 `CostCenter` 标签。附加到账户的单独标签策略可能会将 `CostCenter` 限制为四个合规值中的两个。这些标签策略的组合组成了有效标签策略。结果是，在组织根标签策略中定义的四个合规标签值中，只有两个符合该账户的要求。

聊天机器人策略示例

聊天应用程序中的 Amazon Q 开发者版 将根据有效的聊天机器人策略重新评估任何先前创建的 聊天应用程序中的 Amazon Q 开发者版 配置，如果这些配置与有效策略中允许的设置和护栏一致，则会拒绝任何先前允许的操作。成员账户的有效策略定义了允许的设置和护栏。例如，假设将某个会拒绝访问公有 Slack 频道的聊天机器人策略应用于成员账户，则该成员账户中公有 Slack 频道的现有 聊天应用程序中的 Amazon Q 开发者版 配置将被禁用。聊天机器人不会发送通知，频道成员也无法在被阻止的频

道中运行任何任务。聊天应用程序中的 Amazon Q 开发者版 控制台会将受影响的频道标记为已禁用，并在其旁边显示相应的错误消息。

AI 服务选择退出策略示例

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

如何查看有效管理策略

您可以从 Amazon Web Services Management Console、Amazon API 或 Amazon Command Line Interface 查看账户的管理策略类型的有效策略。

> **最小权限**
>
> 要查看账户的管理策略类型的有效策略，您必须要有运行以下操作的权限：
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要

Amazon Web Services Management Console

查看账户的管理策略类型的有效策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Amazon Web Services 账户页面上，选择要查看其有效策略的账户的名称。您可能需要展开 OU（选择 ）以查找所需的账户。
3. 在策略选项卡上，选择要查看其有效策略的管理策略类型。
4. 选择查看此 Amazon Web Services 账户的有效策略。

   控制台显示应用于指定账户的有效策略。

> **Note**
>
> 您无法复制和粘贴有效策略，并在不进行重大更改的情况下将其用作其他策略的 JSON。策略文档必须包含继承运算符，用来指定如何将每个设置合并到最终的有效策略中。

Amazon CLI & Amazon SDKs

查看账户的管理策略类型的有效策略

您可以使用以下方法之一查看有效策略：

- Amazon CLI：describe-effective-policy

  以下示例显示了账户的有效 AI 服务选择退出策略。

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

- Amazon SDK：DescribeEffectivePolicy

声明式策略

声明式策略允许您在整个组织中大规模地集中声明和强制执行所需的配置。 Amazon Web Services 服务 连接后，当服务添加新功能或时，配置将始终保持不变 APIs。使用声明性策略来防止不合规的操作。例如，您可以屏蔽整个组织中对 Amazon VPC 资源的公共互联网访问。

使用声明式策略的主要好处是：

- 易用性：您可以通过 Amazon Organizations 和 Amazon Control Tower 控制台中的几个选项或使用 Amazon CLI & 使用几个命令来强制执行基本配置 Amazon SDKs。 Amazon Web Services 服务
- 设置一次就算了：的基准配置始终保持 Amazon Web Services 服务 不变，即使服务引入了新功能或 APIs。当向组织添加新帐户或创建新的委托人和资源时，也会保留基准配置。
- 透明度：账户状态报告允许您查看范围内账户的声明性策略支持的所有属性的当前状态。您还可以创建可自定义的错误消息，这可以帮助管理员将最终用户重定向到内部维基页面，或者提供描述性消息，帮助最终用户了解操作失败的原因。

有关支持的属 Amazon Web Services 服务 性和属性的完整列表，请参阅支持 Amazon Web Services 服务 和属性。

主题

声明式政策是如何运作的

声明式策略是在服务的控制平面中强制执行的，这与诸如服务控制策略 (SCPs) 和资源控制策略 () 之类的授权策略有重要区别。RCPs虽然授权策略规范访问权限 APIs，但声明性策略直接应用于服务级别，以强制执行持久意图。这样可以确保始终强制执行基准配置，即使服务引入了新功能或新功能 APIs 也是如此。

下表有助于说明这种区别，并提供了一些用例。

	服务控制策略	资源控制政策	声明式策略		
为什么？	大规模集中定义和实施对委	大规模集中定义和实施一致	集中定义和强制执行大规模		

	服务控制策略	资源控制政策	声明式策略		
	托人（例如 IAM 用户和 IAM 角色）的一致访问控制。	的资源访问控制	Amazon 服务的基准配置。		
怎么样？	通过在 API 级别控制委托人的最大可用访问权限。	通过在 API 级别控制资源的最大可用访问权限。	通过在 Amazon Web Services 服务不使用 API 操作的情况下强制执行所需的配置。		
管理与服务相关的角色？	否	否	是		
反馈机制	不可自定义的访问被拒绝 SCP 错误。	不可自定义的访问被拒绝 RCP 错误。	可自定义的错误消息。有关更多信息，请参阅 声明式策略的自定义错误消息。		
策略示例	根据请求的 Amazon Web Services 区域拒绝访问Amazon	限制仅通过 HTTPS 连接访问您的资源	允许的图像设置		

在您创建并附加声明性政策后，该政策将在您的组织中应用和执行。声明式策略可以应用于整个组织、组织单位 (OUs) 或帐户。加入组织的账户将自动继承组织中的声明性政策。有关更多信息，请参阅 了解管理策略继承。

有效的策略是从组织根目录继承的一组规则， OUs 以及直接关联到账户的规则。有效策略指定适用于账户的最终规则集。有关更多信息，请参阅 查看有效管理策略。

如果分离了声明性策略，则该属性状态将回滚到附加声明性策略之前的先前状态。

声明式策略的自定义错误消息

声明性策略允许您创建自定义错误消息。例如，如果 API 操作因声明性策略而失败，则可以设置错误消息或提供自定义 URL，例如指向内部 wiki 的链接或描述失败的消息的链接。如果您未指定自定义错误消息，则会 Amazon Organizations 提供以下默认错误消息：`Example: This action is denied due to an organizational policy in effect`。

您还可以使用审核创建声明性策略、更新声明性策略和删除声明性策略的过程。 Amazon CloudTrail CloudTrail 可以标记由于声明式策略而导致的 API 操作失败。有关更多信息，请参阅日志和监控。

> **Important**
>
> 请勿在自定义错误消息中包含个人身份信息 (PII) 或其他敏感信息。PII 包括可用于识别或定位个人的一般信息。它涵盖财务、医疗、教育或就业等记录。PII 示例包括地址、银行账号和电话号码。

声明性政策的账户状态报告

账户状态报告允许您查看范围内账户的声明性策略支持的所有属性的当前状态。您可以选择要包含在报告范围内的账户和组织单位 (OUs)，也可以通过选择根目录来选择整个组织。

此报告通过提供区域细分来帮助您评估准备情况，以及属性的当前状态是跨账户（通过`numberOfMatchedAccounts`）一致还是不一致（通过`numberOfUnmatchedAccounts`）。您还可以看到最常用的值，即该属性中最常观察到的配置值。

在图 1 中，生成了一份账户状态报告，该报告显示了不同账户在以下属性上的统一性：VPC 阻止公共访问和图像阻止公共访问、实例元数据默认值、快照块公共访问和允许的图像设置。这意味着，对于每个属性，范围内的所有帐户对该属性的配置都相同。

生成的账户状态报告显示以下属性的账户不一致：允许的图像设置、实例元数据默认值、串行控制台访问权限和快照区块公共访问权限。在此示例中，账户不一致的每个属性都是由于存在一个具有不同配置值的账户。

如果存在频率最高的值，则该值将显示在相应的列中。有关每个属性控制的内容的更多详细信息，请参阅声明式策略语法和示例策略。

您也可以展开属性以查看区域划分。在此示例中，Image Block Public Access 得到了扩展，在每个区域中，您都可以看到不同账户之间也有统一性。

选择附加用于强制执行基准配置的声明性策略取决于您的具体用例。在附加声明性政策之前，使用账户状态报告来帮助你评估自己的准备情况。

有关更多信息，请参阅生成账户状态报告。

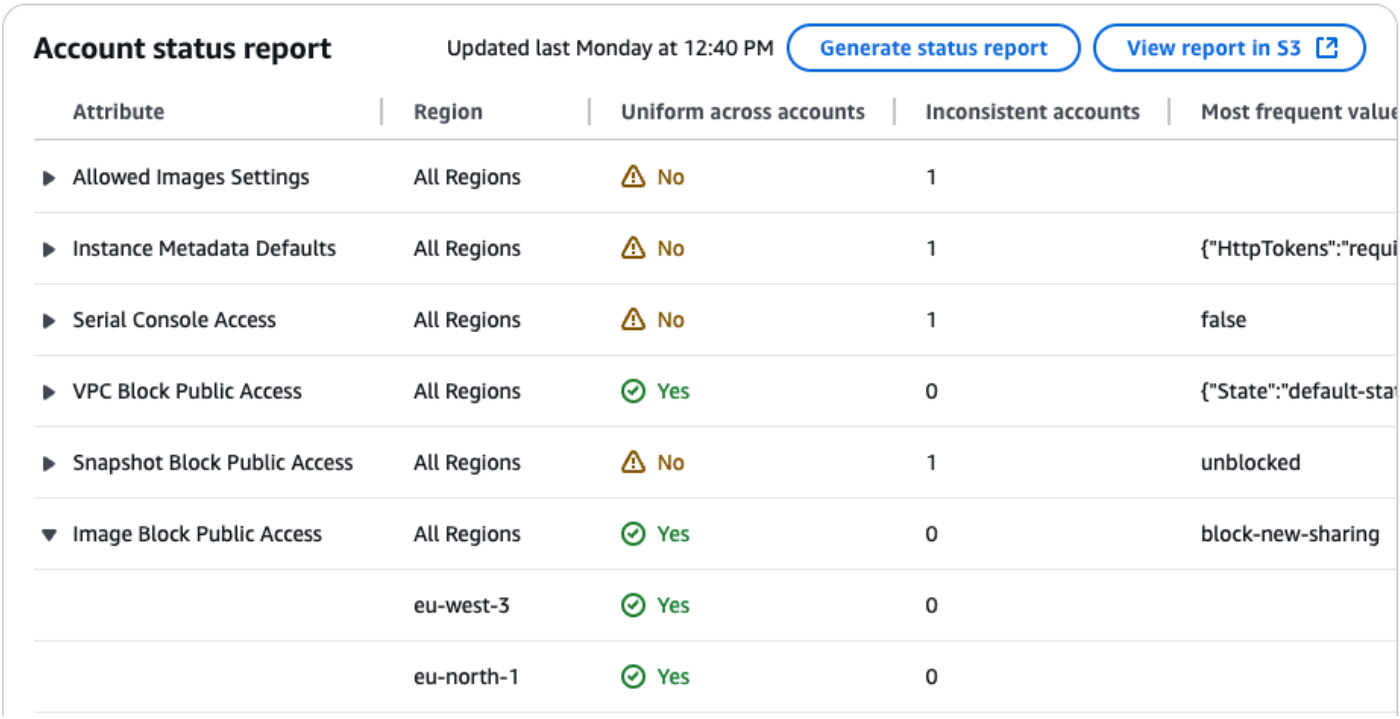


图 1：账户状态报告示例，其中包含 VPC 封锁公共访问和镜像屏蔽公共访问的账户状态报告保持一致。

支持 Amazon Web Services 服务 和属性

的声明式策略支持的属性 EC2

下表显示了 Amazon EC2 相关服务支持的属性。

的声明性政策 EC2

Amazon 服务	属性	政策效应	政策内容	更多信息
Amazon VPC	VPC 阻止公有访问	控制 Amazon VPCs 和子网中的资源能否通过互联网网关访问互联网（IGWs）。	查看策略	有关更多信息，请参阅 A mazon VPC 用户指南中的阻止对子网的公有访问。VPCs

Amazon 服务	属性	政策效应	政策内容	更多信息
Amazon EC2	串行控制台访问	控制是否可以访问 EC2 串行控制台。	查看策略	有关更多信息，请参阅 Amazon 弹性计算云用户指南中的配置 EC2 串行控制台访问权限。
	图像屏蔽公共访问	控制 Amazon 机器映像 (AMIs) 是否可公开共享。	查看策略	有关更多信息，请参阅《Amazon 弹性计算云用户指南》 AMIs中的“了解封锁公共访问”。
	允许的图像设置	使用 “允许” 控制亚马逊系统映像 (AMI) 的发现 EC2 和使用 AMIs。	查看策略	有关更多信息，请参阅《亚马逊弹性计算云用户指南》中的亚马逊系统映像 (AMIs)。
	实例元数据默认值	控制所有新 EC2 实例启动的 IMDS 默认值。	查看策略	有关更多信息，请参阅 Amazon Elastic Compute Cloud 用户指南中的为新实例配置实例元数据选项。

Amazon 服务	属性	政策效应	政策内容	更多信息
Amazon EBS	快照阻止公共访问	控制 Amazon EBS 快照是否可公开访问。	查看策略	有关更多信息，请参阅 Amazon Ela stic Block Store 用户指南中的禁止公开访问 Amazon EBS 快照。

声明式政策入门

请按照以下步骤开始使用声明性策略。

1. 了解执行声明性策略任务必须具备的权限。
2. 为您的组织启用声明性政策。

> **Note**
>
> 需要启用信任访问权限
> 您必须为声明性策略将强制执行基准配置的服务启用可信访问。这将创建一个只读的服务相关角色，该角色用于生成账户状态报告，说明组织中账户的现有配置。
> 使用控制台
> 如果您使用 Organizations 控制台，则此步骤是启用声明性策略过程的一部分。
> 使用 Amazon CLI
> 如果您使用 Amazon CLI，则有两个分开的 APIs：
>
> - EnablePolicyType，您可以使用它来启用声明式策略。
> - 启用AWSService访问权限，用于启用可信访问。
>
> 有关如何为特定服务启用可信访问权限的更多信息， Amazon CLI 请参阅 Amazon Web Services 服务 ，您可以与一起使用 Amazon Organizations。

3. 运行账户状态报告。
4. 创建声明性政策。
5. 将声明性政策附加到您组织的根目录、OU 或账户。
6. 查看适用于账户的有效声明式组合政策。

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

其他信息

- 学习声明式策略语法并查看策略示例

使用声明式策略的最佳实践

Amazon 推荐使用声明式策略的以下最佳实践。

利用准备情况评估

使用声明性策略账户状态报告来评估范围内账户的声明性策略支持的所有属性的当前状态。您可以选择要包含在报告范围内的账户和组织单位 (OUs)，也可以通过选择根目录来选择整个组织。

此报告通过提供区域细分来帮助您评估准备情况，以及属性的当前状态是跨账户（通过`numberOfMatchedAccounts`）一致还是不一致（通过`numberOfUnmatchedAccounts`）。您还可以看到最常用的值，即该属性中最常观察到的配置值。

选择附加用于强制执行基准配置的声明性策略取决于您的具体用例。

有关更多信息和说明性示例，请参阅声明性政策的账户状态报告。

从小处着手，然后扩大规模

要简化调试，请从测试策略开始。在进行下一个更改之前，验证每个更改的行为和影响。这种方法减少了发生错误或意外结果时必须考虑的变量数量。

例如，在非关键测试环境中，您可以从附加到单个账户的测试策略开始。在确认该政策符合您的规格后，您可以逐步将该策略在组织结构中向上移动到更多账户和更多组织单位（OUs）。

建立审查流程

实施流程以监控新的声明属性，评估政策例外情况，并进行调整以保持与组织安全和运营要求的一致性。

使用验证更改 **`DescribeEffectivePolicy`**

对声明式政策进行更改后，请查看低于更改级别的代表账户的有效政策。您可以通过使用 Amazon Web Services Management Console、或使用DescribeEffectivePolicyAPI操作或其 Amazon CLI 中的一个或多个 Amazon SDK变体来查看有效的策略。确保您所做的更改对有效策略产生预期影响。

沟通和训练

确保您的组织了解您的声明性政策的目的和影响。就预期行为以及如何处理因执行政策而导致的失败提供明确的指导。

为声明性政策生成账户状态报告

账户状态报告允许您查看范围内账户的声明性策略支持的所有属性的当前状态。您可以选择要包含在报告范围内的账户和组织单位 (OUs)，也可以通过选择根目录来选择整个组织。

此报告通过提供区域细分来帮助您评估准备情况，以及属性的当前状态是跨账户（通过`numberOfMatchedAccounts`）一致还是不一致（通过`numberOfUnmatchedAccounts`）。您还可以看到最常用的值，即该属性中最常观察到的配置值。

选择附加用于强制执行基准配置的声明性策略取决于您的具体用例。

有关更多信息和说明性示例，请参阅声明性政策的账户状态报告。

先决条件

在生成账户状态报告之前，必须执行以下步骤

1. `StartDeclarativePoliciesReport`API只能由组织的管理账户或委托管理员调用。
2. 在生成报告之前，您必须拥有 S3 存储桶（创建新存储桶或使用现有存储桶），该存储桶必须位于发出请求的同一区域，并且必须具有相应的 S3 存储桶策略。有关 S3 策略的示例，请参阅《亚马逊EC2API参考资料》中示例下的 Amazon S3 策略示例
3. 您必须为声明性策略将强制执行基准配置的服务启用可信访问。这将创建一个只读的服务相关角色，该角色用于生成账户状态报告，说明组织中账户的现有配置。

   使用控制台

   对于 Organizations 控制台，此步骤是启用声明性策略过程的一部分。

   使用 Amazon CLI

   对于 Amazon CLI，请使用 E A nableAWSService ccess API。

   有关如何为特定服务启用可信访问权限的更多信息， Amazon CLI 请参阅 Amazon Web Services 服务 ，您可以与一起使用 Amazon Organizations。
4. 每个组织一次只能生成一份报告。在另一份报告正在进行时尝试生成报告会导致错误。

访问合规状态报告

最小权限

要生成合规性状态报告，您需要获得运行以下操作的权限：

- `ec2:StartDeclarativePoliciesReport`
- `ec2:DescribeDeclarativePoliciesReports`
- `ec2:GetDeclarativePoliciesReportSummary`
- `ec2:CancelDeclarativePoliciesReport`
- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:DescribeOrganizationalUnit`
- `organizations:ListAccounts`
- `organizations:ListDelegatedAdministrators`
- `organizations:ListAWSServiceAccessForOrganization`

Amazon Web Services Management Console

使用以下步骤生成账户状态报告。

生成账户状态报告

1. 登录 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在 “政策” 页面上，选择 “声明性策略”。EC2
3. 在 “声明性政策 EC2” 页面上，从 “操作” 下拉菜单中选择 “查看账户状态报告”。
4. 在查看账户状态报告页面上，选择生成状态报告。
5. 在 “组织结构” 控件中，指定要在报告中包含哪些组织单位 (OUs)。
6. 选择提交。

Amazon CLI & Amazon SDKs

生成账户状态报告

使用以下操作生成合规性状态报告、检查其状态和查看报告：

- `ec2:start-declarative-policies-report`：生成账户状态报告。报告是异步生成的，可能需要几个小时才能完成。有关更多信息，请参阅 Amazon EC2 API 参考StartDeclarativePoliciesReport中的。
- `ec2:describe-declarative-policies-report`：描述账户状态报告的元数据，包括报告的状态。有关更多信息，请参阅 Amazon EC2 API 参考DescribeDeclarativePoliciesReports中的。
- `ec2:get-declarative-policies-report-summary`：检索账户状态报告摘要。有关更多信息，请参阅 Amazon EC2 API 参考GetDeclarativePoliciesReportSummary中的。
- `ec2:cancel-declarative-policies-report`：取消生成账户状态报告。有关更多信息，请参阅 Amazon EC2 API 参考CancelDeclarativePoliciesReport中的。

声明式策略语法和示例

本页描述了声明式策略语法并提供了示例。

注意事项

- 当您使用声明式策略配置服务属性时，它可能会影响多个 APIs属性。任何不合规的操作都将失败。
- 账户管理员将无法在个人账户级别修改服务属性的值。

声明式策略的语法

声明式策略是根据 JSON 规则构造的纯文本文件。声明性策略的语法遵循所有管理策略类型的语法。有关该语法的完整讨论，请参阅管理策略类型的策略语法和继承。本主题重点介绍如何将该通用语法应用于声明式策略类型的特定要求。

以下示例显示了基本的声明式策略语法：

```
{
    "ec2_attributes": {
        "exception_message": {
            "@@assign": "Your custom error message.https://myURL"
        },

        ...

        [Insert supported service attributes]
```

```
        ...
    }
}
```

- ec2_attributes 字段键名称。声明式策略始终以给 Amazon Web Services 服务定密钥的固定密钥名称开头。它是上面示例策略中的顶行。目前，声明性政策仅支持 EC2 与Amazon相关的服务。
- 在下方 ec2_attributesexception_message，您可以使用设置自定义错误消息。有关更多信息，请参阅声明式策略的自定义错误消息。
- 在下方ec2_attributes，您可以插入一个或多个支持的声明式策略。有关这些架构，请参阅支持的声明式策略。

支持的声明式策略

以下是声明式策略支持的 Amazon Web Services 服务 和属性。在以下某些示例中，可能会压缩 JSON 空白格式以节省空间。

VPC Block Public Access

政策影响

控制 Amazon VPCs 和子网中的资源能否通过互联网网关访问互联网（IGWs）。有关更多信息，请参阅 Amazon Virtual Private Cloud 用户指南中的互联网访问配置。

政策内容

```
"vpc_block_public_access": {
    "internet_gateway_block": { // (optional)
        "mode": { // (required)
            "@@assign": "block_ingress" // off | block_ingress | block_bidirectional
        },
        "exclusions_allowed": { // (required)
            "@@assign": "enabled" // enabled | disabled
        }
    }
}
```

以下是此属性的可用字段：

- "internet_gateway":

- "mode":
  - "off": VPC BPA 未启用。
  - "block_ingress"：所有流向的互联网流量 VPCs （ VPCs 或不包括的子网除外）都已被阻止。仅允许进出 NAT 网关和仅出口互联网网关的流量，因为这些网关仅允许建立出站连接。
  - "block_bidirectional"：所有进出互联网网关和仅限出口的互联网网关（排除的 VPCs 和子网除外）的流量都已被阻止。
- "exclusions_allowed"：排除是一种可以应用于单个 VPC 或子网的模式，可将其排除在账户的 VPC BPA 模式之外，并允许双向或仅限出口访问。
  - "enabled"：排除项可以由账户创建。
  - "disabled"：账户无法创建排除项。

> **Note**
>
> 您可以使用该属性来配置是否允许排除，但不能使用此属性本身创建排除项。要创建排除项，您必须在拥有 VPC 的账户中创建排除项。有关创建 VPC BPA 排除项的更多信息，请参阅 Amazon VPC 用户指南中的创建和删除排除项。

注意事项

如果您在声明性策略中使用此属性，则无法使用以下操作来修改范围内账户的强制配置。此列表并不详尽：

- ModifyVpcBlockPublicAccessOptions
- CreateVpcBlockPublicAccessExclusion
- ModifyVpcBlockPublicAccessExclusion

Serial Console Access

政策影响

控制是否可以访问 EC2 串行控制台。有关 EC2 串行控制台的更多信息，请参阅 Amazon 弹性计算云用户指南中的EC2 串行控制台。

政策内容

```
"serial_console_access": {
    "status": { // (required)
        "@@assign": "enabled" // enabled | disabled
    }
}
```

以下是此属性的可用字段：

- "status":
  - "enabled": 允许 EC2 串行控制台访问。
  - "disabled": EC2 串行控制台访问已被阻止。

注意事项

如果您在声明性策略中使用此属性，则无法使用以下操作来修改范围内账户的强制配置。此列表并不详尽：

- EnableSerialConsoleAccess
- DisableSerialConsoleAccess

Image Block Public Access

政策影响

控制 Amazon 机器映像 (AMIs) 是否可公开共享。有关更多信息 AMIs，请参阅《亚马逊弹性计算云用户指南》中的亚马逊系统映像 (AMIs)。

政策内容

```
"image_block_public_access": {
    "state": { // (required)
        "@@assign": "block_new_sharing" // unblocked | block_new_sharing
    }
}
```

以下是此属性的可用字段：

- "state":
  - "unblocked": 对公开共享没有限制 AMIs。

- "block_new_sharing": 阻止新的公开共享 AMIs。 AMIs 已经公开分享的内容仍然是公开的。

注意事项

如果您在声明性策略中使用此属性，则无法使用以下操作来修改范围内账户的强制配置。此列表并不详尽：

- EnableImageBlockPublicAccess
- DisableImageBlockPublicAccess

Allowed Images Settings

政策影响

使用 “允许” 控制亚马逊系统映像 (AMI) 的发现 EC2 和使用 AMIs... 有关更多信息 AMIs，请参阅《亚马逊弹性计算云用户指南》中的亚马逊系统映像 (AMIs)。

政策内容

以下是此属性的可用字段：

```
"allowed_images_settings": {
    "state": { // (required)
        "@@assign": "enabled" // enabled | disabled | audit_mode
    },
    "image_criteria": { // (optional)
        "criteria_1": {
            "allowed_image_providers": { // limit 200
                "@@append": [
                    "amazon" // amazon | aws_marketplace | aws_backup_vault | 12
 digit account ID
                ]
            }
        }
    }
}
```

- "state":
  - "enabled"：该属性处于活动状态且已强制执行。

- "disabled"：该属性处于非活动状态且未强制执行。
- "audit_mode"：该属性处于审核模式。这意味着它将识别不合规的图像，但不会阻止其使用。

- "image_criteria"：定义允许的 AMI 源的allowed_image_providers对象列表。
  - "allowed_image_providers"：以逗号分隔的提供商名称或帐户列表。 IDs

注意事项

如果您在声明性策略中使用此属性，则无法使用以下操作来修改范围内账户的强制配置。此列表并不详尽：

- EnableAllowedImagesSettings
- ReplaceImageCriteriaInAllowedImagesSettings
- DisableAllowedImagesSettings

Instance Metadata Defaults

政策影响

控制所有新 EC2 实例启动的 IMDS 默认值。有关 IMDS 默认值的更多信息，请参阅《亚马逊弹性计算云用户指南》中的 IMDS。

政策内容

以下是此属性的可用字段：

```
"instance_metadata_defaults": {
    "http_tokens": { // (required)
        "@@assign": "required" // no_preference | required | optional
    },
    "http_put_response_hop_limit": { // (required)
        "@@assign": "4" // -1 | 1 -> 64
    },
    "http_endpoint": { // (required)
        "@@assign": "enabled" // no_preference | enabled | disabled
    },
    "instance_metadata_tags": { // (required)
        "@@assign": "enabled" // no_preference | enabled | disabled
    }
```

```
}
```

- "http_tokens":
  - "no_preference": 其他默认值适用。例如，AMI 会默认设置（如果适用）。
  - "required": IMDSv2 必须使用。 IMDSv1 是不允许的。
  - "optional": 两者 IMDSv1 IMDSv2 都允许。

> **Note**
>
> 元数据版本
> 在设置http_tokens为required（IMDSv2 必须使用）之前，请确保您的所有实例都没有进行 IMDSv1 调用。

- "http_put_response_hop_limit":
  - "*Integer*": -1 到 64 之间的整数值，表示元数据令牌可以传输的最大跳数。要表示没有偏好，请指定 -1。

> **Note**
>
> 跳跃限制
> 如果设置http_tokens为required，则建议至少设置http_put_response_hop_limit为 2。有关更多信息，请参阅 Amazon 弹性计算云用户指南中的实例元数据访问注意事项。

- "http_endpoint":
  - "no_preference": 其他默认值适用。例如，AMI 会默认设置（如果适用）。
  - "enabled"：实例元数据服务终端节点可访问。
  - "disabled"：无法访问实例元数据服务终端节点。
- "instance_metadata_tags":
  - "no_preference": 其他默认值适用。例如，AMI 会默认设置（如果适用）。
  - "enabled"：可以从实例元数据访问实例标签。
  - "disabled"：无法从实例元数据访问实例标签。

Snapshot Block Public Access

政策影响

控制 Amazon EBS 快照是否可公开访问。有关 EBS 快照的更多信息，请参阅《亚马逊弹性区块存储用户指南》中的 Amazon EBS 快照。

政策内容

```
"snapshot_block_public_access": {
    "state": { // (required)
        "@@assign": "block_new_sharing" // unblocked | block_new_sharing |
 block_all_sharing
    }
}
```

以下是此属性的可用字段：

- "state":
  - "block_all_sharing"：阻止所有公开共享快照。已公开共享的快照将被视为私有快照，不再公开可用。
  - "block_new_sharing"：阻止新的快照公开共享。已经公开共享的快照仍可公开获取。
  - "unblocked"：对公开共享快照没有限制。

注意事项

如果您在声明性策略中使用此属性，则无法使用以下操作来修改范围内账户的强制配置。此列表并不详尽：

- EnableSnapshotBlockPublicAccess
- DisableSnapshotBlockPublicAccess

备份策略

Backup 策略允许您集中管理备份计划并将其应用于组织账户中的 Amazon 资源。

Amazon Backup使您能够创建定义如何备份 Amazon 资源的备份计划。计划中的规则包括各种设置，例如备份频率、备份发生的时间窗口、 Amazon Web Services 区域 包含要备份的资源以及存储备

份的存储库。然后，您可以将备份计划应用于使用标签标识的 Amazon 资源组。您还必须确定一个 Amazon Identity and Access Management (IAM) 角色，该角色授予代表您执行备份操作的 Amazon Backup 权限。

Backup 策略 Amazon Organizations 将所有这些部分合并成JSON文本文档。您可以将备份策略附加到组织结构中的任何元素，例如根帐户、组织单位 (OUs) 和个人帐户。Organizations 应用继承规则来合并组织根目录OUs、任何父级或账户关联的策略。这将为每个账户生成有效备份策略。这项有效的政策指导了 Amazon Backup 如何自动备份您的 Amazon 资源。

备份策略的工作原理

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

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

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

组织 Amazon Web Services 账户 中每个人的有效备份计划作为该账户的不可变计划显示在 Amazon Backup 控制台中。您可以查看该计划，但不能更改。但是，您可以使用TagResource和添加或移除备份计划标签UntagResourceAPIs。

当根据策略创建的备份计划 Amazon Backup 开始备份时，您可以在 Amazon Backup 控制台中看到备份任务的状态。成员账户中的用户可以查看该成员账户中的备份作业的状态和任何错误。如果您还使用启用可信服务访问权限 Amazon Backup，则组织管理账户中的用户可以看到组织中所有备份任务的状态和错误。有关更多信息，请参阅《Amazon Backup 开发人员指南》中的启用跨账户管理。

备份策略入门

请按照以下步骤开始使用备份策略。

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

在所有这些步骤中，您都需要以IAM用户身份登录、代入IAM角色或以根用户身份登录（不推荐）在组织的管理账户中登录。

其他信息

- 了解备份策略语法并查看示例策略

使用备份策略的最佳实践

Amazon 推荐以下使用备份策略的最佳实践。

决定备份策略

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

使用 **`GetEffectivePolicy`** 验证对备份策略的更改

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

简单开始并进行一些小更改

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

将备份的副本存储在其他Amazon Web Services 区域和您组织中的账户中

为了增强灾难恢复能力，您可以存储备份的副本。

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

限制每个策略的计划数量

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

使用堆栈套创建所需的备份文件库和 IAM 角色

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

通过查看在每个账户中创建的第一个备份来检查您的结果

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

使用 Amazon CloudTrail 事件监控组织中的备份策略

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

备份策略语法和示例

本页介绍备份策略语法并提供示例。

备份策略的语法

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

备份策略的这一部分是备份计划及其规则。备份策略中备份计划的语法在结构上与使用的语法相同 Amazon Backup，但密钥名称不同。 Amazon Organizations 在下面对策略密钥名称的描述中，每个名称都包含等效的 Amazon Backup 计划密钥名称。有关 Amazon Backup 计划的更多信息，请参阅Amazon Backup 开发人员指南CreateBackupPlan中的。

> **Note**
>
> 使用 JSON 时，重复的键名称将被拒绝。如果您想在单个策略中包含多个计划、规则或选项，请确保每个键名称都是唯一的。

有效备份策略要完整而实用，必须不仅仅包括备份计划及其时间安排和规则。该策略还必须确定要备份的 Amazon Web Services 区域 和资源，以及 Amazon Backup 可用于执行备份的 Amazon Identity and Access Management (IAM) 角色。

以下功能完整的策略显示了基本备份策略语法。如果此示例直接关联到账户，则 Amazon Backup 会备份该账户在`us-east-1`和`eu-north-1`区域中标签值`dataType`为`PII`或的所有资源`RED`。它每天上午 5:00 将这些资源备份到 `My_Backup_Vault` 中，同时将副本存储在 `My_Secondary_Vault` 中。这两个文件库与资源位于同一个账户中。它还会将备份的副本存储在另一个明确指定的账户中的 `My_Tertiary_Vault` 中。这些文件库必须已经存在于每个接收有效策略 Amazon Web Services 区域 的指定文件库中。 Amazon Web Services 账户 如果任何备份的资源是 EC2 实例，则这些实例上的备份将启用对 Microsoft 卷影复制服务 (VSS) 的支持。该备份将标签 `Owner:Backup` 应用到每个恢复点。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "rules": {
                "My_Hourly_Rule": {
                    "schedule_expression": {"@@assign": "cron(0 5 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "complete_backup_window_minutes": {"@@assign": "604800"},
                    "enable_continuous_backup": {"@@assign": false},
                    "target_backup_vault_name": {"@@assign": "My_Backup_Vault"},
                    "recovery_point_tags": {
                        "Owner": {
                            "tag_key": {"@@assign": "Owner"},
                            "tag_value": {"@@assign": "Backup"}
                        }
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "delete_after_days": {"@@assign": "270"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"},
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        },
                        "arn:aws:backup:us-east-1:111111111111:backup-
vault:My_Tertiary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
east-1:111111111111:backup-vault:My_Tertiary_Vault"
                            },
                            "lifecycle": {
```

```
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"},
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "regions": {
                "@@append": [
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "selections": {
                "tags": {
                    "My_Backup_Assignment": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {"@@assign": "enabled"}
                }
            },
            "backup_plan_tags": {
                "stage": {
                    "tag_key": {"@@assign": "Stage"},
                    "tag_value": {"@@assign": "Beta"}
                }
            }
        }
    }
```

```
}
```

备份策略语法包括以下组件：

- `$account` 变量 – 在策略的某些文本字符串中，可以使用 `$account` 变量来表示当前 Amazon Web Services 账户。在有效策略中 Amazon Backup 运行计划时，它会自动将此变量替换为有效策略及其计划正在运行的当前 Amazon Web Services 账户 变量。

  > **Important**
  >
  > 您只能在可以包含 Amazon Resource Name（ARN）的策略元素中使用 `$account` 变量，例如指定要存储备份的备份文件库的元素或具有执行备份的权限的 IAM 角色。

  例如，以下内容要求该策略适用的每个文件库中都`My_Vault` Amazon Web Services 账户 存在名为的文件库。

  ```
  arn:aws:backup:us-west-2:$account:backup-vault:My_Vault"
  ```

  我们建议您使用 Amazon CloudFormation 堆栈集及其与 Organizations 的集成，为组织中的每个成员账户自动创建和配置备份库和 IAM 角色。有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的创建具有自行管理权限的堆栈套。

- 继承运算符 – 备份策略可以同时使用继承值设置运算符和子控制运算符。

- `plans`

  策略的顶级键是 `plans` 键。在策略文件顶部，备份策略必须始终以此固定键名称开头。在此键下，您可以有一个或多个备份计划。

- `plans` 顶级键下的每个计划都有一个由用户分配的备份计划名称组成的键名称。在前面的示例中，备份计划名称为 `PII_Backup_Plan`。一个策略中可以有多个计划，每个计划都有自己的 `rules`、`regions`、`selections` 和 `tags`。

  备份策略中的此备份计划密钥名称映射到 Amazon Backup 计划中该`BackupPlanName`密钥的值。

  每个计划可以包含以下元素：

  - `rules` – 此键包含规则集合。每个规则都转换为一个计划任务，其中包含有效备份策略中由 `selections` 和 `regions` 元素标识的资源的开始时间和时段。

- regions— 此密钥包含一个数组列表，其中列出了此策略可以备份 Amazon Web Services 区域其资源。
- selections – 此键包含一个或多个按指定 rules 备份的资源集合（在指定的 regions 内）。
- advanced_backup_settings – 此键包含特定于在某些资源上运行的备份的设置。
- backup_plan_tags – 此键指定附加到备份计划本身的标签。

- rules

  rules 策略键映射到 Amazon Backup 计划中的 Rules 键。rules 键下可以有一个或多个规则。每个规则都会成为执行选定资源备份的计划任务。

  每个规则都包含一个其名称是规则名称的键。在前一个示例中，规则名称为“My_Hourly_Rule”。规则键的值是以下规则元素集合：

  - schedule_expression— 此策略密钥映射到 Amazon Backup 计划中的ScheduleExpression密钥。

    指定备份的开始时间。此键包含@@assign继承值运算符和带有 CRON 表达式的字符串值，该表达式指定何时 Amazon Backup 启动备份作业。CRON 字符串的一般格式为：“cron( )”。每一项都是一个数字或通配符。例如，cron(0 5 ? * 1,3,5 *) 表示在每个星期一、星期三和星期五的上午 5 点开始备份。cron(0 0/1 ? * * *) 表示在每周中的每天中的每小时开始一次备份。

  - target_backup_vault_name— 此策略密钥映射到 Amazon Backup 计划中的TargetBackupVaultName密钥。

    指定要在其中存储备份的备份文件库的名称。您可以通过使用来创造价值 Amazon Backup。此键包含 @@assign 继承值运算符和一个具有文件库名称的字符串值。

    > **Important**
    >
    > 首次启动备份计划时，该文件库必须已存在。我们建议您使用 Amazon CloudFormation 堆栈集及其与 Organizations 的集成，为组织中的每个成员账户自动创建和配置备份库和 IAM 角色。有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的创建具有自行管理权限的堆栈集。

  - start_backup_window_minutes— 此策略密钥映射到 Amazon Backup 计划中的StartWindowMinutes密钥。

    （可选）指定在取消未成功启动的作业之前等待的分钟数。此键包含 @@assign 继承值运算符和一个具有整数分钟数的值。

- `complete_backup_window_minutes` – 此策略键映射到 Amazon Backup 计划中的 `CompletionWindowMinutes` 键。

  （可选）指定备份作业成功启动之后到备份作业必须完成或由 Amazon Backup取消之前的分钟数。此键包含 @@assign 继承值运算符和一个具有整数分钟数的值。

- `enable_continuous_backup`— 此策略密钥映射到 Amazon Backup 计划中的`EnableContinuousBackup`密钥。

  （可选）指定是否 Amazon Backup 创建连续备份。 `True`导致创建 Amazon Backup 能够 point-in-time恢复的连续备份 (PITR)。 `False`（或未指定）创建快照备份的原因 Amazon Backup 。

  > **Note**
  >
  > 由于启用 PITR 的备份最多可以保留 35 天，因此如果设置了以下选项之一，您必须选择 `False` 或不指定值：
  >
  > - 将 `delete_after_days` 设置为大于 35。
  > - 将 `move_to_cold_storage_after_days` 设置为任何值。

  有关持续备份的更多信息，请参阅《Amazon Backup 开发人员指南》中的Point-in-time 恢复。

- `lifecycle`— 此策略密钥映射到 Amazon Backup 计划中的`Lifecycle`密钥。

  （可选）指定何 Amazon Backup 时将此备份转换为冷存储以及何时过期。

  - `move_to_cold_storage_after_days` — 此策略密钥映射到 Amazon Backup 计划中的`MoveToColdStorageAfterDays`密钥。

    指定备份发生之后到 Amazon Backup 将恢复点移到冷存储之前的天数。此键包含 @@assign 继承值运算符和一个具有整数天数的值。

  - `delete_after_days`— 此策略密钥映射到 Amazon Backup 计划中的`DeleteAfterDays`密钥。

    指定备份发生之后到 Amazon Backup 删除恢复点之前的天数。此键包含 @@assign 继承值运算符和一个具有整数天数的值。此值必须是 `move_to_cold_storage_after_days` 中指定的天数后至少 90 天。

  - `opt_in_to_archive_for_supported_resources`— 此策略密钥映射到 Amazon Backup 计划中的`OptInToArchiveForSupportedResources`密钥。

如果此值设置为 `true`，则您的备份计划将根据您的生命周期设置将支持的资源转移到归档（冷）存储层。有关 Amazon EBS 快照归档更多信息，请参阅《Amazon EBS 用户指南》中的归档 Amazon EBS 快照。

您只能在满足以下条件时启用此设置：

- 您的备份策略的频率为一个月或更长时间一次。
- `move_to_cold_storage_after_days` 必须存在。
- `delete_after_days` 减去 `move_to_cold_storage_after_days` 后大于或等于 90 天。

此键包含 `@@assign` 继承值运算符和一个 `true` 或 `false` 值。

- `copy_actions`— 此策略密钥映射到 Amazon Backup 计划中的`CopyActions`密钥。

（可选）指定 Amazon Backup 应将备份复制到一个或多个其他位置。每个备份副本位置描述如下：

- 其名称唯一标识此复制操作的键。目前，键名称必须是备份文件库的 Amazon Resource Name（ARN）。此键包含两个条目。
  - `target_backup_vault_arn` – 此策略键映射到 Amazon Backup 计划中的 `DestinationBackupVaultArn` 键。

    （可选）指定 Amazon Backup 存储额外备份副本的存储库。此键的值包含 `@@assign` 继承值运算符和文件库的 ARN。
    - 要在中 Amazon Web Services 账户 引用运行备份策略的文件库，请使用 ARN 中的`$account`变量代替账户 ID 号。 Amazon Backup 运行备份计划时，它会自动将变量替换为运行策略 Amazon Web Services 账户 的账户 ID 号。这样，当备份策略应用于组织中的多个账户时，备份就可以正确运行。
    - 要在同一组织内的不同 Amazon Web Services 账户 中引用文件库，请使用 ARN 中的实际账户 ID 号。

    > **Important**
    >
    > - 如果缺少此键，则使用父键名称中所有小写版本的 ARN。由于区 ARNs 分大小写，因此此字符串可能与文件库的实际 ARN 不匹配，因此计划会失败。为此，我们建议您始终提供此键和值。
    > - 首次启动备份计划时，您希望复制的备份文件库必须已存在。我们建议您使用 Amazon CloudFormation 堆栈套及其与 Organizations 的集成，为组织中的每个成

员账户自动创建和配置备份文件库和 IAM 角色。有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的创建具有自行管理权限的堆栈套。

- `lifecycle`— 此策略密钥映射到 Amazon Backup 计划中`CopyAction`密`Lifecycle`钥下的密钥。

  （可选）指定何 Amazon Backup 时将此备份副本转换为冷存储以及何时过期。

  - `move_to_cold_storage_after_days` – 此策略键映射到 Amazon Backup 计划中的 `MoveToColdStorageAfterDays` 键。

    指定备份创建日期之后将恢复点 Amazon Backup 移至冷存储之前的天数。此键包含 `@@assign` 继承值运算符和一个具有整数天数的值。

  - `delete_after_days` – 此策略键映射到 Amazon Backup 计划中的 `DeleteAfterDays` 键。

    指定备份发生后在 Amazon Backup 删除恢复点之前的天数。此键包含 `@@assign` 继承值运算符和一个具有整数天数的值。如果将备份过渡到冷存储，则备份必须至少保持冷存储 90 天，因此该值必须至少比 `move_to_cold_storage_after_days` 值多 90 天。

- `recovery_point_tags`— 此策略密钥映射到 Amazon Backup 计划中的`RecoveryPointTags`密钥。

  （可选）指定 Amazon Backup 附加到根据该计划创建的每个备份的标签。此键的值包含以下一个或多个元素：

  - 此键名称和值对的标识符。`recovery_point_tags` 下的每个元素的此名称都是全部小写的标签键名称，即使 `tag_key` 具有不同的大小写处理方式也是如此。此标识符不 区分大小写。在前一个示例中，此键对由名称 `Owner` 标识。每个键对都包含以下元素：

    - `tag_key` – 指定要附加到备份计划的标签键名称。此键包含 `@@assign` 继承值运算符和一个字符串值。 值区分大小写。

    - `tag_value`：指定附加到备份计划并与 `tag_key` 关联的值。此键包含任何继承值运算符以及一个或多个要在有效策略中替换、追加或删除的值。这些值区分大小写。

- `regions`

  `regions`策略密钥指定 Amazon Web Services 区域 在哪些资源中 Amazon Backup 查找与`selections`密钥中的条件相匹配的资源。此键包含任何继承值运算符以及 Amazon Web Services 区域 代码的一个或多个字符串值，例如：`["us-east-1", "eu-north-1"]`。

- `selections`

selections 策略键指定由此策略中的计划规则备份的资源。此键大致对应于中的BackupSelection对象 Amazon Backup。资源由匹配标签键名称和值的查询指定。selections密钥下方包含两个密钥—— tags 和resources。

> **Note**
>
> 在同一个选择中，tags和resources键不能一起使用。如果您想要同时包含标签条件和资源条件的选择，则必须使用resources密钥。有效的策略必须选择tags或resources才能生效。

- tags – 指定标识资源以及具有查询和备份资源权限的 IAM 角色的标签。此键的值包含以下一个或多个元素：
  - 此标签元素的标识符。tags 下的此标识符是全部小写的标签键名称，即使要查询的标签具有不同的大小写处理方式也是如此。此标识符不 区分大小写。在前一个示例中，一个元素是由名称 My_Backup_Assignment 标识的。tags 下的每个标识符都包含以下元素：
    - iam_role_arn – 指定有权访问资源（由 regions 键指定的 Amazon Web Services 区域 中的标签查询标识）的 IAM 角色。此值包含@@assign继承值运算符和包含角色的 ARN 的字符串值。 Amazon Backup 使用此角色查询和发现资源以及执行备份。

      您可以使用 ARN 中的 $account 变量来代替账户 ID 号。当备份计划由运行时 Amazon Backup，它会自动将变量替换为运行该策略的实际账户 ID 号。 Amazon Web Services 账户

      > **Important**
      >
      > 首次启动备份计划时，该角色必须已存在。我们建议您使用 Amazon CloudFormation 堆栈集及其与 Organizations 的集成，为组织中的每个成员账户自动创建和配置备份库和 IAM 角色。有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的创建具有自行管理权限的堆栈套。

    - tag_key – 指定要搜索的标签键名称。此键包含 @@assign 继承值运算符和一个字符串值。值区分大小写。
    - tag_value— 指定必须与匹配的键名关联的值tag_key。 Amazon Backup 只有当tag_key和都tag_value匹配时，才会将资源包含在备份中。此键包含任何继承值运算符以及一个或多个要在有效策略中替换、追加或删除的值。这些值区分大小写。

- conditions— 指定要包含或排除的标签键和值。您可以使用 string_equals 或 string_not_equals to include or exclude tags of an exact match。也可以使用string_like和string_not_like来包含或排除包含或不包含特定字符的标签。

> **Note**
>
> 每个选择的上限conditions为 30。

示例：使用**tags**方块指定资源

以下示例包括所有带有 tag_key = “env” 和 = "prod" 和 tag_value = 的资源"gamma"。此示例不包括带有 tag_key = "backup" 和 tag_value = 的资源"false"。

```
...
"selections":{
    "tags":{
        "selection_name":{
            "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "tag_key":{"@@assign": "env"},
            "tag_value":{"@@assign": ["prod", "gamma"]},
            "conditions":{
                "string_not_equals":{
                    "condition_name1":{
                        "condition_key": { "@@assign": "aws:ResourceTag/backup"  },
                        "condition_value": {  "@@assign": "false" }
                    }
                }
            }
        }
    }
},
...
```

- resources— 如果要同时使用标签条件和资源条件来指定资源，则必须使用resources密钥。
  - iam_role_arn – 指定有权访问资源（由 regions 键指定的 Amazon Web Services 区域 中的标签查询标识）的 IAM 角色。此值包含@@assign继承值运算符和包含角色的 ARN 的字符串值。 Amazon Backup 使用此角色查询和发现资源以及执行备份。

    您可以使用 ARN 中的 $account 变量来代替账户 ID 号。当备份计划由运行时 Amazon Backup，它会自动将变量替换为运行该策略的实际账户 ID 号。 Amazon Web Services 账户

> **Important**
>
> 首次启动备份计划时，该角色必须已存在。我们建议您使用 Amazon CloudFormation 堆栈集及其与 Organizations 的集成，为组织中的每个成员账户自动创建和配置备份库和 IAM 角色。有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的创建具有自行管理权限的堆栈集。

> **Note**
>
> 在中 Amazon GovCloud (US) Regions，您必须将分区的名称添加到 ARN。例如，`"arn:aws:ec2:*:*:volume/*"`必须是`"arn:aws-us-gov:ec2:*:*:volume/*"`。

- `resource_types`— 指定要包含在备份计划中的资源类型。
- `not_resource_types`— 指定要在备份计划中排除的资源类型。

  Organizations 支持`resource_types`和的以下资源类型`not_resource_types`：

  - Amazon Backup gateway 虚拟机：`"arn:aws:backup-gateway:*:*:vm/*"`
  - Amazon CloudFormation 堆栈：`"arn:aws:cloudformation:*:*:stack/*"`
  - 亚马逊 DynamoDB 表：`"arn:aws:dynamodb:*:*:table/*"`
  - 亚马逊 EC2 实例：`"arn:aws:ec2:*:*:instance/*"`
  - 亚马逊 EBS 交易量：`"arn:aws:ec2:*:*:volume/*"`
  - 亚马逊 EFS 文件系统：`"arn:aws:elasticfilesystem:*:*:file-system/*"`
  - 亚马逊 Aurora/Amazon DocumentDB/Amazon Neptune 集群：`"arn:aws:rds:*:*:cluster:*"`
  - 亚马逊 RDS 数据库：`"arn:aws:rds:*:*:db:*"`
  - 亚马逊 Redshift 集群：`"arn:aws:redshift:*:*:cluster:*"`
  - Amazon S3：`"arn:aws:s3:::*"`
  - 适用于 SAP 的 Amazon Systems Manager HANA 数据库：`"arn:aws:ssm-sap:*:*:HANA/*"`
  - Amazon Storage Gateway 网关：`"arn:aws:storagegateway:*:*:gateway/*"`
  - 亚马逊 Timestream 数据库：`"arn:aws:timestream:*:*:database/*"`

- Amazon FSx 文件系统："arn:aws:fsx:*:*:file-system/*"
- 亚马逊 FSx 交易量："arn:aws:fsx:*:*:volume/*"

- conditions— 指定要包含或排除的标签键和值。您可以使用 string_equals 或 string_not_equals to include or exclude tags of an exact match。也可以使用string_like和string_not_like来包含或排除包含或不包含特定字符的标签。

> **Note**
>
> 每个选择的上限conditions为 30。

示例：使用**resources**方块指定资源

以下是使用resources区块指定资源的示例。

Example: Select all resources in my account

布尔逻辑与您可能在 IAM 策略中使用的逻辑类似。该"resource_types"区块使用布尔值AND来组合资源类型。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        }
    }
},
...
```

Example: Select all resources in my account, but exclude Amazon EBS volumes

布尔逻辑与您可能在 IAM 策略中使用的逻辑类似。"resource_types"和"not_resource_types"块使用布尔值AND来组合资源类型。

```
...
"resources":{
    "resource_selection_name":{
```

```
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        }
    }
},
...
```

Example: Select all resources tagged with "backup" : "true", but exclude Amazon EBS volumes

布尔逻辑与您可能在 IAM 策略中使用的逻辑类似。"resource_types"和"not_resource_types"块使用布尔值AND来组合资源类型。该"conditions"方块使用布尔值AND。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key": { "@@assign":"aws:ResourceTag/backup"},
                    "condition_value": {  "@@assign":"true" }
                }
            }
        }
```

```
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS DB instances tagged with both "backup" : "true" and "stage" : "prod"

布尔逻辑与您可能在 IAM 策略中使用的逻辑类似。该"resource_types"区块使用布尔值AND来组合资源类型。该"conditions"区块使用布尔值AND来组合资源类型和标签条件。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                },
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"prod"}
                }
            }
        }
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS instances tagged with "backup" : "true" but not "stage" : "test"

布尔逻辑与您可能在 IAM 策略中使用的逻辑类似。该"resource_types"区块使用布尔值AND来组合资源类型。该"conditions"区块使用布尔值AND来组合资源类型和标签条件。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                  }
            },
            "string_not_equals":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"test"}
                }
            }
        }
    }
},
...
```

Example: Select all resources tagged with "key1" and a value which begins with "include" but not with "key2" and value that contains the word "exclude"

布尔逻辑与您可能在 IAM 策略中使用的逻辑类似。该"resource_types"区块使用布尔值AND来组合资源类型。该"conditions"区块使用布尔值AND来组合资源类型和标签条件。

在此示例中，请注意在include**exclude*、和(*)arn:aws:rds:*:*:db:*中使用通配符。可以在字符串的开头、结尾和中间使用通配符(*)。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
```

```
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "conditions":{
            "string_like":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key1"},
                    "condition_value":{"@@assign":"include*"}
                }
            },
            "string_not_like":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key2"},
                    "condition_value":{"@@assign":"*exclude*"}
                }
            }
        }
    }
},
...
```

Example: Select all resources tagged with "backup" : "true" except Amazon FSx file systems and Amazon RDS resources

布尔逻辑与您可能在 IAM 策略中使用的逻辑类似。"resource_types"和"not_resource_types"块使用布尔值AND来组合资源类型。该"conditions"区块使用布尔值AND来组合资源类型和标签条件。

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "resource_types":{
                "@@assign": [
                    "*"
               ]
            },
            "not_resource_types":{
                "@@assign":[
                    "arn:aws:fsx:*:*:file-system/*",
                    "arn:aws:rds:*:*:db:*"
```

```
                ]
            },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                }
            }
        }
    },
...
```

- advanced_backup_settings – 指定特定备份方案的设置。此键包含一个或多个设置。每个设置都是一个 JSON 对象字符串，其中包含以下元素：
  - 对象键名称 – 一个字符串，它指定应用以下高级设置的资源类型。
  - 对象值 – 一个 JSON 对象字符串，包含特定于关联资源类型的一个或多个备份设置。

  目前，唯一支持的高级备份设置为在亚马逊 EC2 实例上运行的 Windows 或 SQL Server 启用微软卷影复制服务 (VSS) 备份。密钥名称必须是"ec2"资源类型，该值指定"windows_vss"支持disabled对这些 Amazon EC2 实例执行的备份。enabled

  有关此功能的更多信息，请参阅《Amazon Backup 开发人员指南》中的创建启用 VSS 的 Windows Backup。

  示例：使用**advanced_backup_settings**区块指定备份方案

  以下示例说明如何为在亚马逊 EC2 实例上运行的 Windows 或 SQL Server 启用微软卷影复制服务 (VSS) 备份。

```
...
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
    }
},
...
```

- backup_plan_tags – 指定附加到备份计划本身的标签。这不会影响任何规则或选择中指定的标签。

  （可选）您可以将标签附加到备份计划。此键的值是元素的集合。

  backup_plan_tags 下的每个元素的键名称都是全部小写的标签键名称，即使要查询的标签具有不同的大小写处理方式也是如此。此标识符不 区分大小写。这些条目中的每一个条目的值都由以下键组成：

  - tag_key – 指定要附加到备份计划的标签键名称。此键包含 @@assign 继承值运算符和一个字符串值。此值区分大小写。
  - tag_value：指定附加到备份计划并与 tag_key 关联的值。此键包含 @@assign 继承值运算符和一个字符串值。此值区分大小写。

备份策略示例

下面的示例备份策略仅供参考。在以下某些示例中，可能会压缩 JSON 空白格式以节省空间。

示例 1：分配给父节点的策略

以下示例显示了分配给账户的父节点之一的备份策略。

父策略 – 此策略可以附加到组织根，或附加到作为所有预期账户父级的任何 OU。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "480"
                    },
```

```
                    "complete_backup_window_minutes": {
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        },
                        "opt_in_to_archive_for_supported_resources": {
                            "@@assign": "false"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
                                }
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
```

```
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
                                }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": {
                                "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                            },
                            "tag_key": {
                                "@@assign": "dataType"
                            },
                            "tag_value": {
                                "@@assign": [
                                    "PII",
                                    "RED"
                                ]
                            }
                        }
                    }
                },
                "advanced_backup_settings": {
                    "ec2": {
                        "windows_vss": {
                            "@@assign": "enabled"
                        }
                    }
                }
            }
        }
}
```

如果账户没有继承或附加其他政策，则每个适用政策中提供的有效政策 Amazon Web Services 账户 如下所示。CRON 表达式会使备份每小时运行一次。账户 ID 123456789012 将是每个账户的实际账户 ID。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "delete_after_days": "28",
```

```
                                "move_to_cold_storage_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": "enabled"
                }
            }
        }
    }
}
```

示例 2：父策略与子策略合并

在以下示例中，继承的父级策略和子级策略继承或直接附加到 Amazon Web Services 账户 合并以形成有效策略。

父策略 – 此策略可以附加到组织根或任何父 OU。

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
```

```
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "delete_after_days": { "@@assign": "180" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "delete_after_days": { "@@assign": "180" },
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
                            "tag_value": { "@@assign": [ "PII", "RED" ] }
                        }
                    }
                }
            }
        }
}
```

子策略 – 此策略可以直接附加到账户，或附加到父策略所附加到的级别以下的任何级别的 OU。

```
{
    "plans": {
```

```
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "delete_after_days": { "@@assign": "365" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "delete_after_days": { "@@assign": "365" },
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "MonthlyDatatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                        "tag_key": { "@@assign": "BackupType" },
                        "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                    }
                }
            }
        }
    }
```

```
}
```

生成的有效策略 – 应用于账户的有效策略包含两个计划，每个计划都有自己的规则集以及要应用这些规则的资源集。

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
```

```
                    }
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "delete_after_days": "365",
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "monthlydatatype": {
                        "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                        "tag_key": "BackupType",
                        "tag_value": [ "MONTHLY", "RED" ]
                    }
                }
            }
        }
```

```
    }
}
```

示例 3：父策略阻止子策略进行任何更改

在以下示例中，继承的父策略使用子控制运算符强制执行所有设置，并防止它们被子策略更改或覆盖。

父策略 – 此策略可以附加到组织根或任何父 OU。策略的每个节点都存在 "@@operators_allowed_for_child_policies": ["@@none"] 意味着，子策略不能对计划进行任何类型的更改。子策略也不能将其他计划添加到有效策略。此策略将成为其附加到的每个 OU 以及 OU 下的账户的有效策略。

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
```

```
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        },
                        "opt_in_to_archive_for_supported_resources": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "false"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "delete_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "180"
                                },
                                 "opt_in_to_archive_for_supported_resources": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "false"
                                }
                            }
                        }
                    }
                }
```

```
            },
            "selections": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "tags": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "datatype": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "iam_role_arn": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                },
                "advanced_backup_settings": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "ec2": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "windows_vss": {
                            "@@assign": "enabled",
                            "@@operators_allowed_for_child_policies": ["@@none"]
                        }
                    }
                }
            }
        }
    }
```

生成的有效策略 – 如果存在任何子备份策略，则会忽略这些策略，而父策略将成为有效策略。

```
{
    "plans": {
```

```
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:backup-vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "delete_after_days": "180",
                            "opt_in_to_archive_for_supported_resources": "false"
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
    }
```

```
}
```

示例 4：父策略阻止子策略对一个备份计划进行更改

在以下示例中，继承的父策略使用子控制运算符强制执行单个计划的设置，并防止它们被子策略更改或覆盖。子策略仍然可以添加其他计划。

父策略 – 此策略可以附加到组织根或任何父 OU。此示例与前一个示例类似，所有子继承运算符都被阻止，但 plans 顶级处除外。该级别的 @@append 设置使子策略能够将其他计划添加到有效策略中的集合。对继承计划的任何更改仍被阻止。

为清楚起见，截断了计划中的相应部分。

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        }
    }
}
```

子策略 – 此策略可以直接附加到账户，或附加到父策略所附加到的级别以下的任何级别的 OU。此子策略定义一个新计划。

为清楚起见，截断了计划中的相应部分。

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

生成的有效策略 – 有效策略包括这两个计划。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

示例 5：子策略覆盖父策略中的设置

在以下示例中，子策略使用值设置运算符来覆盖从父策略继承的某些设置。

父策略 – 此策略可以附加到组织根或任何父 OU。子策略可以覆盖任何设置，因为在没有阻止子策略的子控制运算符的情况下，默认行为是允许子策略执行 @@assign、@@append 或 @@remove。父策略包含有效备份计划所需的所有元素，因此，如果它按原样继承，则会成功备份您的资源。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "lifecycle": {
                        "delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
```

```
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "delete_after_days": {"@@assign": "180"},
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
    }
}
```

子策略 – 子策略仅包含需要与继承的父策略不同的设置。必须有一个继承的父策略，该策略在合并到有效策略时提供其他所需设置。否则，有效备份策略会包含无效的备份计划，无法按预期备份您的资源。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
```

```
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "delete_after_days": {"@@assign": "365"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    }
                }
            }
        }
    }
}
```

生成的有效策略 – 有效策略包括来自这两个策略的设置，由子策略提供的设置将覆盖从父级继承的设置。在此示例中，将发生以下更改：

- 区域列表替换为完全不同的列表。如果要将区域添加到继承的列表中，请在子策略中使用 @@append 而不是 @@assign。
- Amazon Backup 每隔一小时执行一次，而不是每小时执行一次。
- Amazon Backup 允许开始备份的时间为 80 分钟，而不是 60 分钟。
- Amazon Backup 使用保Default管库而不是FortKnox。
- 向冷存储转移和最终删除备份的生命周期都会延长。

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
```

```
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": "false"

                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

标签策略

标签策略允许您标准化附加到组织账户中 Amazon 资源的标签。

您可以使用标签策略来维护一致的标签，包括标签键和标签值的首选大小写处理。

标签是什么？

标签是您分配或 Amazon 分配给 Amazon 资源的自定义属性标签。每个标签具有两个部分：

- 标签键（例如，CostCenter、Environment 或 Project）。标签键区分大小写。
- 一个称为标签值 的可选字段（例如，111122223333 或 Production）。省略标签值与使用空字符串效果相同。与标签键一样，标签值区分大小写。

本页的其余部分描述了标签策略。有关标签的更多信息，请参阅以下资源：

- 有关标签的一般信息，包括命名和使用惯例，请参阅《标记 Amazon 资源用户指南》。
- 有关支持使用标签的服务列表，请参阅 Res ource Groups 标记API参考。
- 有关使用标签对资源进行分类的信息，请参阅《标记 Amazon 资源的最佳实践》白皮书。
- 有关标记 Organizations 资源的信息，请参阅为资源添加标签 Amazon Organizations。
- 有关为其他资源添加标签的信息 Amazon Web Services 服务，请参阅该服务的文档。

什么是标签策略？

标签策略 是策略的一种类型，可帮助您在组织账户中跨资源标准化标签。在标签策略中，您可以指定在标记资源时适用于资源的标记规则。

例如，标签策略可以指定当 CostCenter 标签附加到资源时，它必须使用标签策略定义的大小写处理和标签值。标签策略还可以指定在指定资源类型上强制执行 不合规的标记操作。换句话说，阻止在指定的资源类型上完成不合规的标记操作。不会评估未标记的资源或未在标签策略中定义的标签是否符合标签策略。

使用标签策略涉及使用多个 Amazon Web Services 服务：

- 使用 Amazon Organizations 管理标签策略。登录到组织的管理账户时，您可以使用 Organizations 启用标签策略功能。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。然后，您可以创建标签策略并将其附加到组织实体，以使这些标记规则生效。
- 使用 Amazon Resource Groups 管理与标签策略的合规性。登录组织中的账户时，您可以使用 Resource Groups 查找账户中资源的不合规标签。您可以在创建资源的 Amazon 服务中更正不合规的标签。您还可以使用标签编辑器和 Resource Groups 标签API来标记和取消标记来自多个服务的资源。

如果您登录组织的管理账户，则可以查看组织所有账户的合规性信息。

标签策略仅在启用所有功能的组织中可用。有关使用标签策略所需条件的更多信息，请参阅的管理策略的先决条件和权限 Amazon Organizations。

> **Important**
>
> 要开始使用标签策略， Amazon 强烈建议您先按照中所述的示例工作流程进行操作，标签策略入门然后再继续使用更高级的标签策略。在将标签策略扩展到整个 OU 或组织之前，最好了解将一个简单标签策略附加到单个账户的效果。在强制实施 与任何标签策略的合规性之前，了解某个标签策略的影响尤为重要。标签策略入门页面上的表还提供了更多高级策略相关任务的说明的链接。

使用标签策略的最佳实践

Amazon 推荐使用标签策略的以下最佳实践。

确立标签大小写策略

确定您希望如何设定标签的大小写并在所有资源类型中一致地实施该策略。例如，决定是使用 `Costcenter`、`costcenter` 还是 `CostCenter`，以及是否对所有标签使用相同的约定。为了在合规性报告中获得一致的结果，请避免使用具有不一致大小写处理的类似标签。此策略将帮助您定义组织的标签策略。

使用推荐的工作流程

从小事开始做，创建一个简单的标签策略。然后将其附加到用于测试用途的会员账户。使用标签策略入门中描述的工作流。

确定标记规则

这将取决于您组织的需求。例如，您可能需要指定将`CostCenter`标签附加到 Amazon Secrets Manager 密钥时，它必须使用指定的大小写处理。创建定义合规标签的标签策略，并将其附加到希望这些标记规则生效的组织实体。

培训账户管理员

当您准备扩展标签策略的使用时，请按照以下方式对账户管理员进行培训：

- 沟通您的标签策略。
- 强调管理员需要对特定资源类型使用标签。

  这一点很重要，因为未标记的资源在合规性结果中不会显示为不合规。
- 提供有关使用标签策略检查合规性的指导。指导管理员使用《标记资源用户指南》中评估账户合规性中描述的步骤查找和更正其账户中 Amazon 资源上的不合规标签。告知他们您希望的合规性检查频率。

在强制执行合规性时要谨慎

强制执行合规性可能会阻止组织账户中的用户标记他们所需的资源。查看了解强制执行中的信息。另请参阅标签策略入门中描述的工作流。

考虑围绕资源创建SCP请求设置防护栏

从未附加标签的资源在报告中不会显示为不合规。账户管理员仍然可以创建未标记的资源。在某些情况下，您可以使用服务控制策略 (SCP) 来围绕资源创建请求设置防护栏。有关示例SCP，请参阅 需要在指定的已创建资源上使用标签。

要了解某项 Amazon 服务是否支持使用标签控制访问权限，请参阅Amazon Web Services 服务 《IAM 用户指南》IAM中的 Th a t with with。在 ABAC（基于标签的授权）列中查找标有 “是” 的服务。选择服务名称以查看该服务的授权和访问控制文档。

标签策略入门

使用标签策略涉及使用多个 Amazon Web Services 服务。要开始使用，请查看以下页面。然后按照此页面上的工作流来熟悉标签策略及其效果。

- 的管理策略的先决条件和权限 Amazon Organizations
- 使用标签策略的最佳实践

首次使用标签策略

首次使用标签策略时，请按照以下步骤开始。

任务	要登录的账户	要使用的 Amazon 服务控制台
步骤 1：为您的组织启用标签策略。	组织的管理账户。[1]	Amazon Organizations

任务	要登录的账户	要使用的 Amazon 服务控制台
步骤 2：创建标签策略。 保持第一个标签策略简单。输入您要使用的一个大小写处理标签键，并将所有其他选项保留为默认值。	组织的管理账户。[1]	Amazon Organizations
步骤 3：将标签策略附加到可用于测试的单个成员账户。 在下一步中您需要登录此账户。	组织的管理账户。[1]	Amazon Organizations
步骤 4：创建一些具有合规标签的资源，以及一些具有不合规标签的资源。	您用于测试目的的成员账户。	您想使用的任何 Amazon 服务。例如，您可以使用 Amazon Secrets Manager 并按照创建基本密钥中的过程创建具有合规和不合规密钥的密钥。
步骤 5：查看有效标签策略并评估账户的合规性状态。	您用于测试目的的成员账户。	创建了资源的 Resource Groups 和Amazon服务。 如果您创建了具有合规和不合规标签的资源，则应在结果中看到不合规标签。
步骤 6：重复查找和纠正合规性问题的过程，直到测试账户中的资源均符合标签策略。	您用于测试目的的成员账户。	创建了资源的 Resource Groups 和Amazon服务。
您可以随时评估组织级的合规性。	组织的管理账户。[1]	资源组

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

扩大标签策略的使用

您可以按任意顺序执行以下任务以扩展标签策略的使用范围。

高级任务	要登录的账户	要使用的 Amazon 服务控制台
创建更多高级标签策略。 遵循与初次用户相同的流程，但尝试其他任务。例如，定义其他键或值，或为标签键指定不同的大小写处理。 您可以使用了解管理策略继承和标签策略语法中的信息创建更详细的标签策略。	组织的管理账户。[1]	Amazon Organizations
将标签策略附加到其他账户或 OU。 在将更多策略附加到账户或账户是其成员的任何 OU 之后，检查账户的有效标签策略。	组织的管理账户。[1]	Amazon Organizations
创建 SCP，以便在任何人创建新资源时要求标签。有关示例，请参阅 需要在指定的已创建资源上使用标签。	组织的管理账户。[1]	Amazon Organizations
当账户更改时，继续根据有效标签策略评估账户的合规性状态。更正不合规标签。	具有有效标签策略的成员账户。	创建了资源的 Resource Groups 和Amazon服务。
评估组织级的合规性。	组织的管理账户。[1]	资源组

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

首次强制执行标签策略

要首次强制执行标签策略，请遵循类似于首次使用标签策略使用测试账户的工作流。

> **Warning**
>
> 在强制执行合规性时要谨慎。请确保您了解使用标签策略的效果并遵循推荐的工作流。在将强制执行扩展到更多账户之前，在测试账户中测试强制执行的影响。否则，您可能会阻止组织账户中的用户标记他们所需的资源。有关更多信息，请参阅 了解强制执行。

强制执行任务	要登录的账户	要使用的 Amazon 服务控制台
步骤 1：创建标签策略。 保持第一个强制执行的标签策略简单。输入您要使用的一个大小写处理标签键，然后选择 Prevent noncompliant operations for this tag (防止此标签的不合规操作) 选项。然后指定要在其上强制执行的资源类型。继续我们之前的例子，您可以选择在 Secrets Manager 密钥上强制执行它。	组织的管理账户。[1]	Amazon Organizations
步骤 2：将标签策略附加到单个测试账户。	组织的管理账户。[1]	Amazon Organizations
步骤 3：尝试创建一些具有合规标签的资源，一些具有不合规标签的资源。不允许在标签策略中指定的带有不兼容标签类型的资源上创建标签。	您用于测试目的的成员账户。	您想使用的任何 Amazon 服务。例如，您可以使用 Amazon Secrets Manager 并按照创建基本密钥中的过程创建具有合规和不合规密钥的密钥。

强制执行任务	要登录的账户	要使用的 Amazon 服务控制台
步骤 4：根据有效标签策略评估账户的合规性状态，并更正不合规的标签。	您用于测试目的的成员账户。	创建了资源的 Resource Groups 和Amazon服务。
步骤 5：重复查找和纠正合规性问题的过程，直到测试账户中的资源均符合标签策略。	您用于测试目的的成员账户。	创建了资源的 Resource Groups 和Amazon服务。
您可以随时评估组织级的合规性。	组织的管理账户。[1]	资源组

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

使用 Amazon EventBridge 监控不合规标签

您可以使用 Amazon EventBridge（之前称为 Amazon CloudWatch Events）监控何时引入了不合规标签。在以下示例事件中，`tag-policy-compliant` 的 `"false"` 值表示新标签不符合有效标签策略。

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
  }
```

```
}
```

您可以订阅事件并指定要监控的字符串或模式。有关 EventBridge 的详细信息，请参阅《Amazon EventBridge 用户指南》。

了解强制执行

标签策略可以指定在指定资源类型上强制执行 不合规的标记操作。换句话说，阻止在指定的资源类型上完成不合规的标记操作。

> **Important**
>
> 强制执行不会对创建时不带标签的资源造成影响。

要强制遵守标签策略，请在创建标签策略时执行以下操作之一：

- 从 Visual editor (可视化编辑器) 选项卡中，选择 Prevent noncompliant operations for this tag (防止此标签的不合规操作)。
- 在 JSON 选项卡中，使用 `enforced_for` 字段。有关标签策略语法的信息，请参阅标签策略语法和示例。

在对标签策略强制执行合规性时，请遵循以下最佳实践：

- 请谨慎强制执行合规性 – 确保您了解使用标签策略的影响，并遵循标签策略入门中推荐的工作流。在将强制执行扩展到更多账户之前，在测试账户中测试强制执行的影响。否则，您可能会阻止组织账户中的用户标记他们所需的资源。
- 了解可以对哪些资源类型强制执行 – 您只能对支持资源类型上的标签策略强制执行合规性。当您使用可视化编辑器构建标签策略时，将列出支持强制执行合规性的资源类型。
- 了解与某些服务的交互 — 有些服务 Amazon Web Services 服务 具有类似容器的资源分组，可以自动为您创建资源，标签可以从一项服务中的资源传播到另一项服务。例如，Amazon A EC2 uto Scaling 群组和 Amazon EMR 集群上的标签可以自动传播到包含的亚马逊实例。 EC2 您对亚马逊 EC2 的标签政策可能比 Auto Scaling 群组或 EMR 集群的标签政策更为严格。如果您启用强制执行，则标签策略会阻止对标记资源，并可能会阻止动态扩展和预配置。

以下各部门介绍如何查找不符合要求的资源，以及如何将其更正为合规。

主题

- 为账户查找不合规的资源 Amazon Organizations
- 使用更正资源中的不合规标签 Amazon Organizations
- 生成组织范围的合规报告 Amazon Organizations
- 支持强制执行的服务和资源类型

为账户查找不合规的资源 Amazon Organizations

对于每个账户，您可以获取有关不合规资源的信息。您应该从账户拥有资源的每个区域运行此命令。

要查找具有标签策略的账户的不合规资源，请运行以下命令将结果保存到文件中：

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

使用更正资源中的不合规标签 Amazon Organizations

找到不符合标签后，请使用以下任意方法进行更正。您必须登录到具有不合规标签的资源的账户：

- 使用创建不合规资源的 Amazon 服务的控制台或标记 API 操作。
- 使用 Amazon Resource Groups TagResources和UntagResources操作添加符合有效策略的标签或删除不合规的标签。

生成组织范围的合规报告 Amazon Organizations

您可以随时生成一份报告，列出 Amazon Web Services 账户 整个组织中所有已标记的资源。报告显示每个资源是否符合有效标签策略。请注意，您对标签策略或资源所做的更改，最多可能需要 48 小时才能反映在组织范围内的合规性报告中。例如，假定您有一个标签策略，为某个资源类型定义新的标准化标签。没有此标签的该类型的资源最多需要 48 小时在报告中显示为合规。

您可以从 us-east-1 区域中的组织管理账户生成报告，前提是该账户具有对 Amazon S3 存储桶的访问权限。存储桶必须具有附加的存储桶策略，如用于存储报告的 Amazon S3 存储桶策略中所示。若要生成报告，请运行以下命令：

```
$ aws resourcegroupstaggingapi start-report-creation --region us-east-1
```

您一次可以生成一个报告。

完成报告可能需要一些时间。您可以通过运行以下命令来检查状态：

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

当上述命令返回 SUCCEEDED 时，您可以从 Amazon S3 存储桶打开报告。

支持强制执行的服务和资源类型

以下服务和资源类型支持使用标签策略强制执行：

服务名称	资源类型	JSON 语法
Amazon API Gateway	• API 密钥 • 域名 • REST API 操作 • 阶段	• "apigateway:apikeys" • "apigateway:domainnames" • "apigateway:restapis" • "apigateway:restapis/stages"
Amazon Amplify	• 组件 • 主题	• "amplifyuibuilder:app/environment/components" • "amplifyuibuilder:app/environment/themes"
Amazon AppConfig	• 应用程序 • 配置文件 • 部署 • 部署策略 • 环境	• "appconfig:application" • "appconfig:application/configurationprofile" • "appconfig:application/environment/deployment" • "appconfig:deploymentstrategy" • "appconfig:application/environment"
Amazon App Mesh	• 全部 • 网关路由 • Mesh • 路线	• "appmesh:*" • "appmesh:mesh/virtualGateway/gatewayRoute" • "appmesh:mesh"

服务名称	资源类型	JSON 语法
	• 虚拟网关 • 虚拟节点 • 虚拟路由器 • 虚拟服务	• "appmesh:mesh/virtualRouter/route" • "appmesh:mesh/virtualGateway" • "appmesh:mesh/virtualNode" • "appmesh:mesh/virtualRouter" • "appmesh:mesh/virtualService"
Amazon Athena	• 全部 • 工作组	• "athena:*" • "athena:workgroup"
Amazon Audit Manager	• 评测 • 评估框架 • 控件	• "auditmanager:assessment " • "auditmanager:assessmentFramework " • "auditmanager:control "
Amazon Backup	• 备份计划 • 文件库 • Gateway • Hyper Visor • VM	• "backup:backup-plan" • "backup:backup-vault" • "backup-gateway:gateway" • "backup-gateway:hypervisor" • "backup-gateway:vm"
Amazon Batch	• 作业 • 作业定义 • 作业队列	• "batch:job" • "batch:job-definition" • "batch:job-queue"
Amazon BugBust	• 事件	• "bugbust:event"
Amazon Certificate Manager	• 全部 • 证书 • Private Certificate Authority	• "acm:*" • "acm:certificate" • "acm-pca:certificate-authority"

服务名称	资源类型	JSON 语法
Amazon Chime	• 应用程序实例 • 频道 • 媒体管线 • 会议 • SIP 媒体应用程序 • 用户应用程序实例 • 语音连接器	• "chime:app-instance" • "chime:app-instance/channel" • "chime:media-pipeline" • "chime:meeting" • "chime:sma" • "chime:app-instance/user" • "chime:vc"
Amazon Clean Rooms	• 协作 • 已配置的表 • 成员资格 • 已配置的表关联	• "cleanrooms:collaboration" • "cleanrooms:configuredtable" • "cleanrooms:membership" • "cleanrooms:membership/configuredtableassociation"
Amazon Cloud9	• 环境	• "cloud9:environment"
Amazon CloudFront	• 全部 • 分配	• "cloudfront:*" • "cloudfront:distribution"
Amazon CloudTrail	• 全部 • 试用	• "cloudtrail:*" • "cloudtrail:trail"
Amazon CloudWatch	• 全部 • 警报 • Contributor Insights 规则 • 指标流	• "cloudwatch:*" • "cloudwatch:alarm" • "cloudwatch:insight-rule" • "cloudwatch:metric-stream"
Amazon CloudWatch 互联网监视器	• 监控	• "internetmonitor:monitor"
Amazon CloudWatch 日志	• 目标 • 日志组	• "logs:destination" • "logs:log-group"

服务名称	资源类型	JSON 语法
Amazon CloudWatch 可观察性访问管理器	• 链接 • sink	• "oam:link" • "oam:sink"
Amazon CodeBuild	• 全部 • Project	• "codebuild:*" • "codebuild:project"
Amazon CodeCatalyst	• 连接	• "codecatalyst:connections"
Amazon CodeCommit	• 全部 • 存储库	• "codecommit:*" • "codecommit:repository"
Amazon CodePipeline	• 全部 • 操作类型 • 管道 • Webhook	• "codepipeline:*" • "codepipeline:actiontype" • "codepipeline:pipeline" • "codepipeline:webhook"
Amazon Cognito Identity	• 全部 • 身份池	• "cognito-identity:*" • "cognito-identity:identitypool"
Amazon Cognito 用户群体	• 全部 • 用户群体	• "cognito-idp:*" • "cognito-idp:userpool"
Amazon Comprehend	• 全部 • 文档分类器 • 实体识别程序	• "comprehend:*" • "comprehend:document-classifier" • "comprehend:entity-recognizer"
Amazon Config	• 全部 • 聚合授权 • Config 聚合器 • Config 规则	• "config:*" • "config:aggregation-authorization" • "config:config-aggregator" • "config:config-rule"

服务名称	资源类型	JSON 语法
Amazon CodeGuru Reviewer	• 关联	• "codeguru-reviewer:association"
Amazon CodeGuru 安全	• Scan	• "codeguru-security:scans"
CodeConnections	• Connection • Host	• "codestar-connections:connection" • "codestar-connections:host"
Amazon Connect	• 接洽流程 • 集成关联 • 队列 • Quick Connect • 路由配置文件 • User	• "connect:instance/contact-flow" • "connect:instance/integration-association" • "connect:instance/queue" • "connect:instance/transfer-destination" • "connect:instance/routing-profile" • "connect:instance/agent"
Amazon Connect Wisdom	• Assistant • 关联 • 内容 • 知识库 • 会话	• "wisdom:assistant" • "wisdom:association" • "wisdom:content" • "wisdom:knowledge-base" • "wisdom:session"

服务名称	资源类型	JSON 语法
Amazon Database Migration Service	• 全部 • 终端节点 • ES • Rep • Subgrp • Task	• "dms:*" • "dms:endpoint" • "dms:es" • "dms:rep" • "dms:subgrp" • "dms:task"
Amazon Data Lifecycle Manager	• 策略	• "dlm:policy"
Amazon Direct Connect	• 全部 • Dxcon • Dxlag • Dxvif	• "directconnect:*" • "directconnect:dxcon" • "directconnect:dxlag" • "directconnect:dxvif"
Amazon DynamoDB	• 全部 • 表	• "dynamodb:*" • "dynamodb:table"

服务名称	资源类型	JSON 语法
Amazon EC2	• 容量预留 • 容量预留实例集 • 运营商网关 • Client VPN 端点 • CoIP 池 • 客户网关 • 专属主机 • DHCP 选项 • 仅出口互联网网关 • 弹性 IP • 事件窗口 • 导出映像任务 • 导出实例任务 • 实例集 • FPGA 映像 • 主机预留 • 图像 • 导入映像任务 • 导入快照任务 • 实例 • 实例连接终端节点 • 互联网网关 • IP 地址管理器 • IP 地址管理器外部资源验证令牌 • IP 地址管理器池 • IP 地址管理器资源发现	• "ec2:capacity-reservation" • "ec2:capacity-reservation-fleet" • "ec2:carrier-gateway" • "ec2:client-vpn-endpoint" • "ec2:coip-pool" • "ec2:customer-gateway" • "ec2:dedicated-host" • "ec2:dhcp-options" • "ec2:egress-only-internet-gateway" • "ec2:elastic-ip" • "ec2:instance-event-window" • "ec2:export-image-task" • "ec2:export-instance-task" • "ec2:fleet" • "ec2:fpga-image" • "ec2:host-reservation" • "ec2:image" • "ec2:import-image-task" • "ec2:import-snapshot-task" • "ec2:instance" • "ec2:instance-connect-endpoint" • "ec2:internet-gateway" • "ec2:ipam" • "ec2:ipam-external-resource-verification-token" • "ec2:ipam-pool"

服务名称	资源类型	JSON 语法
	• IP 地址管理器资源发现协会 • IP 地址管理器范围 • IPv4 泳池 • 密钥对 • 启动模板 • 本地网关路由表 • 本地网关路由表虚拟接口组关联 • 本地网关路由表 VPC 关联 • NAT 网关 • 网络 ACL • 网络接口 • Network Insights 访问范围 • Network Insights 访问范围分析 • Network Insights 分析 • Network Insights 路径 • 置放群组 • 前缀列表 • 替换根卷任务 • 预留实例 • 路由表 • 安全组 • 快照 • 竞价型实例集请求 • 竞价型实例请求	• "ec2:ipam-resource-discovery" • "ec2:ipam-resource-discovery-association" • "ec2:ipam-scope" • "ec2:ipv4pool-ec2" • "ec2:key-pair" • "ec2:launch-template" • "ec2:local-gateway-route-table" • "ec2:local-gateway-route-table-virtual-interface-group-association" • "ec2:local-gateway-route-table-vpc-association" • "ec2:natgateway" • "ec2:network-acl" • "ec2:network-interface" • "ec2:network-insights-access-scope" • "ec2:network-insights-access-scope-analysis" • "ec2:network-insights-analysis" • "ec2:network-insights-path" • "ec2:placement-group" • "ec2:prefix-list" • "ec2:replace-root-volume-task" • "ec2:reserved-instances" • "ec2:route-table" • "ec2:security-group"

服务名称	资源类型	JSON 语法
	• 子网 • 子网 CIDR 预留 • 流量镜像筛选 • 流量镜像会话 • 流量镜像目标 • Transit Gateway • 中转网关连接 • 中转网关对等连接 • 中转网关组播域 • 中转网关策略表 • 中转网关路由表 • 中转网关路由表公告 • Verified Access 端点 • Verified Access 组 • Verified Access 实例 • Verified Access 可信提供商 • Volume • VPC 流日志 • VPC • VPC 端点 • VPC 终端节点服务 • VPC 对等连接 • VPN 连接 • VPN 网关	• "ec2:snapshot" • "ec2:spot-fleet-request" • "ec2:spot-instances-request" • "ec2:subnet" • "ec2:subnet-cidr-reservation" • "ec2:traffic-mirror-filter" • "ec2:traffic-mirror-session" • "ec2:traffic-mirror-target" • "ec2:transit-gateway" • "ec2:transit-gateway-attachment" • "ec2:transit-gateway-connect-peer" • "ec2:transit-gateway-multicast-domain" • "ec2:transit-gateway-policy-table" • "ec2:transit-gateway-route-table" • "ec2:transit-gateway-route-table-announcement" • "ec2:verified-access-endpoint" • "ec2:verified-access-group" • "ec2:verified-access-instance" • "ec2:verified-access-trust-provider" • "ec2:volume" • "ec2:vpc-flow-log" • "ec2:vpc" • "ec2:vpc-endpoint"

服务名称	资源类型	JSON 语法
		• "ec2:vpc-endpoint-service" • "ec2:vpc-peering-connection" • "ec2:vpn-connection" • "ec2:vpn-gateway"
亚马逊 EC2 回收站	• 规则	• "rbin:rule"
Amazon Elastic Beanstalk	• 应用程序 • 应用程序版本 • 配置模板 • 平台	• "elasticbeanstalk:application" • "elasticbeanstalk:applicationversion" • "elasticbeanstalk:configurationtemplate" • "elasticbeanstalk:platform"
Amazon Elastic Container Registry	• 存储库	• "ecr:repository"
Amazon Elastic Container Service	• 容量提供程序 • 集群 • 服务 • 任务定义 • 任务集	• "ecs:capacity-provider" • "ecs:cluster" • "ecs:service" • "ecs:task-definition" • "ecs:task-set"
Amazon Elastic File System	• 全部 • 文件系统	• "elasticfilesystem:*" • "elasticfilesystem:file-system"
Amazon Elastic Kubernetes Service	• 集群	• "eks:cluster"
Amazon Elastic Search	• 域	• "es:domain"

服务名称	资源类型	JSON 语法
Amazon EMR	• 集群 • Editor	• "elasticmapreduce:cluster" • "elasticmapreduce:editor"
Amazon EMR Serverless	• 应用程序	• "emr-serverless:applications"
Amazon 实体分辨率	• 匹配流程 • 架构映射	• "entityresolution:matchingworkflow" • "entityresolution:schemamapping"
Amazon ElastiCache	• 集群	• "elasticache:cluster"
Amazon EventBridge	• 全部 • 事件总线 • 规则	• "events:*" • "events:event-bus" • "events:rule"
亚马逊 Pi EventBridge pes	• Pipe	• "pipes:pipe"
Amazon EventBridge 日程安排	• 计划组	• "scheduler:schedule-group"
Amazon Fraud Detector	• 检测器 • 探测器版本 • 模型 • 规则 • 变量	• "frauddetector:detector" • "frauddetector:detector-version" • "frauddetector:model" • "frauddetector:rule" • "frauddetector:variable"
Amazon Global Accelerator	• Accelerator	• "globalaccelerator:accelerator"

服务名称	资源类型	JSON 语法
Elastic Load Balancing	• 全部 • Listener • 侦听器规则 • 负载均衡器 • 目标组	• "elasticloadbalancing:*" • "elasticloadbalancing:listener" • "elasticloadbalancing:listener-rule" • "elasticloadbalancing:loadbalancer" • "elasticloadbalancing:targetgroup"
Amazon FSx	• 全部 • 备份 • 文件系统	• "fsx:*" • "fsx:backup" • "fsx:file-system"
Amazon GuardDuty	• 检测器 • 筛选条件 • IP 集 • 威胁情报集	• "guardduty:detector" • "guardduty:detector/filter" • "guardduty:detector/ipset" • "guardduty:detector/threatintelset"
Amazon HealthLake	• 数据存储	• "healthlake:datastore "

服务名称	资源类型	JSON 语法
Amazon HealthOmics	• 注释存储 • 注释存储版本 • 参考存储 • 参考 • 运行 • 运行组 • 序列存储 • 读取集 • 变体存储 • 工作流	• "omics:annotationStore" • "omics:annotationStore/version" • "omics:referenceStore" • "omics:referenceStore/reference" • "omics:run" • "omics:runGroup" • "omics:sequenceStore" • "omics:sequenceStore/readSet" • "omics:variantStore" • "omics:workflow"
Amazon Inspector	• 筛选条件	• "inspector2:filter "
Amazon Identity and Access Management	• 实例配置文件 • MFA • OIDC 提供商 • 策略 • SAML 提供商 • 服务器证书	• "iam:instance-profile" • "iam:mfa" • "iam:oidc-provider" • "iam:policy" • "iam:saml-provider" • "iam:server-certificate"
Amazon IoT Analytics	• 全部 • 频道 • 数据集 • 数据存储 • 管道	• "iotanalytics:*" • "iotanalytics:channel" • "iotanalytics:dataset" • "iotanalytics:datastore" • "iotanalytics:pipeline"
Amazon IoT Events	• 全部 • 探测器模型 • 输入	• "iotevents:*" • "iotevents:detectorModel" • "iotevents:input"

服务名称	资源类型	JSON 语法
Amazon IoT Fleet Hub	• 应用程序	• "iotfleethub:application"
Amazon IoT SiteWise	• 资产 • 资产模型	• "iotsitewise:asset" • "iotsitewise:asset-model "
Amazon IoT Greengrass	• 批量部署 • 连接器定义 • 内核定义 • 设备定义 • 功能定义 • 记录器定义 • 资源定义 • 订阅定义	• "greengrass:bulk" • "greengrass:connectorsDefinition" • "greengrass:coresDefinition" • "greengrass:devicesDefinition" • "greengrass:functionsDefinition" • "greengrass:loggersDefinition" • "greengrass:resourcesDefinition" • "greengrass:subscriptionsDefinition"
Amazon Key Management Service	• 全部 • 键	• "kms:*" • "kms:key"
Amazon Kinesis	• 全部 • 应用程序	• "kinesisanalytics:*" • "kinesisanalytics:application"
Amazon Data Firehose	• 全部 • 传输流	• "firehose:*" • "firehose:deliverystream"
Amazon Lambda	• 全部 • 函数	• "lambda:*" • "lambda:function"
Amazon Macie	• 自定义数据标识符	• "macie2:custom-data-identifier"

服务名称	资源类型	JSON 语法
Amazon MediaStore	• 容器	• "mediastore:container"
Amazon MQ	• 代理 • 配置	• "mq:broker" • "mq:configuration"
Amazon Network Firewall	• 防火墙 • 防火墙策略 • 有状态规则组 • 无状态规则组	• "network-firewall:firewall" • "network-firewall:firewall-policy" • "network-firewall:stateful-rulegroup" • "network-firewall:stateless-rulegroup"
Amazon OpenSearch 无服务器	• 集合	• "aoss:collection"
Amazon Organizations	• Account • 组织部门 • 策略 • 根	• "organizations:account" • "organizations:ou" • "organizations:policy" • "organizations:root"
Amazon Pinpoint SMS Voice V2	• 配置集 • 退订列表 • 电话号码 • 池 • 发件人 ID	• "sms-voice:configuration-set" • "sms-voice:opt-out-list" • "sms-voice:phone-number" • "sms-voice:pool" • "sms-voice:sender-id"

服务名称	资源类型	JSON 语法
Amazon RDS	• 集群参数组 • 集群端点 • 事件订阅 • 数据库选项组 • 数据库参数组 • 数据库代理 • 数据库代理端点 • 预留数据库实例 • 数据库安全组 • DB subnet group（数据库子网组） • 目标组	• "rds:cluster-pg" • "rds:cluster-endpoint" • "rds:es" • "rds:og" • "rds:pg" • "rds:db-proxy" • "rds:db-proxy-endpoint" • "rds:ri" • "rds:secgrp" • "rds:subgrp" • "rds:target-group"
Amazon Redshift	• 全部 • 集群 • 事件订阅 • HSM 客户端证书 • HSM 配置 • 参数组 • 快照 • 快照复制授权 • 快照计划 • 子网组	• "redshift:*" • "redshift:cluster" • "redshift:eventsubscription" • "redshift:hsmclientcertificate" • "redshift:hsmconfiguration" • "redshift:parametergroup" • "redshift:snapshot" • "redshift:snapshotcopygrant" • "redshift:snapshotschedule" • "redshift:subnetgroup"
Amazon Redshift Serverless	• 命名空间 • 工作组	• "redshift-serverless:namespace" • "redshift-serverless:workgroup"

服务名称	资源类型	JSON 语法
Amazon Resource Access Manager	• 全部 • 资源共享	• "ram:*" • "ram:resource-share"
Amazon Resource Groups	• 全部 • 组	• "resource-groups:*" • "resource-groups:group"
Amazon Route 53	• 托管区域	• "route53:hostedzone"
Amazon Route 53 Resolver	• 全部 • 解析程序终端节点 • 解析程序规则	• "route53resolver:*" • "route53resolver:resolver-endpoint" • "route53resolver:resolver-rule"
Amazon S3	• 存储桶 • Storage Lens • Storage Lens 组	• "s3:bucket" • "s3:storage-lens" • "s3:storage-lens-group"
亚马逊 SageMaker AI	• App Image Config • Artifact • 上下文 • 训练作业 • 处理任务 • 模型包组 • 人工任务 UI • 模型包 • 操作 • 管道 • 试验 • 流定义 • Project	• "sagemaker:app-image-config" • "sagemaker:artifact" • "sagemaker:context" • "sagemaker:training-job" • "sagemaker:processing-job " • "sagemaker:model-package-group" • "sagemaker:human-task-ui" • "sagemaker:model-package" • "sagemaker:action" • "sagemaker:pipeline" • "sagemaker:experiment" • "sagemaker:flow-definition" • "sagemaker:project"

服务名称	资源类型	JSON 语法
Amazon Secrets Manager	• 全部 • 密钥	• "secretsmanager:*" • "secretsmanager:secret"
Amazon 安全湖	• 数据湖 • 订阅者	• "securitylake:data-lake" • "securitylake:subscriber"
Amazon Service Catalog	• 应用程序 • 属性组 • Portfolio • 产品	• "servicecatalog:applications" • "servicecatalog:attribute-groups " • "catalog:portfolio " • "catalog:product "
Amazon Simple Notification Service（SNS）	• 主题	• "sns:topic"
Amazon Simple Queue Service (SQS)	• 队列	• "sqs:queue"
Amazon States Language	• 全部 • 活动 • 状态机	• "states:*" • "states:activity " • "states:stateMachine "
Amazon Step Functions	• 活动	• "states:activity"
Amazon Storage Gateway	• 全部 • Gateway • 共享 • 磁带 • Volume	• "storagegateway:*" • "storagegateway:gateway" • "storagegateway:share" • "storagegateway:tape" • "storagegateway:gateway/volume"

服务名称	资源类型	JSON 语法
Amazon Systems Manager	• 关联 • 自动化执行 • 文档 • 维护时段 • 托管实例 • 操作项目 • 补丁基准 • 联系人	• "ssm:association" • "ssm:automation-execution" • "ssm:document" • "ssm:maintenancewindow" • "ssm:managed-instance" • "ssm:opsitem" • "ssm:patchbaseline" • "ssm-contacts:contact"
Amazon Textract	• 适配器 • 版本	• "textract:adapters" • "textract:adapters/versions"
Amazon Transer Family	• 服务器 • User • 工作流	• "transfer:server" • "transfer:user" • "transfer:workflow"
Amazon Well-Arch itected	• 工作负载	• "wellarchitected:workload"
Amazon Wickr	• 网络	• "wickr:network"
Amazon WorkSpaces	• 全部 • 连接别名 • 目录 • WorkSpace • WorkSpaces 捆绑包 • WorkSpaces 图片 • WorkSpaces IP 组	• "workspaces:*" • "workspaces:connectionalias" • "workspaces:directory" • "workspaces:workspace" • "workspaces:workspacebundle" • "workspaces:workspaceimage" • "workspaces:workspaceipgroup"

标签策略语法和示例

本页介绍标签策略语法并提供示例。

标签策略语法

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

以下标签策略显示了基本标签策略语法：

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "100",
                    "200"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:*"
                ]
            }
        }
    }
}
```

标签策略语法包括以下元素：

- tags 字段键名称。标签策略始终以此固定键名开头。它是上面示例策略中的顶行。
- 唯一标识策略语句的策略键。它必须与标签键 的值相匹配，除了大小写处理。与标签键不同（下文将介绍），策略值不区分大小写。

  在此示例中，costcenter 是策略键。
- 至少有一个标签键，指定允许的标签键（具有您希望资源遵循的大小写）。如果未定义大小写处理，则标签键的默认大写处理是小写。标签键的值必须与策略键的值匹配。但是，由于策略键值不区分大小写，所以大小写可以不同。

在此示例中，CostCenter 是标签键。这是符合标签策略要求所需的大小写处理。为此标签键使用其他大小写处理的资源不符合标签策略要求。

您可以在一个标签策略中定义多个标签键。

- （可选）标签键的一个或多个可接受标签值 的列表。如果标签策略没有为标签键指定标签值，则任何值（包括没有值）都将视为合规。

  在此示例中，CostCenter 标签键的可接受值为 100 和 200。

- （可选）一个 enforced_for 选项，指示是否阻止对指定服务和资源执行任何不合规标记操作。在控制台中，这是用于创建标签策略的可视化编辑器中的 Prevent noncompliant operations for this tag (防止此标签的不合规操作) 选项。此选项的默认设置为空。

  示例标签策略指定在所有 Amazon Secrets Manager 资源上传递的 CostCenter 标签必须符合此策略。

  > **Warning**
  >
  > 只有当您具有使用标签策略经验的情况下，才可以更改默认选项。否则，您可能会阻止组织账户中的用户创建他们所需的资源。

- 运算符指定标记策略如何与组织树中的其他标记策略合并，以创建账户的有效标签策略。在此示例中，@@assign 用于将字符串分配给 tag_key、tag_value 和 enforced_for。有关运算符的更多信息，请参阅继承运算符。
- – 您可以在标签值和 enforced_for 字段中使用 * 通配符：
  - 您仅可以为每个标签值使用一个通配符。例如，允许使用 *@example.com，但不允许使用 *@*.com。
  - 对于 enforced_for，您可以将 <service>:* 与某些服务一起使用，为该服务的所有资源启用强制执行。有关支持 enforced_for 的服务和资源类型的列表，请参阅支持强制执行的服务和资源类型。

    您不能使用通配符指定所有服务或指定所有服务的某个资源。

标签策略示例

下面的示例标签策略 仅供参考。

> **Note**
>
> 尝试在组织中使用这些示例标签策略之前，请注意以下事项：
>
> - 确保您已按照推荐的工作流开始使用标签策略。
> - 您应根据您的独特要求仔细查看和自定义这些标签策略。
> - 标签策略中的所有字符都受到最大大小的约束。本指南中的示例演示了使用额外空白编排格式的标签策略，以提高其可读性。但是，要在策略大小接近最大大小时节省空间，您可以删除任何空白。空白的示例包括引号外部的空格字符和换行符。
> - 未标记的资源不会在结果中显示为不合规。

示例 1：定义组织级的标签键大小写

以下示例显示了一个标签策略，该策略仅定义了两个标签键和您希望组织中的账户标准化所采用的大小写。

策略 A – 组织根标签策略

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

此标签策略定义两个标签键：CostCenter 和 Project。将此标签策略附加到组织根具有以下效果：

- 组织中的所有账户继承此标签策略。

- 组织中的所有账户都必须使用定义的大小写处理以实现合规性。具有 CostCenter 和 Project 标签的资源符合要求。为标签键（例如，costcenter、Costcenter 或 COSTCENTER）使用其他大小写处理的资源不符合要求。
- @@operators_allowed_for_child_policies": ["@@none"] 行锁定标签键。附加在组织树（子策略）下方的标签策略不能使用值设置运算符来更改标签键，包括其大小写处理。
- 对于所有标签策略，不会评估未标记的资源或未在标签策略中定义的标签是否符合标签策略。

Amazon 建议您使用此示例作为指南，为要使用的标签键创建类似的标签策略。将其附加到组织根。然后创建类似于下一个示例的标签策略，该策略仅为已定义的标签键定义可接受值。

下一步：定义值

假定您将以前的标签策略附加到组织根。接下来，您可以创建类似于下文的标签策略并将其附加到账户。此策略定义 CostCenter 和 Project 标签键的可接受值。

策略 B – 账户标签策略

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

如果将策略 A 附加到组织根，并将策略 B 附加到账户，则这些策略将合并，以便为该账户创建以下有效标签策略：

策略 A + 策略 B = 账户的有效标签策略

```
{
    "tags": {
        "Project": {
            "tag_value": [
                "A",
                "B"
            ],
            "tag_key": "Project"
        },
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

有关策略继承的更多信息，包括继承运算符的工作原理示例和有效标签策略示例，请参阅[了解管理策略继承](#)。

示例 2：防止使用标签键

要防止使用标签键，您可以将类似以下内容的标签策略附加到组织实体。

此示例策略指定 Color 标签键不接受任何值。它还指定子标签策略中不允许[运算符](#)。因此，受影响账户中的资源上的任何 Color 标签都被视为不符合要求。但是，enforced_for 选项实际上可防止受影响的账户仅使用 Color 标签标记 Amazon DynamoDB 表。

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": [
```

```
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
                "@@assign": [
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

支持的区域

标签策略功能在以下区域中可用：

区域名称	区域参数
美国东部（弗吉尼亚北部）区域[1]	**us-east-1**
美国东部（俄亥俄州）区域	us-east-2
美国西部（北加利福尼亚）区域	us-west-1
美国西部（俄勒冈州）区域	us-west-2
非洲（开普敦）区域[2]	af-south-1
亚太地区（香港）区域[2]	ap-east-1
亚太地区（孟买）区域	ap-south-1
亚太地区（海得拉巴）[2]	ap-south-2
Asia Pacific（Tokyo）Region	ap-northeast-1
亚太地区（首尔）区域	ap-northeast-2
亚太地区（大阪）区域	ap-northeast-3
亚太地区（新加坡）区域	ap-southeast-1

区域名称	区域参数
亚太地区（悉尼）区域	ap-southeast-2
亚太地区（雅加达）区域[2]	ap-southeast-3
亚太地区（马来西亚）区域	ap-southeast-5
亚太地区（墨尔本）[2]	ap-southeast-4
亚太地区（泰国）	ap-southeast-7
加拿大（中部）区域	ca-central-1
加拿大西部（卡尔加里）[2]	ca-west-1
欧洲地区（法兰克福）区域	eu-central-1
欧洲（苏黎世）[2]	eu-central-2
欧洲（米兰）区域[2]	eu-south-1
欧洲（西班牙）[2]	eu-south-2
欧洲地区（爱尔兰）区域	eu-west-1
欧洲地区（伦敦）区域	eu-west-2
欧洲（巴黎）区域	eu-west-3
欧洲地区（斯德哥尔摩）区域	eu-north-1
墨西哥（中部）区域	mx-central-1
中东（巴林）区域[2]	me-south-1
南美洲（圣保罗）区域	sa-east-1
以色列（特拉维夫）[2]	il-central-1

[1]调用以下 Organizations 操作时必须指定 **us-east-1** 区域：

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- 对组织根目录进行的任何其他操作，例如ListRoots。

调用以下作为标签策略功能一部分的 Resource Groups 标记 API 操作时，您也必须指定 **us-east-1** 区域：

- DescribeReportCreation
- GetComplianceSummary
- StartReportCreation

> **Note**
>
> 要评估组织范围的标签策略合规性，您还必须能够访问美国东部（弗吉尼亚北部）区域中的 Amazon S3 存储桶以进行报告存储。有关更多信息，请参阅《标记 Amazon 资源用户指南》中的 Amazon S3 存储桶报告存储策略。

[2] 这些区域必须手动启用。要了解有关启用和禁用 Amazon Web Services 区域的更多信息，请参阅《Amazon 账户管理参考指南》中的 Specify which Amazon Web Services 区域 your account can use。在这些区域中，Resource Groups 控制台不可用。

聊天机器人策略

中的聊天机器人策略 Amazon Organizations 使您可以控制聊天应用程序（例如 Slack 和 Microsoft Teams）对组织帐户的访问权限。

聊天应用程序中的 Amazon Q 开发者版是一项 Amazon 服务 DevOps ，使软件开发团队能够使用消息传递程序聊天室来监视和响应其中的操作事件 Amazon Web Services 云。 聊天应用程序中的 Amazon Q 开发者版 处理来自亚马逊简单通知服务 (AmazonSNS) 的 Amazon Web Services 服务 通知，然后将其转发到聊天室，这样团队就可以随时对其进行分析并采取行动，无论身在何处。

聊天机器人策略的工作原理

使用聊天机器人策略时，组织的管理账户或委派管理员可以在整个组织中执行以下操作：

- 强制可以使用哪些受支持的聊天应用程序（Amazon Chime、Microsoft Teams 和 Slack）。
- 将聊天客户端的访问权限范围限定为具体的工作区（Slack）和团队（Microsoft Teams）。
- 将 Slack 频道的可见性限制为公有或私有频道。
- 设置和强制执行特定的角色设置。

聊天机器人策略会限制并优先于账户级别设置，例如角色设置和频道护栏策略。您可以使用 聊天应用程序中的 Amazon Q 开发者版 控制台或 Organizations 控制台访问和修改聊天机器人策略。

将策略附加到账户和组织单位 (OU) 后，范围内账户的任何当前和未来 聊天应用程序中的 Amazon Q 开发者版 配置都将自动符合治理和权限设置。有关更多信息，请参阅了解管理策略继承。

如果您尝试执行受聊天机器人策略限制的操作，则会显示一条错误消息，通知您由于聊天机器人策略不允许执行该操作，并建议您联系组织的管理账户或委派管理员。

> **Note**
>
> 聊天机器人策略在运行时进行验证。这意味着要持续检查现有资源的合规性。由于目前不支持基于运行时的发送通知或与之交互的IAM权限，因此与现有IAM权限 聊天应用程序中的 Amazon Q 开发者版 没有重叠。

聊天机器人策略入门

请按照以下步骤开始使用聊天机器人策略。

1. 了解执行聊天机器人策略任务所必须具备的权限。
2. 为组织启用聊天机器人策略。
3. 创建聊天机器人策略。
4. 将聊天机器人策略附加到组织根、OU 或账户。
5. 查看应用于账户的合并的有效聊天机器人策略。

在所有这些步骤中，您都需要以IAM用户身份登录、代入IAM角色或以根用户身份登录（不推荐）在组织的管理账户中登录。

其他信息

- 学习聊天机器人策略语法并查看策略示例

聊天机器人策略语法和示例

本页介绍聊天机器人策略语法并提供了示例。

聊天机器人策略的语法

聊天机器人策略是一个纯文本文件，根据 JSON 的规则设置结构。聊天机器人策略的语法遵循管理策略类型的语法。有关该语法的完整讨论，请参阅了解管理策略继承。本主题重点介绍如何使用该常规语法来满足聊天机器人策略类型的特定要求。

以下示例展示了聊天机器人策略的基本语法：

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled" // enabled | disabled
             },
             "workspaces": { // limit 255
                   "@@assign":[
                      "Slack-Workspace-Id"
                   ]
             },
             "default":{
                "supported_channel_types":{
                   "@@assign":[
                      "private" // public | private
                   ]
                },
                "supported_role_settings":{
                   "@@assign":[
                      "user_role" // user_role | channel_role
                   ]
                }
             },
             "overrides":{ // limit 255
                "Slack-Workspace-Id":{
                   "supported_channel_types":{
                      "@@assign":[
                         "public" // public | private
                      ]
                   },
                   "supported_role_settings":{
```

```
                    "@@assign":[
                       "user_role" // user_role | channel_role
                    ]
                 }
              }
           }
        },
        "microsoft_teams":{
           "client":{
              "@@assign":"enabled"
           },
           "tenants":{ // limit 36
              "Microsoft-Teams-Tenant-Id":{ // limit 36
                 "@@assign":[
                    "Microsoft-Teams-Team-Id"
                 ]
              }
           },
           "default":{
              "supported_role_settings":{
                 "@@assign":[
                    "user_role" // user_role | channel_role
                 ]
              }
           },
           "overrides":{ // limit 36
              "Microsoft-Teams-Tenant-Id":{ // limit 36
                 "Microsoft-Teams-Team-Id":{
                    "supported_role_settings":{
                       "@@assign":[
                          "user_role" // user_role | channel_role
                       ]
                    }
                 }
              }
           }
        },
        "chime":{
          "client":{
             "@@assign":"disabled" // enabled | disabled
          }
        }
      },
      "default":{
```

```
            "client":{
               "@@assign":"disabled" // enabled | disabled
            }
         }
      }
   }
```

此聊天机器人策略包含以下元素：

- chatbot 字段键名称。聊天机器人策略始终以此固定键名开头。这是此示例策略中的第一行。
- 在 chatbot 下有一个 platforms 块，其中包含不同受支持聊天应用程序的配置：Slack、Microsoft Teams 和 Amazon Chime。
  - 对于 Slack，有以下字段可用：
    - "client":
      - "enabled"：Slack 客户端已启用。允许 Slack 集成。
      - "disabled"：Slack 客户端已禁用。不允许 Slack 集成。
    - "workspaces"：允许的 Slack 工作区列表，以逗号分隔。在此示例中，允许的 Slack 工作区是 *Slack-Workspace-Id1* 和 *Slack-Workspace-Id2*。
    - "default"：Slack 工作区的默认设置。
      - "supported_channel_types":
        - "public"：默认情况下，范围内的 Slack 工作区会允许公有 Slack 频道。
        - "private"：默认情况下，范围内的 Slack 工作区会允许私有 Slack 频道。
      - supported_role_settings:
        - "user_role": 默认情况下，范围内的 Slack 工作区会允许用户级别的 IAM 角色。
        - "channel_role": 默认情况下，范围内的 Slack 工作区会允许频道级别的 IAM 角色。
    - "overrides"：Slack 工作区的覆盖设置。
      - *Slack-Workspace-Id2*：适用覆盖设置的 Slack 工作区列表，以逗号分隔。在此示例中，该 Slack 工作区为 *Slack-Workspace-Id2*。
        - "supported_channel_types":
          - "public"：覆盖有关范围内的 Slack 工作区是否允许公有 Slack 频道的设置。
          - "private"：覆盖有关范围内的 Slack 工作区是否允许私有 Slack 频道的设置。
        - supported_role_settings:
          - "user_role"：覆盖范围内的 Slack 工作区是否允许用户级别的 IAM 角色的设置。

        - "channel_role"：覆盖范围内的 Slack 工作区是否允许频道级别的 IAM 角色的设置。
  - 对于 Microsoft Teams，有以下字段可用：
    - "client":
      - "enabled"：Microsoft Teams 客户端已启用。允许 Microsoft Teams 集成。
      - "disabled"：Microsoft Teams 客户端已禁用。不允许 Microsoft Teams 集成。
    - "tenants"：允许的 Microsoft Teams 租户列表，以逗号分隔。在此示例中，允许的租户是 *Microsoft-Teams-Tenant-Id*。
      - *Microsoft-Teams-Tenant-Id*：该租户内允许的团队列表，以逗号分隔。在此示例中，允许的团队是 *Microsoft-Teams-Team-Id*。
    - "default"：该租户内团队的默认设置。
      - supported_role_settings:
        - "user_role"：默认情况下，范围内的团队会允许用户级别的 IAM 角色。
        - "channel_role"：默认情况下，范围内的团队会允许频道级别的 IAM 角色。
    - "overrides"：Microsoft Teams 租户的覆盖设置。
      - *Microsoft-Teams-Tenant-Id*：适用覆盖设置的租户列表，以逗号分隔。在此示例中，该租户是 *Microsoft-Teams-Tenant-Id*。
        - *Microsoft-Teams-Team-Id*：该租户内的团队列表，以逗号分隔。在此示例中，允许的团队是 *Microsoft-Teams-Team-Id*。
          - supported_role_settings:
            - "user_role"：覆盖范围内的团队是否允许用户级别的 IAM 角色的设置。
            - "channel_role"：覆盖范围内的团队是否允许频道级别的 IAM 角色的设置。
  - 对于 Amazon Chime，有以下字段可用：
    - "client":
      - "enabled"：Amazon Chime 客户端已启用。允许 Amazon Chime 集成。
      - "disabled"：Amazon Chime 客户端已禁用。不允许 Amazon Chime 集成。
- 在 chatbot 下有一个 default 块，除非在更低级别被覆盖，否则该块会在整个组织中禁用 聊天应用程序中的 Amazon Q 开发者版。此默认设置还会禁用 聊天应用程序中的 Amazon Q 开发者版 支持的任何新聊天应用程序。例如，假设 聊天应用程序中的 Amazon Q 开发者版 支持某个新聊天应用程序，则此默认设置也会禁用该新受支持的聊天应用程序。

> **Note**
>
> 有关频道级别 IAM 角色和用户级别 IAM 角色的更多信息，请参阅《聊天应用程序中的 Amazon Q 开发者版 管理员指南》中的 Understanding 聊天应用程序中的 Amazon Q 开发者版 permissions。

聊天机器人策略示例

下面的示例策略仅供参考。

示例 1：仅允许特定工作区内的私有 Slack 频道，禁用 Microsoft Teams，支持所有身份验证模式

以下策略侧重于控制 Slack 和 Microsoft Teams 聊天机器人集成的允许配置。

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
               "@@assign": [
                  "Slack-Workspace-Id"
               ]
            },
            "default": {
               "supported_channel_types": {
                  "@@assign": [
                     "private"
                  ]
               },
               "supported_role_settings": {
                  "@@assign": [
                     "channel_role",
                     "user_role"
                  ]
               }
            }
         },
         "microsoft_teams": {
```

```
            "client": {
               "@@assign": "disabled"
            }
         },
         "chime":{
            "client":{
               "@@assign":"disabled"
            }
         },
         "default":{
            "client":{
               "@@assign":"disabled"
            }
         }
      }
   }
}
```

Slack

- Slack 客户端已启用。
- 仅允许特定的 Slack 工作区 *Slack-Workspace-Id*。
- 默认设置为仅允许私有 Slack 频道、频道级别 IAM 角色和用户级别 IAM 角色。

Microsoft Teams

- Microsoft Teams 客户端已禁用。

Amazon Chime

- Amazon Chime 客户端已禁用。

其他详细信息

- 底部的 `default` 块将客户端设置为禁用，除非在更低级别被覆盖，否则将在整个组织中禁用 聊天应用程序中的 Amazon Q 开发者版。此默认设置还会禁用 聊天应用程序中的 Amazon Q 开发者版 支持的任何新聊天应用程序。例如，假设 聊天应用程序中的 Amazon Q 开发者版 支持某个新聊天应用程序，则此默认设置也会禁用该新受支持的聊天应用程序。

示例 2：仅允许使用用户级别 IAM 角色的 Slack 集成

以下策略对 Slack 采取更宽松的方法，允许所有 Slack 工作区，但将身份验证模式限定为仅限用户级别 IAM 角色。

```
{
   "chatbot":{
      "platforms":{
         "slack":{
            "client":{
               "@@assign":"enabled"
            },
            "workspaces":
               {
                  "@@assign":[
                     "*"
                  ]
               },
            "default":{
               "supported_role_settings":{
                  "@@assign":[
                     "user_role"
                  ]
               }
            }
         },
         "microsoft_teams":{
            "client":{
               "@@assign":"disabled"
            }
         },
         "chime":{
            "client":{
               "@@assign":"disabled"
            }
         }
      },
      "default":{
         "client":{
            "@@assign":"disabled"
         }
      }
   }
```

```
}
```

Slack

- Slack 客户端已启用。
- 没有使用通配符 "*" 定义任何特定的 Slack 工作区，因此允许使用所有工作区。
- 默认设置为仅允许用户级别 IAM 角色。

Microsoft Teams

- Microsoft Teams 客户端已禁用。

Amazon Chime

- Amazon Chime 客户端已禁用。

其他详细信息

- 底部的 `default` 块将客户端设置为禁用，除非在更低级别被覆盖，否则将在整个组织中禁用 聊天应用程序中的 Amazon Q 开发者版。此默认设置还会禁用 聊天应用程序中的 Amazon Q 开发者版 支持的任何新聊天应用程序。例如，假设 聊天应用程序中的 Amazon Q 开发者版 支持某个新聊天应用程序，则此默认设置也会禁用该新受支持的聊天应用程序。

示例 3：仅允许特定租户中的 Microsoft Teams 集成

以下示例策略将组织锁定，从而仅允许指定租户内的 Microsoft Teams 聊天机器人集成，同时完全阻止 Slack 集成。

```
{
   "chatbot":{
      "platforms":{
         "slack":{
            "client": {
               "@@assign": "disabled"
            },
         },
         "microsoft_teams":{
            "client": {
```

```
                "@@assign": "enabled"
            },
            "tenants":{
               "Microsoft-Teams-Tenant-Id":{
                  "@@assign":[
                     "*"
                  ]
               }
            }
         },
         "chime": {
            "client":{
               "@@assign": "disabled"
            }
         }
      }
   }
}
```

Slack

- Slack 客户端已禁用。

Microsoft Teams

- 仅允许使用特定的租户 *Microsoft-Teams-Tenant-Id*，使用通配符 "*" 来允许该租户中的所有团队。

Amazon Chime

- Amazon Chime 客户端已禁用。

其他详细信息

- 底部的 default 块将客户端设置为禁用，除非在更低级别被覆盖，否则将在整个组织中禁用 聊天应用程序中的 Amazon Q 开发者版。此默认设置还会禁用 聊天应用程序中的 Amazon Q 开发者版 支持的任何新聊天应用程序。例如，假设 聊天应用程序中的 Amazon Q 开发者版 支持某个新聊天应用程序，则此默认设置也会禁用该新受支持的聊天应用程序。

示例 4：允许对 Slack 工作区和 Microsoft Teams 租户的受限 聊天应用程序中的 Amazon Q 开发者版访问

以下策略允许对选定的 Slack 工作区和 Microsoft Teams 租户的受限 聊天应用程序中的 Amazon Q 开发者版 访问。

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled"
             },
             "workspaces": {
                   "@@assign":[
                      "Slack-Workspace-Id1",
                      "Slack-Workspace-Id2"
                   ]
             },
             "default":{
                "supported_channel_types":{
                   "@@assign":[
                      "private"
                   ]
                },
                "supported_role_settings":{
                   "@@assign":[
                      "user_role"
                   ]
                }
             },
             "overrides":{
                "Slack-Workspace-Id2":{
                   "supported_channel_types":{
                      "@@assign":[
                         "public",
                         "private"
                      ]
                   },
                   "supported_role_settings":{
                      "@@assign":[
                         "channel_role",
                         "user_role"
```

```
                    ]
                }
            }
        }
    },
    "microsoft_teams":{
        "client":{
            "@@assign":"enabled"
        },
        "tenants":{
            "Microsoft-Teams-Tenant-Id":{
                "@@assign":[
                    "Microsoft-Teams-Team-Id"
                ]
            }
        },
        "default":{
            "supported_role_settings":{
                "@@assign":[
                    "user_role"
                ]
            }
        },
        "overrides":{
            "Microsoft-Teams-Tenant-Id":{
                "Microsoft-Teams-Team-Id":{
                    "supported_role_settings":{
                        "@@assign":[
                            "channel_role",
                            "user_role"
                        ]
                    }
                }
            }
        }
    },
    "default":{
        "client":{
            "@@assign":"disabled"
        }
    }
}
```

```
}
```

Slack

- Slack 客户端已启用。
- 允许的 Slack 工作区是 *Slack-Workspace-Id1* 和 *Slack-Workspace-Id2*。
- Slack 的默认设置为仅允许私有频道和用户级别 IAM 角色。
- 工作区 *Slack-Workspace-Id2* 有一个覆盖设置，该设置会允许公有和私有频道以及频道级别 IAM 角色和用户级别 IAM 角色。

Microsoft Teams

- Microsoft Teams 客户端已启用。
- 允许的 Teams 租户是 *Microsoft-Teams-Tenant-Id*，团队是 *Microsoft-Teams-Team-Id*。
- 默认设置为仅允许用户级别 IAM 角色。
- 租户 *Microsoft-Teams-Tenant-Id* 有一个覆盖设置，该设置会允许团队 *Microsoft-Teams-Team-Id* 的频道级别 IAM 角色和用户级别 IAM 角色。

其他详细信息

- 底部的 `default` 块将客户端设置为禁用，除非在更低级别被覆盖，否则将在整个组织中禁用 聊天应用程序中的 Amazon Q 开发者版。这意味着此示例中禁用了 Amazon Chime。此默认设置还会禁用 聊天应用程序中的 Amazon Q 开发者版 支持的任何新聊天应用程序。例如，假设 聊天应用程序中的 Amazon Q 开发者版 支持某个新聊天应用程序，则此默认设置也会禁用该新受支持的聊天应用程序。

AI 服务选择退出策略

AI 服务选择退出策略允许您控制组织中所有账户的 Amazon AI 服务数据收集。

Amazon AI 服务可能会使用和存储客户内容来改进服务。服务改进是指使用和存储非个人数据的内容来开发和改进 Amazon 以及关联机器学习和人工智能技术。为此，我们可能会将内容存储在您使用服务的地点 Amazon Web Services 区域 以外 Amazon Web Services 区域 的地方。作为 Amazon 客户，您可以随时选择不将您的内容用于服务改进。

您可以为单个 AI 服务或 AI 服务选择退出策略支持的所有服务创建选择退出策略。您还可以查询适用于每个账户的有效政策，以查看您的设置选择的影响。

有关更多详细信息，请参阅服务条款中的 M Amazon achine Learning 和人工智能 Amazon 服务。有关 AI 服务选择退出策略支持的服务列表，请参阅支持的 AI 服务列表。

主题

使用 AI 服务选择退出策略时的注意事项

选择退出适用于所有 Amazon Web Services 区域 除外 Amazon GovCloud (US)

当您为某项服务指定选择加入或选择退出首选项时，该设置是全局性的，适用于除服务之外的所有 Amazon Web Services 区域 设置。 Amazon GovCloud (US) Regions从一个 Amazon Web Services 区域 设置值将复制到所有其他区域。

选择退出可能会影响服务功能

Amazon AI 服务可能需要存储您的内容，以便以与任何服务改进无关的身份向您提供服务，而选择退出可能会影响该功能。例如，Amazon Lex 将话语分析存储为向您提供这些分析的一部分。有关更多详细信息，请参阅服务条款中的 M Amazon achine Learning 和人工智能 Amazon 服务。

选择退出会删除所有相关的历史内容

当您选择不让 Amazon AI 服务使用内容时，该服务会删除在您设置该选项 Amazon 之前与之共享的所有关联历史内容。此删除仅限于对提供服务功能非必需的已存储数据。

例如，您在选择启用后使用某项服务。该服务可能会存储您内容的副本，以用于改进服务。您选择退出。为改进服务而由服务存储的所有副本都将被删除，但用于向您提供服务的任何数据都不会被删除。

AI 服务选择退出策略入门

请按照以下步骤操作，开始使用人工智能（AI）服务选择退出策略。

1. 了解执行备份策略任务所必须具备的权限。
2. 为您的组织启用 AI 服务选择退出策略。

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

在所有这些步骤中，您可以以 Amazon Identity and Access Management (IAM) 用户身份登录、担任 IAM 角色或以根用户身份登录（不推荐）在组织的管理账户中登录。

其他信息

- 了解 AI 服务选择退出策略的策略语法，并查看策略示例

选择退出所有支持的 Amazon AI 服务

本主题内容：

- 您可以在 Amazon Organizations 控制台中通过一键选择来选择退出。
- 您可以通过使用 Amazon CLI 和 Amazon SDK 附加提供的示例策略来选择退出。
- 您可以查看 AI 服务选择退出策略支持的 Amazon Web Services 服务列表。

选择退出所有支持的 AI 服务

您可以通过创建并附加 AI 服务选择退出策略，来选择不将其内容用于服务改进。此策略适用于所有当前和未来受支持的 Amazon AI 服务。成员账户无法更新此策略。

Amazon Web Services Management Console

选择退出所有 AI 服务

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 AI 服务选择退出策略页面上，选中选择退出所有服务。
3. 在选择退出所有服务确认页面上，选中选择退出所有服务。

Amazon CLI & Amazon SDKs

选择退出所有 AI 服务

1. 复制 AI 服务选择退出示例中的“示例 1：选择退出组织中所有账户的所有 AI 服务”。

2. 按照附加和分离 AI 服务选择退出中的说明进行操作。

> **Note**
>
> 选择退出 Amazon Monitron 需要执行额外的步骤。有关更多信息，请参阅 Amazon 服务条款。

AI 服务选择退出策略支持的服务列表

以下是 AI 服务选择退出策略支持的 Amazon Web Services 服务列表：

- Amazon Supply Chain
- Amazon Database Migration Service
- Amazon Chime SDK 语音分析
- Amazon CloudWatch
- Amazon CodeGuru Profiler
- Amazon CodeWhisperer（现为 Amazon Q 开发者版的一部分）
- Amazon Comprehend
- Amazon Connect
- Amazon Connect Optimization
- Amazon Connect Contact Lens
- Amazon DataZone
- Amazon Entity Resolution 数据匹配服务
- Amazon Fraud Detector
- Amazon Glue
- Amazon GuardDuty
- Amazon Lex
- Amazon Polly
- Amazon Q
- Amazon QuickSight
- Amazon Rekognition

- Amazon Security Lake
- Amazon Textract
- Amazon Transcribe
- Amazon Translate

AI 服务选择退出策略语法和示例

本主题介绍人工智能（AI）服务选择退出策略语法并提供示例。

AI 服务选择退出策略的语法

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

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

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

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

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

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

AI 服务选择退出策略语法包括以下元素：

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

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

  - 服务名称键，用于标识Amazon AI 服务。以下键名称是此字段的有效值：
    - **default** – 代表所有当前可用的 AI 服务，并隐式和自动包括将来可能添加的任何 AI 服务。
    - awssupplychain
    - dms
    - chimesdkvoiceanalytics
    - cloudwatch

- codeguruprofiler
- codewhisperer
- comprehend
- connectamd
- connectoptimization
- contactlens
- datazone
- entityresolution
- frauddetector
- glue
- guardduty
- lex
- polly
- q
- quicksightq
- rekognition
- securitylake
- textract
- transcribe
- translate

由服务名称键标识的每个策略语句都可以包含以下元素：

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

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

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

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

- 在任何级别上，您都可以指定 @@operators_allowed_for_child_policies 运算符来控制子策略可以执行哪些操作来覆盖父策略施加的设置。可以指定以下值之一：
  - @@assign – 此策略的子策略可以通过 @@assign 运算符使用其他值来覆盖继承值。
  - @@none – 此策略的子策略不能更改该值。

  @@operators_allowed_for_child_policies 的行为取决于您放置它的位置。您可以使用以下位置：
  - services 键下 – 控制子策略是否可以添加或更改有效策略中的服务列表。
  - 在特定 AI 服务的键或 default 键下 – 控制子策略是否可以添加或更改此特定条目下的键列表。
  - 特定服务的 opt_out_policies 键下 – 控制子策略是否只能更改此特定服务的设置。

AI 服务选择退出策略示例

下面的示例策略仅供参考。

示例 1：选择退出组织中所有账户的所有 AI 服务

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

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

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

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

示例 2：为所有服务设置组织默认设置，但允许子策略覆盖单个服务的设置

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

- 因为 services 键没有 "@@operators_allowed_for_child_policies": ["@@none"]，子策略可以为单个服务添加新部分。
- default 下的 "@@operators_allowed_for_child_policies": ["@@none"] 会阻止任何子策略添加除已存在 opt_out_policy 部分之外的任何新部分。
- opt_out_policy 下的 "@@operators_allowed_for_child_policies": ["@@none"] 会阻止子策略更改 optOut 设置的值或添加任何其他设置。

组织根用户 AI 服务选择退出父策略

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

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

AI 服务选择退出子策略

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

为Amazon Web Services 账户产生的有效政策是，由于继承了父策略中的 `default` 选择退出设置，该账户仅选择启用 Amazon Lex，并选择退出所有其他 Amazon AI 服务。

示例 3：为单个服务定义组织范围内的 AI 服务选择退出策略

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

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

的委派管理员 Amazon Organizations

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

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

有关基于资源的委派策略示例，请参阅基于资源的策略示例 Amazon Organizations。

主题

使用创建基于资源的授权策略 Amazon Organizations

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

> **最小权限**
>
> 要创建基于资源的委派策略，您需要有运行以下操作的权限：
>
> - `organizations:PutResourcePolicy`
> - `organizations:DescribeResourcePolicy`
>
> 此外，您必须向委托管理员账户中的角色和用户授予相应的 IAM 权限，以执行所需操作。如果没有 IAM 权限，则假设调用方委托人没有管理 Amazon Organizations 策略所需的权限。

Amazon Web Services Management Console

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

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

使用 JSON 策略编辑器创建委派策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择设置。
3. 在 Amazon Organizations的委托管理员部分中，选择委托以创建 Organizations 委托策略。
4. 输入 JSON 策略文档。有关 IAM policy 语言的详细信息，请参阅 IAM JSON 策略参考。
5. 解决策略验证过程中生成的任何安全警告、错误或常规警告，然后选择 Create policy（创建策略）以保存工作。

使用可视化编辑器创建委派策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择设置。
3. 在 Amazon Organizations的委托管理员部分中，选择委托以创建 Organizations 委托策略。
4. 在 Create Delegation policy（创建委托策略）页面上，选择 Add new statement（添加新语句）。
5. 将 Effect 设置为 `Allow`。
6. 添加 `Principal` 以定义要委托的成员账户。
7. 从 Actions（操作）列表中选择要委托的操作。您可使用 Filter actions（筛选操作）缩小所选内容的范围。
8. 要指定委托成员账户是否可以将策略附加到组织根目录或组织单位 (OUs)，请设置`Resources`。您还必须选择 `policy` 作为资源类型。您可以通过以下方式指定资源：
   - 选择 Add a resource（添加资源），并按照对话框中的提示构建 Amazon 资源名称（ARN）。
   - 在编辑器中 ARNs 手动列出资源。有关 ARN 语法的更多信息，请参阅《通用参考指南》中的 Amazon 资源名称 (ARN)。 Amazon 有关在策略的资源元素 ARNs 中使用的信息，请参阅 IAM JSON 策略元素：资源。
9. 选择 Add a condition（添加条件）以指定其他条件，包括要委托的策略类型。选择条件的 Condition key（条件键）、Tag key（标签键）、Qualifier（限定词）和 Operator（运算符），然后键入 **`Value`**。完成后，选择 Add condition（添加条件）。有关 Condition 元素的更多信息，请参阅 IAM JSON 策略参考中的 IAM JSON 策略元素：Condition。

10. 要添加更多权限块，请选择 Add new statement（添加新语句）。对于每个块，重复步骤 5 到步骤 9。
11. 解决策略验证过程中生成的任何安全警告、错误或常规警告，然后选择 Create policy（创建策略）以保存工作。

Amazon CLI & Amazon SDKs

创建委派策略

您可以使用以下命令创建委派策略：

- Amazon CLI: put-resource-policy

  以下示例会创建一个委派策略。

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

```
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- Amazon 软件开发工具包：PutResourcePolicy

支持的委托策略操作

委托策略支持以下操作：

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent

- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy
- TagResource
- UntagResource
- UpdatePolicy

支持的条件键

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

使用以下命令更新基于资源的授权策略 Amazon Organizations

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

最小权限

要更新基于资源的委派策略，您需要有运行以下操作的权限：

- organizations:PutResourcePolicy

- `organizations:DescribeResourcePolicy`

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

Amazon Web Services Management Console

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

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

使用 JSON 策略编辑器更新委派策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择设置。
3. 在 Amazon Organizations的委派管理员部分中，选择编辑以更新 Organizations 委派策略。
4. 输入 JSON 策略文档。有关 IAM 策略语言的详细信息，请参阅 IAM JSON 策略参考。
5. 解决在策略验证过程中生成的任何安全警告、错误或常规警告，然后选择创建策略。

使用可视化编辑器更新委派策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择设置。
3. 在 Amazon Organizations的委派管理员部分中，选择编辑以更新 Organizations 委派策略。
4. 在 Create Delegation policy（创建委托策略）页面上，选择 Add new statement（添加新语句）。
5. 将 Effect 设置为 `Allow`。

6. 添加 `Principal` 以定义要委托的成员账户。
7. 从 Actions（操作）列表中选择要委托的操作。您可使用 Filter actions（筛选操作）缩小所选内容的范围。
8. 要指定委托成员账户是否可以将策略附加到组织根目录或组织单位 (OUs)，请设置`Resources`。您还必须选择 `policy` 作为资源类型。您可以通过以下方式指定资源：
   - 选择 Add a resource（添加资源），并按照对话框中的提示构建 Amazon 资源名称（ARN）。
   - 在编辑器中 ARNs 手动列出资源。有关 ARN 语法的更多信息，请参阅《通用参考指南》中的 Amazon 资源名称 (ARN)。 Amazon 有关在策略的资源元素 ARNs 中使用的信息，请参阅 IAM JSON 策略元素：资源。
9. 选择 Add a condition（添加条件）以指定其他条件，包括要委托的策略类型。选择条件的 Condition key（条件键）、Tag key（标签键）、Qualifier（限定词）和 Operator（运算符），然后键入 **`Value`**。完成后，选择 Add condition（添加条件）。有关 Condition 元素的更多信息，请参阅 IAM JSON 策略参考中的 IAM JSON 策略元素：Condition。
10. 要添加更多权限块，请选择 Add new statement（添加新语句）。对于每个块，重复步骤 5 到步骤 9。
11. 解决在策略验证过程中生成的任何安全警告、错误或常规警告，然后选择保存策略。

Amazon CLI & Amazon SDKs

创建或更新委托策略

可以使用以下命令创建或更新委托策略：

- Amazon CLI: put-resource-policy

以下为创建或更新委托策略的示例。

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
```

```
            },
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- Amazon 软件开发工具包：PutResourcePolicy

支持的委托策略操作

委托策略支持以下操作：

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus

- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy
- TagResource
- UntagResource
- UpdatePolicy

支持的条件键

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

通过以下方式查看基于资源的授权策略 Amazon Organizations

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

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

Amazon Web Services Management Console

查看委托策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择设置。
3. 在 Amazon Organizations的委托管理员部分中，滚动查看完整的委托策略。

Amazon CLI & Amazon SDKs

查看委托策略

可以使用以下命令查看委托策略：

- Amazon CLI: describe-resource-policy

  以下为检索策略的示例。

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

- Amazon 软件开发工具包：DescribeResourcePolicy

使用删除基于资源的委托策略 Amazon Organizations

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

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

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

Amazon Web Services Management Console

删除委托策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 选择设置。
3. 在 Amazon Organizations的委托管理员部分中，选择删除。
4. 在 Delete policy（删除策略）确认对话框中，键入 **delete**。然后，选择 Delete policy（删除策略）。

Amazon CLI & Amazon SDKs

删除委托策略

可以使用以下命令删除委托策略：

- Amazon CLI: delete-resource-policy

以下为删除策略的示例。

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

- Amazon 软件开发工具包：DeleteResourcePolicy

启用策略类型

在创建策略并将其附加到组织之前，必须启用该策略类型才能使用。启用策略类型是组织根上的一次性任务。您只能通过组织的管理账户或指定为委派管理员的成员账户启用策略类型。

> 最小权限
>
> 要启用策略类型，您需要运行以下操作的权限：
>
> - `organizations:EnablePolicyType`
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
> - `organizations:ListRoots` – 仅当使用 Organizations 控制台时才需要

Amazon Web Services Management Console

启用策略类型

1. 登录 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在 Policies (策略) 页面上，选择要启用的策略的名称。
3. 在策略类型页面上，选择启用***policy type***。

   该页面会被指定类型的可用策略列表替换。

Amazon CLI & Amazon SDKs

启用策略类型

您可以使用以下命令之一启用策略类型：

- Amazon CLI: enable-policy-type

  以下示例说明如何为组织启用备份策略。请注意，您必须指定组织根的 ID。

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

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

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

- Amazon SDKs: EnablePolicyType

禁用策略类型

如果您不想再在组织中使用某种策略类型，则可以禁用该类型以防止其意外使用。您只能从组织的管理账户或指定为委托管理员的成员账户中禁用策略类型。

注意事项

已禁用的策略会与所有实体分离，但不会被删除

禁用策略类型时，指定类型的所有策略都会自动从组织根中的所有实体分离。策略不会 被删除。

（仅限服务控制策略类型）根目录中的所有实体最初仅附加到默认实体 **FullAWSAccess** SCP

（仅限服务控制策略类型）如果您稍后重新启用该SCP策略类型，则组织根目录中的所有实体最初都仅附加到默认FullAWSAccessSCP策略类型。在组织中禁SCPs用实体时SCPs，实体的附件将丢失。如果您以后想重新启用SCPs，则必须根据需要将它们重新关联到组织的根和账户。OUs

禁用策略类型

最小权限

要禁用SCPs，您需要获得运行以下操作的权限：

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

Amazon Web Services Management Console

禁用策略类型

1. 登录 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在 Policies (策略) 页面上，选择要禁用的策略的名称。
3. 在策略类型页面上，选择禁用***policy type***。
4. 在确认对话框中，输入单词 **disable**，然后选择 Disable (禁用)。

   指定类型的可用策略列表将消失。

Amazon CLI & Amazon SDKs

禁用策略类型

可以使用以下命令之一禁用策略类型：

- Amazon CLI: disable-policy-type

  以下示例说明如何为组织禁用备份策略。请注意，您必须指定组织根的 ID。

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

输出中的 PolicyTypes 列表不再包含指定的策略类型。

- Amazon SDKs: DisablePolicyType

使用创建组织政策 Amazon Organizations

为组织启用策略后，您可以创建策略。

本主题介绍如何使用创建策略 Amazon Organizations。策略定义了您要应用于一组的控制措施 Amazon Web Services 账户。

主题

- 创建服务控制策略（SCP）
- 创建资源控制策略 (RCP)
- 创建声明性政策
- 创建备份策略
- 创建标签策略
- 创建聊天机器人策略
- 创建 AI 服务选择退出策略

创建服务控制策略（SCP）

最小权限

要创建 SCPs，您需要获得运行以下操作的权限：

- organizations:CreatePolicy

Amazon Web Services Management Console

创建服务控制策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Service control policies (服务控制策略) 页面上，选择 Create policy (创建策略)。

3. 在 CCreate new service control policy (创建新的服务控制策略) 页面上，输入策略的 Policy name (策略名称) 和可选 Policy description (策略说明)。

4. （可选）添加一个或多个标签，方法是选择 Add tag (添加标签)，然后输入一个键和可选的值。将值留空，设置为空字符串；它并非 null。您最多可以向策略附加 50 个标签。有关更多信息，请参阅 为资源添加标签 Amazon Organizations。

> **Note**
>
> 在接下来的大多数步骤中，我们讨论如何使用 JSON 编辑器右侧的控件来逐个元素构建策略。或者，您可以随时在窗口左侧的 JSON 编辑器中输入文本。您可以直接键入，也可以使用复制和粘贴。

5. 为了构建策略，您的后续步骤因您是否要添加拒绝或允许访问的语句而异。有关更多信息，请参阅 SCP 评估。如果您使用Deny语句，则可以获得额外的控制权，因为您可以限制对特定资源的访问权限，定义 SCPs 何时生效的条件以及使用该NotAction元素。有关语法的详细信息，请参阅SCP 语法。

   要添加拒绝 访问的语句，请执行以下操作：

   a. 在编辑器右侧的 “编辑语句” 窗格中，在 “添加操作” 下，选择一项 Amazon 服务。

      当您选择右侧的选项时，JSON 编辑器会更新，以在左侧显示相应的 JSON 策略。

   b. 选择服务后，将打开一个列表，其中包含该服务的可用操作。您可以选择 All actions (所有操作)，或选择要拒绝的一个或多个单独操作。

      左侧的 JSON 将更新，以包含您选择的操作。

      > **Note**
      >
      > 如果您选择一个单独的操作，然后返回并选择 All actions (所有操作)，那么 *servicename*:* 的预期条目会添加到 JSON 中，但您之前选择的单个操作将保留在 JSON 中，而不会被删除。

   c. 如果要添加来自其他服务的操作，您可以选择 Statement (语句) 框顶部的 All services (所有服务)，然后根据需要重复前面两个步骤。

   d. 指定要包含在语句中的资源。

      - 在添加资源旁边，选择添加。

- 在 Add resource (添加资源) 对话框中，从列表中选择要控制其资源的服务。您只能从上一步骤选择的服务中进行选择。
- 在 Resource type (资源类型) 下，选择要控制的资源的类型。
- 最后，在 Resource ARN 中填写 Amazon Resource Name（ARN），以标识您要控制访问权限的特定资源。必须替换由大括号 {} 包围的所有占位符。您可以在资源类型的 ARN 语法允许的地方指定通配符（*）。有关可在何处使用通配符的信息，请参阅特定资源类型的文档。
- 保存您对策略添加的内容，方法是选择 Add resource (添加资源)。JSON 中的 `Resource` 元素反映了您的添加或更改。需要 Resource (资源) 元素。

> **Tip**
>
> 如果要指定选定服务的所有资源，请选择列表中的 All resources (所有资源) 选项，或者直接在 JSON 中编辑 `Resource` 语句以读取 `"Resource":"*"`。

e. （可选）要指定限制策略语句生效时间的条件，请在添加条件旁边选择添加。

- 条件密钥-从列表中，您可以选择适用于所有 Amazon 服务的任何条件密钥（例如`aws:SourceIp`），或者仅为在本语句中选择的一项服务选择特定于服务的密钥。
- 限定符-（可选）当请求具有多个多值上下文键值的值时，您可以指定一个限定符来根据这些值测试请求。有关更多信息，请参阅 IAM 用户指南中的单值与多值上下文密钥。要检查请求是否可以有多个值，请参阅《服务授权参考》 Amazon Web Services 服务中的操作、资源和条件键。
  - 默认值 – 根据策略中的条件键值测试请求中的单个值。如果请求中的值均与策略中的值匹配，则条件返回 true。如果策略指定了多个值，则它们将被视为“or”测试，如果请求值与任何策略值匹配，则条件返回 true。
  - 对于请求中的任何值 – 当请求可以具有多个值时，此选项测试是否有至少一个请求值与策略中的至少一个条件键值匹配。如果请求中的任何一个键值与策略中的任何一个条件值匹配，则条件返回 true。对于没有匹配的键或空数据集，条件返回 false。
  - 对于请求中的所有值 – 当请求可以具有多个值时，此选项测试是否每个请求值都与策略中的条件键值匹配。如果请求中的每个键值均与策略中的至少一个值匹配，则条件返回 true。如果请求中没有键或者键值解析为空数据集（如空字符串），则也会返回 true。

- 运算符 – 运算符指定要进行比较的类型。显示的选项取决于条件键的数据类型。例如，`aws:CurrentTime` 全局条件键允许您从任何日期比较运算符（或 `Null`）中选择，您可以使用它来测试请求中是否存在该值。

  对于除`Null`检验之外的任何条件运算符，您可以选择该IfExists选项。

- 值 – （可选）指定要测试请求的一个或多个值。

选择 添加条件。

有关条件键的更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

6. 要添加允许 访问的语句，请执行以下操作：

   a. 在左侧的 JSON 编辑器中，将行 `"Effect": "Deny"` 改为 `"Effect": "Allow"`。

   当您选择右侧的选项时，JSON 编辑器会更新，以在左侧显示相应的 JSON 策略。

   b. 选择服务后，将打开一个列表，其中包含该服务的可用操作。您可以选择 All actions (所有操作)，或选择要允许的一个或多个单独操作。

   左侧的 JSON 将更新，以包含您选择的操作。

   > **Note**
   >
   > 如果您选择一个单独的操作，然后返回并选择 All actions (所有操作)，那么 *servicename*`:*` 的预期条目会添加到 JSON 中，但您之前选择的单个操作将保留在 JSON 中，而不会被删除。

   c. 如果要添加来自其他服务的操作，您可以选择 Statement (语句) 框顶部的 All services (所有服务)，然后根据需要重复前面两个步骤。

7. （可选）要向策略添加另一个语句，请选择 Add statement (添加语句) 并使用可视化编辑器构建下一条语句。

8. 添加完语句后，选择 Create policy (创建策略) 以保存已完成的 SCP。

您的新 SCP 会显示在组织的策略列表中。现在，您可以将 SCP 附加到根或账户。 OUs

Amazon CLI & Amazon SDKs

创建服务控制策略

您可以使用以下命令之一创建 SCP：

- Amazon CLI：create-policy

  以下示例假定您有一个名为 Deny-IAM.json 的文件，其中包含 JSON 策略文本。它使用该文件创建新的服务控制策略。

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- Amazon SDKs: CreatePolicy

> **Note**
>
> SCPs 不要对管理账户和其他几种情况生效。有关更多信息，请参阅 不受限制的任务和实体 SCPs。

创建资源控制策略 (RCP)

> **最小权限**
>
> 要创建 RCPs，您需要获得运行以下操作的权限：

- `organizations:CreatePolicy`

Amazon Web Services Management Console

创建资源控制策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在资源控制策略页面上，选择创建策略。
3. 在创建新的资源控制策略页面上，输入策略名称和可选的策略描述。
4. （可选）添加一个或多个标签，方法是选择 Add tag (添加标签)，然后输入一个键和可选的值。将值留空，设置为空字符串；它并非 `null`。您最多可以向策略附加 50 个标签。有关更多信息，请参阅 为资源添加标签 Amazon Organizations。

   > **Note**
   >
   > 在接下来的大多数步骤中，我们讨论如何使用 JSON 编辑器右侧的控件来逐个元素构建策略。或者，您可以随时在窗口左侧的 JSON 编辑器中输入文本。您可以直接键入，也可以使用复制和粘贴。

5. 要添加语句，请执行以下操作：

   a. 在编辑器右侧的 “编辑语句” 窗格中，在 “添加操作” 下，选择一项 Amazon 服务。

      当您选择右侧的选项时，JSON 编辑器会更新，以在左侧显示相应的 JSON 策略。

   b. 选择服务后，将打开一个列表，其中包含该服务的可用操作。您可以选择 All actions (所有操作)，或选择要拒绝的一个或多个单独操作。

      左侧的 JSON 将更新，以包含您选择的操作。

      > **Note**
      >
      > 如果您选择一个单独的操作，然后返回并选择 All actions (所有操作)，那么 *`servicename`*`:*` 的预期条目会添加到 JSON 中，但您之前选择的单个操作将保留在 JSON 中，而不会被删除。

c. 如果要添加来自其他服务的操作，您可以选择 Statement (语句) 框顶部的 All services (所有服务)，然后根据需要重复前面两个步骤。

d. 指定要包含在语句中的资源。

- 在添加资源旁边，选择添加。
- 在 Add resource (添加资源) 对话框中，从列表中选择要控制其资源的服务。您只能从上一步骤选择的服务中进行选择。
- 在 Resource type (资源类型) 下，选择要控制的资源的类型。
- 填写资源 ARN 中的 Amazon 资源名称 (ARN)，以确定您要控制访问权限的特定资源。必须替换由大括号 {} 包围的所有占位符。您可以在资源类型的 ARN 语法允许的地方指定通配符（*）。有关可以在何处使用通配符的信息，请参阅特定资源类型的文档。
- 保存您对策略添加的内容，方法是选择 Add resource (添加资源)。JSON 中的 `Resource` 元素反映了您的添加或更改。需要 Resource (资源) 元素。

> **Tip**
>
> 如果要指定选定服务的所有资源，请选择列表中的 All resources (所有资源) 选项，或者直接在 JSON 中编辑 `Resource` 语句以读取 `"Resource":"*"`。

e. （可选）要指定限制策略语句生效时间的条件，请在添加条件旁边选择添加。

- 条件密钥-从列表中，您可以选择适用于所有 Amazon 服务的任何条件密钥（例如`aws:SourceIp`），或者仅为在本语句中选择的一项服务选择特定于服务的密钥。
- 限定符-（可选）当请求具有多个多值上下文键值的值时，您可以指定一个限定符来根据这些值测试请求。有关更多信息，请参阅 IAM 用户指南中的单值与多值上下文密钥。要检查请求是否可以有多个值，请参阅《服务授权参考》 Amazon Web Services 服务中的操作、资源和条件键。
  - 默认值 – 根据策略中的条件键值测试请求中的单个值。如果请求中的值均与策略中的值匹配，则条件返回 true。如果策略指定了多个值，则它们将被视为“or”测试，如果请求值与任何策略值匹配，则条件返回 true。
  - 对于请求中的任何值 – 当请求可以具有多个值时，此选项测试是否有至少一个请求值与策略中的至少一个条件键值匹配。如果请求中的任何一个键值与策略中的任何一个条件值匹配，则条件返回 true。对于没有匹配的键或空数据集，条件返回 false。
  - 对于请求中的所有值 – 当请求可以具有多个值时，此选项测试是否每个请求值都与策略中的条件键值匹配。如果请求中的每个键值均与策略中的至少一个值匹配，则条件

返回 true。如果请求中没有键或者键值解析为空数据集（如空字符串），则也会返回 true。

- 运算符 – 运算符指定要进行比较的类型。显示的选项取决于条件键的数据类型。例如，aws:CurrentTime 全局条件键允许您从任何日期比较运算符（或 Null）中选择，您可以使用它来测试请求中是否存在该值。

  对于除Null检验之外的任何条件运算符，您可以选择该IfExists选项。
- 值 –（可选）指定要测试请求的一个或多个值。

选择 添加条件。

有关条件键的更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

f. （可选）要使用 NotAction 元素来拒绝对所有操作（指定操作除外）的访问权限，请将左窗格中的 Action 替换为 NotAction（位于 "Effect": "Deny", 元素后）。有关更多信息，请参阅 IAM 用户指南 NotAction中的 IAM JSON 策略元素：。

6. （可选）要向策略添加另一个语句，请选择 Add statement (添加语句) 并使用可视化编辑器构建下一条语句。
7. 添加完对账单后，选择创建策略以保存已完成的 RCP。

您的新 RCP 将出现在该组织的政策列表中。现在，您可以将 RCP 附加到一个或多个 OUs根账户。

Amazon CLI & Amazon SDKs

创建资源控制策略

您可以使用以下命令之一创建 RCP：

- Amazon CLI：create-policy

以下示例假定您有一个名为 Deny-IAM.json 的文件，其中包含 JSON 策略文本。它使用该文件来创建新的资源控制策略。

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMRCP \
    --type RESOURCE_CONTROL_POLICY
{
```

```
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
resource_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMRCP",
            "Description": "Deny all IAM actions",
            "Type": "RESOURCE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- Amazon SDKs: CreatePolicy

> **Note**
>
> RCPs 不要对管理账户和其他几种情况生效。有关更多信息，请参阅 不受限制的资源和实体 RCPs。

创建声明性政策

> **最小权限**
>
> 要创建声明性策略，您需要获得运行以下操作的权限：
>
> - `organizations:CreatePolicy`

Amazon Web Services Management Console

创建声明性政策

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在声明性策略页面上，选择创建策略。
3. 在 “为其创建新的声明性策略 EC2” 页面上，输入策略名称和可选的策略描述。

4. （可选）您可以向策略添加一个或多个标签，方法是选择 Add tag (添加标签)，然后输入一个键和可选的值。将值留空，设置为空字符串；它并非 null。您最多可以向策略附加 50 个标签。有关更多信息，请参阅 为资源添加标签 Amazon Organizations。
5. 您可以使用可视化编辑器构建策略，如此过程中所述。您也可以在 JSON 选项卡中输入或粘贴策略文本。有关声明式策略语法的信息，请参见声明式策略语法和示例。

   如果您选择使用可视化编辑器，请选择要包含在声明式策略中的服务属性。有关更多信息，请参阅 支持 Amazon Web Services 服务 和属性。
6. 选择添加服务属性，然后根据您的规格配置该属性。有关每种效果的更多详细信息，请参阅声明式策略语法和示例。
7. 编辑完策略后，选择位于页面右下角的 Create policy (创建策略)。

Amazon CLI & Amazon SDKs

创建声明性政策

您可以使用以下方法之一来创建声明性策略：

- Amazon CLI：create-policy

1. 创建如下所示的声明性策略，并将其存储在文本文件中。

```
{
    "ec2_attributes": {
        "image_block_public_access": {
            "state": {
                "@@assign": "block_new_sharing"
            }
        }
    }
}
```

   此声明性政策规定，必须对受该政策影响的所有账户进行配置，确保新的 Amazon 系统映像 (AMIs) 不可公开共享。有关声明式策略语法的信息，请参见声明式策略语法和示例。
2. 导入 JSON 策略文件以在组织中创建新的策略。在本示例中，上一个 JSON 文件名为 policy.json。

```
$ aws organizations create-policy \
    --type DECLARATIVE_POLICY_EC2 \
```

```
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "DECLARATIVE_POLICY_EC2"
        }
    }
}
```

- Amazon SDKs: CreatePolicy

后续操作

创建声明性政策后，使用账户状态报告评估准备情况。然后，您可以强制执行基准配置。为此，您可以将策略附加到组织根目录、组织单位 (OUs)、组织 Amazon Web Services 账户 内部或所有这些的组合。

创建备份策略

> **最小权限**
>
> 要创建备份策略，您需要运行以下操作的权限：
>
> - `organizations:CreatePolicy`

Amazon Web Services Management Console

您可以通过以下两种 Amazon Web Services Management Console 方式之一来创建备份策略：

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

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

创建备份策略

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

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

   a. Backup 计划一般详细信息
      - 备份文计划名称只能由字母数字、连字符和下划线字符组成。
      - 您必须从列表中至少选择一个备份计划区域。该计划只能备份选定资源中的资源 Amazon Web Services 区域。

   b. 一个或多个指定 Amazon Backup 的操作方式和时间的备份规则。每个备份规则定义以下项目：
      - 包含备份频率和可以进行备份的时间窗口的计划。
      - 要使用的备份文件库的名称。备份文件库名称只能由字母数字、连字符和下划线字符组成。备份文件库必须存在，才能成功运行计划。使用 Amazon Backup 控制台或 Amazon CLI 命令创建文件库。
      - （可选）一个或多个复制到区域规则，以同时将备份复制到其他 Amazon Web Services 区域中的文件库。
      - 一个或多个标签键值对，要附加到每次运行此备份计划时创建的备份恢复点。

- 生命周期选项，它们指定备份过渡到冷存储的时间以及备份到期时间。

选择 Add rule (添加规则) 将您需要的每个规则添加到计划中。

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

c. 一种资源分配，它指定 Amazon Backup 应使用此计划备份的资源。通过指定用于查找和匹配资源的标签对 Amazon Backup 来进行分配

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

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

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

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

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

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

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

Amazon CLI & Amazon SDKs

创建备份策略

您可以使用以下方法之一创建备份策略：

- Amazon CLI：create-policy

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

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

此备份计划规定， Amazon Backup 应备份受影响 Amazon Web Services 账户 区域中指定 Amazon Web Services 区域 dataType且标签值为的所有资源PII。

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

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

- Amazon SDKs: CreatePolicy

创建标签策略

> **最小权限**
>
> 要创建标签策略，您需要运行以下操作的权限：
>
> - `organizations:CreatePolicy`

您可以通过以下两种 Amazon Web Services Management Console 方式之一来创建标签策略：

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

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

Amazon Web Services Management Console

您可以通过以下两种 Amazon Web Services Management Console 方式之一来创建标签策略：

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

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

创建标签策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Tag policies (标签策略) 页面上，选择 Create policy (创建策略)。
3. 在 Create policy (创建策略) 页面上，输入策略的 Policy name (策略名称) 和可选 Policy description (策略说明)。
4. （可选）您可以向策略对象本身添加一个或多个标签。这些标签不是策略的一部分。为此，请选择 Add tag (添加标签)，然后输入键和可选值。将值留空，设置为空字符串；它并非 `null`。您最多可以向策略附加 50 个标签。有关更多信息，请参阅 为资源添加标签 Amazon Organizations。
5. 您可以使用可视化编辑器构建标签策略，如此过程中所述。您也可以在 JSON 选项卡中键入或粘贴标签策略。有关标签策略语法的信息，请参阅标签策略语法。

   如果您选择使用可视化编辑器，请指定以下内容：

6. 对于 New tag key (新标签键 1)，指定要添加的标签键的名称。
7. 对于合规性选项，您可以选择以下选项：

a. 使用您在上面为标签键指定的大写 – 请务必清除此选项（默认设置），以指定继承的父级标签策略（如果存在）应定义标签键的大小写处理。

如果要使用此策略规定标签键的特定大写，请启用此选项。如果选择此选项，则您为 Tag Key (标签键) 指定的大小写将覆盖继承的父策略中指定的大小写处理。

如果父策略不存在且您没有启用此选项，则仅全小写字符的标签键将被视为符合要求。有关从父策略继承的更多信息，请参阅了解管理策略继承。

> **Tip**
>
> 在创建定义标签键及其大小写处理的标签策略时，请考虑使用示例 1：定义组织级的标签键大小写中显示的示例标签策略作为指南。将其附加到组织根。稍后，您可以创建其他标签策略并将其附加到 OUs 或账户，以创建其他标记规则。

b. 指定此标签键的允许值 – 如果要将此标签键的允许值添加到从父级策略继承的任何值，请启用此选项。

默认情况下，将清除此选项，这意味着仅将从父策略定义和继承的这些值视为符合要求。如果父策略不存在并且您没有指定标签值，则任何值（包括没有值）都视为符合要求。

要更新可接受的标签值列表，请选择 Specify allowed values for this tag key (为此标签键指定允许的值)，然后选择 Specify values (指定值)。出现提示时，输入新值（每个框一个值）然后选择 Save changes (保存更改)。

8. 对于要强制执行的资源类型，您可以选择为此标签阻止不合规操作。

我们建议您务必清楚此选项（默认设置），除非您有丰富的使用标签策略的经验。请确保您已查看了解强制执行中的建议并测试技术。否则，您可能会阻止组织账户中的用户标记他们所需的资源。

如果要强制实施此标签键的合规性，请选中该复选框，然后选择 Specify resource types (指定资源类型)。出现提示后，选择要包含在策略中的资源类型。然后选择 Save changes（保存更改)。

> **Important**
>
> 选择此选项后，只有在操作生成符合策略的标签时，操作指定类型资源的标签的任何操作才会成功。

9. （可选）要向此标签策略添加另一个标签键，请选择 Add tag key (添加标签键)。然后执行步骤 6–9 来定义标签键。
10. 完成标签策略构建后，选择 Save changes (保存更改)。

Amazon CLI & Amazon SDKs

创建标签策略

您可以使用以下方法之一来创建标签策略：

- Amazon CLI：create-policy

  您可使用任何文本编辑器创建标签策略。使用 JSON 语法并将标签策略以任意名称和扩展名在您选择的位置另存为文件。标签策略最多可具有 2,500 个字符，包括空格。有关标签策略语法的信息，请参阅标签策略语法。

  创建标签策略

  1. 在文本文件中创建类似于以下内容的标签策略：

     testpolicy.json 的内容：

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

     此标签策略定义 CostCenter 标签键。该标签可以接受任何值或不接受值。这样的策略意味着带有或不带值的 CostCenter 标签的资源都是合规的。

  2. 创建包含文件中策略内容的策略。为了便于阅读，输出中的额外空格已被截断。

     ```
     $ aws organizations create-policy \
         --name "MyTestTagPolicy" \
         --description "My Test policy" \
         --content file://testpolicy.json \
     ```

```
    --type TAG_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-a1b2c3d4e5",
            "Name": "MyTestTagPolicy",
            "Description": "My Test policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign
\":\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

- Amazon SDKs: CreatePolicy

创建聊天机器人策略

> **最小权限**
>
> 要创建聊天机器人策略，您需要有运行以下操作的权限：
>
> - `organizations:CreatePolicy`

Amazon Web Services Management Console

您可以通过以下两种 Amazon Web Services Management Console 方式之一创建聊天机器人政策：

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

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

提供对子控制运算符的任何访问权限。只有在手动编辑 JSON 策略文本时，才能添加子控制运算符。

创建聊天机器人策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在聊天机器人策略页面上，选择创建策略。
3. 在创建策略页面上，输入策略名称和可选的策略描述。
4. （可选）您可以向策略添加一个或多个标签，方法是选择 Add tag (添加标签)，然后输入一个键和可选的值。将值留空，设置为空字符串；它并非 null。您最多可以向策略附加 50 个标签。有关更多信息，请参阅 为资源添加标签 Amazon Organizations。
5. 您可以使用可视化编辑器构建策略，如此过程中所述。您也可以在 JSON 选项卡中输入或粘贴策略文本。有关聊天机器人策略语法的信息，请参阅聊天机器人策略语法和示例。

   如果您选择使用可视化编辑器，请通过为聊天客户端指定访问控制来配置聊天机器人策略。

   a. 对于设置 Amazon Chime 聊天客户端访问权限，请选择以下选项之一

   - 拒绝 Chime 访问。
   - 允许 Chime 访问。

   b. 对于设置 Microsoft Teams 聊天客户端访问权限，请选择以下选项之一

   - 拒绝所有 Teams 访问
   - 允许所有 Teams 访问
   - 限定指定 Teams 访问

   c. 对于设置 Slack 聊天客户端访问权限，请选择以下选项之一

   - 拒绝访问所有 Slack 工作区
   - 允许访问所有 Slack 工作区
   - 限定指定 Slack 工作区访问

   > **Note**
   >
   > 此外，您可以选择 “仅限私有 Slack 频道 聊天应用程序中的 Amazon Q 开发者版 使用”。

   d. 对于设置 IAM 权限类型，请选择以下选项

- 启用频道级别 IAM 角色 – 所有频道成员共享在频道中运行任务的 IAM 角色权限。如果频道成员需要相同的权限，则适合使用频道角色。
- 启用用户级别 IAM 角色 – 频道成员必须选择一个 IAM 用户角色才能执行操作（需要控制台访问权限才能选择角色）。如果频道成员需要不同的权限并且可以选择自己的用户角色，则适合使用用户角色。

6. 创建完策略后，选择 Create policy (创建策略)。该策略将在聊天机器人备份策略列表中显示。

Amazon CLI & Amazon SDKs

创建聊天机器人策略

您可以使用以下方法之一来创建聊天机器人策略：

- Amazon CLI：create-policy

  您可使用任何文本编辑器创建聊天机器人策略。使用 JSON 语法，并将聊天机器人策略以任意名称和扩展名在您选择的位置另存为文件。聊天机器人策略最多可包含？个字符，包括空格。有关标签策略语法的信息，请参阅聊天机器人策略语法和示例。

  创建聊天机器人策略

  1. 在文本文件中创建类似于以下内容的聊天机器人策略：

     testpolicy.json 的内容：

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
               "@@assign": [
                  "Slack-Workspace-Id"
               ]
            },
            "default": {
               "supported_channel_types": {
                  "@@assign": [
                     "private"
```

```
                ]
             }
          }
       },
       "microsoft_teams": {
          "client": {
             "@@assign": "disabled"
          }
       }
    }
 }
}
```

此聊天机器人策略仅允许在特定工作区中使用私有 Slack 频道，禁用 Microsoft Teams，并支持所有角色设置。

2. 创建包含文件中策略内容的策略。为了便于阅读，输出中的额外空格已被截断。

```
$ aws organizations create-policy \
    --name "MyTestChatbotPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type CHATBOT_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-a1b2c3d4e5",
            "Name": "MyTestChatbotPolicy",
            "Description": "My Test policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-
Id"]},"supported_channel_types":{"@@assign":["private"]}},"microsoft_teams":
{"client":{"@@assign":"disabled"}}}}}"
    }
}
```

- Amazon SDKs: CreatePolicy

创建 AI 服务选择退出策略

最小权限

要创建 AI 服务选择退出策略，您需要运行以下操作的权限：

- `organizations:CreatePolicy`

Amazon Web Services Management Console

创建 AI 服务选择退出策略

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

Amazon CLI & Amazon SDKs

创建 AI 服务选择退出策略

您可以使用以下方法之一来创建标签策略：

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

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

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

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

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

- Amazon SDKs: CreatePolicy

使用更新组织政策 Amazon Organizations

当策略要求发生变化时，您可以更新现有策略。

本主题介绍如何使用更新策略 Amazon Organizations。策略定义了您要应用于一组的控制措施 Amazon Web Services 账户。

主题

更新服务控制策略（SCP）

当登录到您组织的管理账户后，您可以重命名或更改策略内容。更改 SCP 的内容会立即影响所有附加账户中的任何用户、组和角色。

最小权限

若要更新 SCP，您需要运行以下操作的权限：

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

Amazon Web Services Management Console

更新策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在服务控制策略页面上，选择要更新的策略的名称。
3. 在策略的详细信息页面上，选择 Edit policy (编辑策略)。
4. 进行以下任何或全部更改：
   - 您可以通过在 Policy name (策略名称) 中输入新名称来重命名策略。
   - 您可以通过在 Policy description (策略说明) 中输入新文本来更改策略说明。
   - 您可以通过在左窗格中以 JSON 格式编辑策略来编辑策略文本。或者，您可以在右侧的编辑器中选择一个语句，然后使用控件更改其元素。有关每个控件的详细信息，请参阅本主题前面的创建 SCP 过程。
5. 完成后，选择保存更改。

Amazon CLI & Amazon SDKs

更新策略

可以使用以下命令之一来更新策略：

- Amazon CLI：update-policy

  以下示例重命名策略。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
```

```
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

以下示例添加或更改服务控制策略的说明。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

以下示例通过指定包含新 JSON 策略文本的文件来更改 SCP 的策略文档。

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
```

```
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- Amazon SDKs: UpdatePolicy

更新资源控制策略 (RCP)

当登录到您组织的管理账户后，您可以重命名或更改策略内容。更改 RCP 的内容会立即影响所有关联账户中的所有资源。

> **最小权限**
>
> 要更新 RCP，您需要获得运行以下操作的权限：
>
> - `organizations:UpdatePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。
> - `organizations:DescribePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。

Amazon Web Services Management Console

更新策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在资源控制策略页面上，选择要更新的策略的名称。
3. 在策略的详细信息页面上，选择 Edit policy (编辑策略)。
4. 进行以下任何或全部更改：
   - 您可以通过在 Policy name (策略名称) 中输入新名称来重命名策略。
   - 您可以通过在 Policy description (策略说明) 中输入新文本来更改策略说明。

- 您可以通过在左窗格中以 JSON 格式编辑策略来编辑策略文本。或者，您可以在右侧的编辑器中选择一个语句，然后使用控件更改其元素。有关每个控件的更多详细信息，请参阅本主题前面的创建 RCP 过程。

5. 完成后，选择保存更改。

Amazon CLI & Amazon SDKs

更新策略

可以使用以下命令之一来更新策略：

- Amazon CLI：update-policy

以下示例重命名策略。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

以下示例添加或更改了资源控制策略的描述。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
```

```
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

以下示例通过指定包含新 JSON 策略文本的文件来更改 RCP 的策略文档。

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- Amazon SDKs: UpdatePolicy

更新声明性政策

最小权限

要更新声明式策略，您必须拥有运行以下操作的权限：

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

Amazon Web Services Management Console

更新声明性政策

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在声明性策略页面上，选择要更新的策略的名称。
3. 在策略的详细信息页面上，选择 Edit policy (编辑策略)。
4. 您可以输入一个新的 Policy name (策略名称)、Policy description (策略说明)，或编辑 JSON 策略文本。有关声明式策略语法的信息，请参见声明式策略语法和示例。
5. 完成更新策略后，选择保存更改。

Amazon CLI & Amazon SDKs

更新策略

您可以使用以下命令之一来更新策略：

- Amazon CLI：update-policy

以下示例重命名了声明式策略。

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

```
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "DECLARATIVE_POLICY_EC2",
            "AwsManaged": false
        },
        "Content": "{"ec2-configuration":{"ec2_attributes":
{"image_block_public_access":{"state":{"@@assign":"block_new_sharing"}}}}".
    }
}
```

以下示例添加或更改了声明式策略的描述。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "DECLARATIVE_POLICY_EC2",
            "AwsManaged": false
        },
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
    }
}
```

- Amazon SDKs: UpdatePolicy

更新备份策略

登录到组织的管理账户后，您可以编辑需要在组织中进行更改的策略。

最小权限

要更新备份策略，您必须具有运行以下操作的权限：

- `organizations:UpdatePolicy`，且同一条策略语句中有一个 `Resource` 元素包含要更新的策略的 ARN（或“*”）
- `organizations:DescribePolicy`，且同一条策略语句中有一个 `Resource` 元素包含要更新的策略的 ARN（或“*”）

Amazon Web Services Management Console

更新备份策略

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

Amazon CLI & Amazon SDKs

更新备份策略

您可以使用以下命令之一来更新备份策略：

- Amazon CLI：update-policy

以下示例重命名备份策略。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
```

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

以下示例添加或更改备份策略的说明。

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

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

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
```

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

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
```

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

- Amazon SDKs: UpdatePolicy

更新标签策略

> **最小权限**
>
> 要更新标签策略，您必须具有运行以下操作的权限：
>
> - `organizations:UpdatePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。
> - `organizations:DescribePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。

Amazon Web Services Management Console

更新标签策略

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

Amazon CLI & Amazon SDKs

更新策略

您可以使用以下命令之一来更新策略：

- Amazon CLI：update-policy

  以下示例重命名标签策略。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

  以下示例添加或更改标签策略的说明。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
```

```
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

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

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage
\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":
{\"@@assign\":[\"ec2:instance\"]}}}}"
```

```
}
```

- Amazon SDKs: UpdatePolicy

更新聊天机器人策略

> **最小权限**
>
> 要更新聊天机器人策略，您必须具有运行以下操作的权限：
>
> - `organizations:UpdatePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。
> - `organizations:DescribePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。

Amazon Web Services Management Console

更新聊天机器人策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在聊天机器人策略页面上，选择要更新的聊天机器人策略。
3. 选择编辑策略。
4. 您可以输入一个新的 Policy name (策略名称)、Policy description (策略说明)。您可以通过使用可视化编辑器或通过编辑 JSON 来更改策略内容。
5. 完成更新标签策略后，选择 Save changes (保存更改)。

Amazon CLI & Amazon SDKs

更新策略

您可以使用以下命令之一来更新策略：

- Amazon CLI：update-policy

以下示例会重命名一个聊天机器人策略。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed chatbot policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-i9j8k7l6m5",
            "Name": "Renamed chatbot policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-Id"]},"default":
{"supported_channel_types":{"@@assign":["private"]}}},"microsoft_teams":{"client":
{"@@assign":"disabled"}}}}}"
    }
}
```

- Amazon SDKs: UpdatePolicy

更新 AI 服务选择退出策略

> **最小权限**
>
> 要更新 AI 服务选择退出策略，您必须具有运行以下操作的权限：
>
> - `organizations:UpdatePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 ARN（或“*”）。
> - `organizations:DescribePolicy`，且同一条策略语句中有一个 `Resource` 元素包含所指定策略的 Amazon Resource Name（ARN）（或“*”）。

Amazon Web Services Management Console

更新 AI 服务选择退出策略

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

2. 在 AI services opt-out policies (AI 服务选择退出策略) 页面上，选择要更新的策略的名称。
3. 在策略的详细信息页面上，选择 Edit policy (编辑策略)。
4. 您可以输入一个新的 Policy name (策略名称)、Policy description (策略说明)，或编辑 JSON 策略文本。有关 AI 服务选择退出策略语法的信息，请参阅AI 服务选择退出策略语法和示例。有关可用作起始点的策略的示例，请参阅AI 服务选择退出策略示例。
5. 完成更新策略后，选择保存更改。

Amazon CLI & Amazon SDKs

更新策略

您可以使用以下命令之一来更新策略：

- Amazon CLI：update-policy

以下示例重命名 AI 服务选择退出策略。

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

以下示例添加或更改 AI 服务选择退出策略的说明。

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
```

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

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

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

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

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

- Amazon SDKs: UpdatePolicy

使用编辑附加到组织策略的标签 Amazon Organizations

本主题介绍如何使用编辑附加策略的标签 Amazon Organizations。策略定义了您要应用于一组的控制措施 Amazon Web Services 账户。

主题

- 编辑附加到服务控制策略（SCP）的标签
- 编辑附加到资源控制策略 (RCP) 的标签
- 编辑附加到声明性策略的标签
- 编辑附加到备份策略的标签
- 编辑附加到标签策略的标签
- 编辑附加到聊天机器人策略的标签
- 编辑附加到 AI 服务选择退出策略的标签

编辑附加到服务控制策略（SCP）的标签

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

最小权限

要编辑附加到组织中 SCP 的标签，您必须拥有以下权限：

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

Amazon Web Services Management Console

编辑附加到 SCP 的标签

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Service control policies (服务控制策略) 页面上，选择带有您想要编辑的标签的策略名称。
3. 在策略详细信息页面上，选择 Tags (标签) 选项卡，然后选择 Manage tags (管理标签)。
4. 进行以下任何或全部更改：
   - 更改标签的值，方法是在旧标签上输入新值。您不能直接修改标签键。要更改键，您必须删除带有旧键的标签，然后添加使用新键的标签。
   - 删除任何现有的标签，方法是选择 Remove (删除)。
   - 添加新的标签键和值对。选择 Add tag (添加标签)，然后在提供的框中输入新的键名称和可选值。如果您将 Value (值) 框留空，则值是空字符串；它并非 `null`。
5. 完成后，选择保存更改。

Amazon CLI & Amazon SDKs

编辑附加到 SCP 的标签

您可以使用以下命令之一编辑附加到 SCP 的标签：

- Amazon CLI：tag-resource 和 untag-resource
- Amazon SDKsTagResource 和 UntagResource

编辑附加到资源控制策略 (RCP) 的标签

登录组织的管理账户时，可以添加或移除 RCP 上附加的标签。有关标记的更多信息，请参阅为资源添加标签 Amazon Organizations。

最小权限

要编辑 Amazon 组织中附加到 RCP 的标签，您必须具有以下权限：

- `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
- `organizations:DescribePolicy` – 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 RCP 的标签

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在资源控制策略页面上，选择包含要编辑的标签的策略名称。
3. 在策略详细信息页面上，选择标签选项卡，然后选择管理标签。
4. 进行以下任何或全部更改：
   - 更改标签的值，方法是在旧标签上输入新值。您不能直接修改标签键。要更改键，您必须删除带有旧键的标签，然后添加使用新键的标签。
   - 删除任何现有的标签，方法是选择 Remove (删除)。
   - 添加新的标签键和值对。选择 Add tag (添加标签)，然后在提供的框中输入新的键名称和可选值。如果您将 Value (值) 框留空，则值是空字符串；它并非 `null`。
5. 完成后，选择保存更改。

Amazon CLI & Amazon SDKs

编辑附加到 RCP 的标签

您可以使用以下命令之一来编辑附加到 RCP 的标签：

- Amazon CLI：tag-resource 和 untag-resource
- Amazon SDKsTagResource 和 UntagResource

编辑附加到声明性策略的标签

登录组织的管理账户时，可以添加或删除声明性政策所附的标签。有关标记的更多信息，请参阅为资源添加标签 Amazon Organizations。

> **最小权限**
>
> 要编辑 Amazon 组织中声明性策略所附的标签，您必须具有以下权限：
>
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要
> - `organizations:DescribePolicy` – 仅当使用 Organizations 控制台时才需要
> - `organizations:TagResource`
> - `organizations:UntagResource`

Amazon Web Services Management Console

编辑附加到声明性策略的标签

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

Amazon CLI & Amazon SDKs

编辑附加到声明性策略的标签

您可以使用以下命令之一来编辑附加到声明性策略的标签：

- Amazon CLI：tag-resource 和 untag-resource
- Amazon SDKsTagResource 和 UntagResource

编辑附加到备份策略的标签

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

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

Amazon Web Services Management Console

编辑附加到备份策略的标签

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. Backup policies (备份策略) 页
3. 选择具有要修改的标签的策略名称。

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

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

6. 在完成所有要进行的添加、删除和编辑操作之后，选择 Save changes (保存更改)。

Amazon CLI & Amazon SDKs

编辑附加到备份策略的标签

您可以使用以下命令之一编辑附加到备份策略的标签：

- Amazon CLI：tag-resource 和 untag-resource
- Amazon SDKsTagResource 和 UntagResource

编辑附加到标签策略的标签

当您登录到组织的管理账户时，您可以添加或删除附加到标签策略的标签。为此，请完成以下步骤。

最小权限

要编辑附加到组织中备份策略的标签，您必须拥有以下权限：

- `organizations:DescribeOrganization`（仅限控制台 – 导航到策略）
- `organizations:DescribePolicy`（仅限控制台 – 导航到策略）
- `organizations:TagResource`
- `organizations:UntagResource`

Amazon Web Services Management Console

编辑附加到标签策略的标签

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

2. 在 Tag policies (标签策略) 页面上，选择带有您想要编辑的标签的策略名称。
3. 在所选策略的详细信息页面上，选择 Tags (标签) 选项卡，然后选择 Manage tags (管理标签)。
4. 您可以在此页面上执行以下操作：
   - 编辑任何标签的值，方法是在旧标签上输入新值。您不能修改键。要更改键，您必须删除带有旧键的标签，然后添加使用新键的标签。
   - 删除任何现有的标签，方法是选择 Remove (删除)。
   - 添加新的标签键和值对。选择 Add tag (添加标签)，然后在提供的框中输入新的键名称和可选值。如果您将 Value (值) 框留空，则值是空字符串；它并非 null。
5. 在完成所有要进行的添加、删除和编辑操作之后，选择 Save changes (保存更改)。

Amazon CLI & Amazon SDKs

编辑附加到标签策略的标签

您可以使用以下命令之一编辑附加到标签策略的标签：

- Amazon CLI：tag-resource 和 untag-resource
- Amazon SDKsTagResource 和 UntagResource

编辑附加到聊天机器人策略的标签

当您登录到组织的管理账户时，您可以添加或移除附加到聊天机器人策略的标签。为此，请完成以下步骤。

最小权限

要编辑附加到组织中聊天机器人策略的标签，您必须拥有以下权限：

- `organizations:DescribeOrganization`（仅限控制台 – 导航到策略）
- `organizations:DescribePolicy`（仅限控制台 – 导航到策略）
- `organizations:TagResource`
- `organizations:UntagResource`

Amazon Web Services Management Console

编辑附加到聊天机器人策略的标签

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

Amazon CLI & Amazon SDKs

编辑附加到聊天机器人策略的标签

您可以使用以下命令之一编辑附加到聊天机器人策略的标签：

- Amazon CLI：tag-resource 和 untag-resource
- Amazon SDKsTagResource 和 UntagResource

编辑附加到 AI 服务选择退出策略的标签

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

> **最小权限**
>
> 要编辑附加到组织中 AI 选择退出策略的标签，您必须拥有以下权限：
>
> - `organizations:DescribeOrganization` – 仅当使用 Organizations 控制台时才需要

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

Amazon Web Services Management Console

编辑附加到 AI 服务选择退出策略的标签

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

Amazon CLI & Amazon SDKs

编辑附加到 AI 服务选择退出策略的标签

您可以使用以下命令之一编辑附加到 AI 服务选择退出策略的标签：

- Amazon CLI：tag-resource 和 untag-resource
- Amazon SDKsTagResource 和 UntagResource

将组织策略附加到 Amazon Organizations

本主题介绍如何使用 Amazon Organizations附加策略。策略定义了您要应用于一组的控制措施 Amazon Web Services 账户。

主题

将策略附加到 Amazon Organizations

最小权限

要附加策略，您必须具有运行以下操作的权限：

- `organizations:AttachPolicy`

最小权限

要将授权策略（SCP 或 RCP）附加到根、OU 或账户，您需要获得运行以下操作的权限：

- `organizations:AttachPolicy`，且同一条策略语句中有一个 `Resource` 元素包含“*”、指定策略的 Amazon Resource Name（ARN）或是您要附加该策略的根、OU 或账户的 ARN。

Amazon Web Services Management Console

Service control policies (SCPs)

您可以导航到要附加策略的根、OU 或账户，为其附加 SCP。

通过导航到根、OU 或账户来附加 SCP

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在Amazon Web Services 账户页面上，导航到要将 SCP 附加到的根、OU 或账户，并选择其旁边的复选框。您可能需要展开 OUs（选

择▶)
才能找到所需的 OU 或帐户。

3. 在 Policies (策略) 选项卡上的 Service control policies (服务控制策略) 条目中，选择 Attach (附加)。
4. 找到所需的策略，然后选择 Attach policy (附加策略)。

   “策略” 选项卡 SCPs 上的附件列表已更新，以包含新增内容。策略更改会立即影响所附加的根或 OU 下方的所附加账户或所有账户中 IAM 用户和角色的权限。

通过导航到策略来附加 SCP

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Service control policies (服务控制策略) 页面上，选择要附加的策略的名称。
3. 在 Targets (目标) 选项卡上，选择 Attach (附加)。
4. 选择要附加策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OUs（选择▶ ）
才能找到所需的 OU 或帐户。
5. 选择附加策略。

   “目标” 选项卡 SCPs 上的附件列表已更新，以包含新增内容。策略更改会立即影响所附加的根或 OU 下方的所附加账户或所有账户中 IAM 用户和角色的权限。

Resource control policies (RCPs)

您可以通过导航到策略或要将策略关联到的根、OU 或账户来附加 RCP。

通过导航到根、OU 或账户来附加 RCP

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在Amazon Web Services 账户页面上，导航到要将 RCP 附加到的根用户、OU 或账户旁边的复选框。您可能需要展开 OUs（选择▶ ）
才能找到所需的 OU 或帐户。
3. 在策略选项卡的资源控制策略条目中，选择附加。

4. 找到所需的策略，然后选择 Attach policy (附加策略)。

   “策略” 选项卡 RCPs 上的附件列表已更新，以包含新增内容。政策变更会立即生效，这会影响关联账户中的资源或附加根或 OU 下的所有账户的权限。

通过导航到策略来附加 RCP

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在资源控制策略页面上，选择要附加的策略的名称。
3. 在 Targets (目标) 选项卡上，选择 Attach (附加)。
4. 选择要附加策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OUs（选择）才能找到所需的 OU 或帐户。
5. 选择附加策略。

   “目标” 选项卡 RCPs 上的附件列表已更新，以包含新增内容。政策变更会立即生效，这会影响关联账户中的资源或附加根或 OU 下的所有账户的权限。

Declarative policies

您可以通过导航到策略或要关联策略的根、OU 或账户来附加声明性策略。

通过导航到根目录、OU 或账户来附加声明性策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在Amazon Web Services 账户页面上，导航到要将策略附加到的根、OU 或账户的相应名称并选择其名称。您可能需要展开 OUs（选择）才能找到所需的 OU 或帐户。
3. 在 “策略” 选项卡的 “声明性策略” 条目中，选择 “附加”。
4. 找到所需的策略，然后选择 Attach policy (附加策略)。

   “政策” 选项卡上附加的声明性策略列表已更新，以包含新增的政策。策略更改会立即生效。

通过导航到政策来附加声明性策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在声明性策略页面上，选择要附加的策略的名称。
3. 在 Targets (目标) 选项卡上，选择 Attach (附加)。
4. 选择要附加策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OUs（选择）才能找到所需的 OU 或帐户。
5. 选择附加策略。

   “目标” 选项卡上附加的声明性策略列表已更新，以包含新增的策略。策略更改会立即生效。

Backup policies

您可以导航到要附加策略的根、OU 或账户，为其附加备份策略。

通过导航到根、OU 或账户来附加备份策略

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

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

通过导航到策略来附加备份策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Backup policies (备份策略) 页面上，选择要附加的策略的名称。

3. 在 Targets (目标) 选项卡上，选择 Attach (附加)。
4. 选择要附加策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OUs（选择）才能找到所需的 OU 或帐户。
5. 选择附加策略。

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

Tag policies

您可以导航到要附加策略的根、OU 或账户，为其附加标签策略。

通过导航到根、OU 或账户来附加标签策略

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

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

通过导航到策略来附加标签策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Tag policies (标签策略) 页面上，选择要附加的策略的名称。
3. 在 Targets (目标) 选项卡上，选择 Attach (附加)。
4. 选择要附加策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OUs（选择）才能找到所需的 OU 或帐户。

5. 选择附加策略。

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

Chatbot policies

您可以导航到要附加策略的根、OU 或账户，为其附加聊天机器人策略。

通过导航到根、OU 或账户来附加聊天机器人策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在Amazon Web Services 账户页面上，导航到要将策略附加到的根、OU 或账户的相应名称并选择其名称。您可能需要展开 OUs（选择）才能找到所需的 OU 或帐户。
3. 在策略选项卡的聊天机器人策略条目中，选择附加。
4. 找到所需的策略，然后选择 Attach policy (附加策略)。

   策略选项卡上的已附加聊天机器人策略列表将会更新，以包含新添加的策略。策略更改会立即生效。

通过导航到策略来附加聊天机器人策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在聊天机器人策略页面上，选择要附加的策略的名称。
3. 在 Targets (目标) 选项卡上，选择 Attach (附加)。
4. 选择要附加策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OUs（选择）才能找到所需的 OU 或帐户。
5. 选择附加策略。

   目标选项卡上的已附加聊天机器人策略列表会更新，以包含新添加的策略。策略更改会立即生效。

AI services opt-out policies

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

通过导航到根、OU 或账户来附加 AI 服务选择退出策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在Amazon Web Services 账户页面上，导航到要将策略附加到的根、OU 或账户的相应名称并选择其名称。您可能需要展开 OUs（选择）才能找到所需的 OU 或帐户。
3. 在 Policies (策略) 选项卡上的 AI service opt-out policies (AI 服务选择退出策略) 条目中，选择 Attach (附加)。
4. 找到所需的策略，然后选择 Attach policy (附加策略)。

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

通过导航到策略来附加 AI 服务选择退出策略

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

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

Amazon CLI & Amazon SDKs

附加策略

以下代码示例演示如何使用 AttachPolicy。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then calls the
    /// AttachPolicyAsync method to attach the policy to the root
    /// organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var policyId = "p-00000000";
        var targetId = "r-0000";

        var request = new AttachPolicyRequest
        {
            PolicyId = policyId,
            TargetId = targetId,
        };

        var response = await client.AttachPolicyAsync(request);
```

```
            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
 Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考AttachPolicy中的。

CLI

Amazon CLI

将策略附加到根、OU 或账户

示例 1

以下示例演示如何将服务控制策略（SCP）附加到 OU：

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

示例 2

以下示例演示如何将服务控制策略直接附加到账户：

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id 333333333333
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考AttachPolicy中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- 有关 API 的详细信息，请参阅适用AttachPolicy于 Python 的Amazon SDK (Boto3) API 参考。

策略更改会立即影响所附加的根或 OU 下方的所附加账户或所有账户中 IAM 用户和角色的权限

将组织策略与分离 Amazon Organizations

本主题介绍如何使用 Amazon Organizations分离策略。策略定义了您要应用于一组的控制措施 Amazon Web Services 账户。

主题

将策略与分离 Amazon Organizations

最小权限

要从组织根、OU 或账户分离策略，您必须具有运行以下操作的权限：

- `organizations:DetachPolicy`

Note

您无法将最后一个授权策略（SCP 或 RCP）与根目录、组织单位或账户分离。必须始终为每个根、OU 和账户关联至少一个 SCP 和 RCP。

Amazon Web Services Management Console

Service control policies (SCPs)

您可以导航到要从中分离策略的根、OU 或账户，为其分离 SCP。

通过导航到已附加策略的根、OU 或账户来分离 SCP

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在Amazon Web Services 账户页面导航到要分离策略的根、OU 或账户。您可能需要展开 OUs（选
   择▶ ）
   才能找到所需的 OU 或帐户。选择根、OU 或账户的名称。
3. 在 Policies (策略) 选项卡上，选择要分离的 SCP 旁边的单选按钮，然后选择 Detach (分离)。

4. 在确认对话框中，选择 Detach policy (分离策略)。

   所附列表 SCPs 已更新。分离 SCP 引起的策略更改立即生效。例如，分离 SCP 会立即影响以前附加的账户或以前附加的组织根或 OU 下的账户中 IAM 用户和角色的权限。

通过导航到策略来分离 SCP

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Service control policies (服务控制策略) 页面上，选择要从根、OU 或账户分离的策略的名称。
3. 在 Targets (目标) 选项卡上，选择要分离策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OUs（选
   择
   才能找到所需的 OU 或帐户。
4. 选择分离。
5. 在确认对话框中，选择 Detach (分离)。

   所附列表 SCPs 已更新。分离 SCP 引起的策略更改立即生效。例如，分离 SCP 会立即影响以前附加的账户或以前附加的组织根或 OU 下的账户中 IAM 用户和角色的权限。

Resource control policies (RCPs)

您可以通过导航到策略或要与之分离策略的根目录、OU 或账户来分离 RCP。将 RCP 与实体分离后，该 RCP 将不再适用于受现已分离实体影响的任何资源。

> **Note**
>
> 您无法分离策略 **`RCPFullAWSAccess`**
> 该`RCPFullAWSAccess`策略会自动附加到根目录、每个 OU 和组织中的每个账户。您无法分离此政策。

要通过导航到 RCP 所关联的根目录、OU 或账户来断开 RCP

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

2. 在Amazon Web Services 账户页面导航到要分离策略的根、OU 或账户。您可能需要展开 OUs（选
   择▶）
   才能找到所需的 OU 或帐户。选择根、OU 或账户的名称。
3. 在 “策略” 选项卡上，选择要分离的 RCP 旁边的单选按钮，然后选择 “分离”。
4. 在确认对话框中，选择 Detach policy (分离策略)。

   所附列表 RCPs 已更新。因断开 RCP 而导致的政策更改会立即生效。例如，断开 RCP 会立即影响先前关联的账户中的 IAM 用户和角色的权限，或者以前关联的组织根或 OU 下的账户。

通过导航到策略来断开 RCP

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在资源控制策略页面上，选择要与根、OU 或账户分离的策略的名称。
3. 在 Targets (目标) 选项卡上，选择要分离策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OUs（选
   择▶）
   才能找到所需的 OU 或帐户。
4. 选择分离。
5. 在确认对话框中，选择 Detach (分离)。

   所附列表 RCPs 已更新。因断开 RCP 而导致的政策更改会立即生效。例如，断开 RCP 会立即影响先前关联的账户中的 IAM 用户和角色的权限，或者以前关联的组织根或 OU 下的账户。

Declarative policies

您可以通过导航到策略或要与之分离的根目录、OU 或账户来分离声明性策略。

要分离声明式策略，请导航到其所关联的根目录、OU 或账户

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在Amazon Web Services 账户页面导航到要分离策略的根、OU 或账户。您可能需要展开 OUs（选
   择▶）
   才能找到所需的 OU 或帐户。选择根、OU 或账户的名称。

3. 在 “策略” 选项卡上，选择要分离的声明式策略旁边的单选按钮，然后选择 “分离”。
4. 在确认对话框中，选择 Detach policy (分离策略)。

   随附的声明性政策列表已更新。策略更改会立即生效。

通过导航到声明性策略来分离声明性策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在声明性策略页面上，选择要与根、OU 或账户分离的策略的名称。
3. 在 Targets (目标) 选项卡上，选择要分离策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OUs（选
   择▶
   ）
   才能找到所需的 OU 或帐户。
4. 选择分离。
5. 在确认对话框中，选择 Detach (分离)。

   随附的声明性政策列表已更新。策略更改会立即生效。

Backup policies

您可以导航到要分离策略的根、OU 或账户，为其分离备份策略。

通过导航到已附加策略的根、OU 或账户来分离备份策略

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

   附加的备份策略的列表将更新。策略更改会立即生效。

通过导航到策略来分离备份策略

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

   附加的备份策略的列表将更新。策略更改会立即生效。

Tag policies

您可以导航到要分离策略的根、OU 或账户，为其分离标签策略。

通过导航到已附加策略的根、OU 或账户来分离标签策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在Amazon Web Services 账户页面导航到要分离策略的根、OU 或账户。您可能需要展开 OUs（选
   择▶
   ）
   才能找到所需的 OU 或帐户。选择根、OU 或账户的名称。
3. 在 Policies (策略) 选项卡上，选择要分离的标签策略旁边的单选按钮，然后选择 Detach (分离)。
4. 在确认对话框中，选择 Detach policy (分离策略)。

   附加的标签策略的列表将更新。策略更改会立即生效。

通过导航到策略来分离标签策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 Tag policies (标签策略) 页面上，选择要从根、OU 或账户分离的策略的名称。

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

   附加的标签策略的列表将更新。策略更改会立即生效。

Chatbot policies

您可以导航到要分离策略的根、OU 或账户，为其分离聊天机器人策略。

通过导航到该策略附加到的根、OU 或账户来分离聊天机器人策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在Amazon Web Services 账户页面导航到要分离策略的根、OU 或账户。您可能需要展开 OUs（选择）才能找到所需的 OU 或帐户。选择根、OU 或账户的名称。
3. 在策略选项卡上，选择要分离的聊天机器人策略旁边的单选按钮，然后选择分离。
4. 在确认对话框中，选择 Detach policy (分离策略)。

   附加的聊天机器人策略的列表将更新。策略更改会立即生效。

通过导航到策略来分离聊天机器人策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在聊天机器人策略页面上，选择要从根、OU 或账户分离的策略的名称。
3. 在 Targets (目标) 选项卡上，选择要分离策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OUs（选择）才能找到所需的 OU 或帐户。
4. 选择分离。

5. 在确认对话框中，选择 Detach (分离)。

   附加的聊天机器人策略的列表将更新。策略更改会立即生效。

AI services opt-out policies

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

通过导航到已附加策略的根、OU 或账户来分离 AI 服务选择退出策略

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

   附加的 AI 服务选择退出策略的列表会更新。策略更改会立即生效。

通过导航到策略来分离 AI 服务选择退出策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在 AI services opt-out policies (AI 服务选择退出策略) 页面上，选择要从根、OU 或账户分离的策略的名称。
3. 在 Targets (目标) 选项卡上，选择要分离策略的根、OU 或账户旁边的单选按钮。您可能需要展开 OUs（选
   择
   ）
   才能找到所需的 OU 或帐户。
4. 选择分离。
5. 在确认对话框中，选择 Detach (分离)。

   附加的 AI 服务选择退出策略的列表会更新。策略更改会立即生效。

Amazon CLI & Amazon SDKs

附加策略

以下代码示例演示如何使用 DetachPolicy。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
    /// DetachPolicyAsync to detach the policy.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";
        var targetId = "r-0000";

        var request = new DetachPolicyRequest
        {
            PolicyId = policyId,
            TargetId = targetId,
```

```
            };

            var response = await client.DetachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考DetachPolicy中的。

CLI

Amazon CLI

从根、OU 或账户分离策略

以下示例演示了如何从 OU 分离策略：

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DetachPolicy中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- 有关 API 的详细信息，请参阅适用DetachPolicy于 Python 的Amazon SDK (Boto3) API 参考。

政策变更将立即生效，影响关联账户或关联根或 OU 下的所有账户中的 IAM 用户以及角色和资源（如果适用）的权限。

获取有关组织策略的信息

本主题介绍了各种可用来获取您组织中策略的详细信息的方法。这些过程适用于所有 策略类型。您必须先在组织根中启用一个策略类型，然后才能将该类型的策略附加到组织根中的任何实体。

主题

- 列出所有策略
- 列出附加到根、OU 或账户的策略
- 列出策略所关联的所有根和账户 OUs
- 获取有关策略的详细信息

列出所有策略

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

您可以使用 Amazon Command Line Interface (Amazon CLI) 命令 Amazon Web Services Management Console 或 Amazon SDK 操作在或中查看组织中的政策。

Amazon Web Services Management Console

列出组织中的所有策略

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

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

Amazon CLI & Amazon SDKs

以下代码示例演示如何使用 `ListPolicies`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
```

```
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
        var request = new ListPoliciesRequest
        {
            Filter = "SERVICE_CONTROL_POLICY",
            MaxResults = 5,
        };

        var response = new ListPoliciesResponse();
        try
        {
            do
            {
                response = await client.ListPoliciesAsync(request);
                response.Policies.ForEach(p => DisplayPolicies(p));
                if (response.NextToken is not null)
                {
                    request.NextToken = response.NextToken;
                }
            }
            while (response.NextToken is not null);
        }
        catch (AWSOrganizationsNotInUseException ex)
```

```
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
 {policy.Name}\t{policy.Description}";

            Console.WriteLine(policyInfo);
        }
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考ListPolicies中的。

CLI

Amazon CLI

检索特定类型组织中所有策略的列表

以下示例向您展示了如何获取 filter 参数所指定的列表： SCPs

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

输出包括含摘要信息的策略列表：

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
```

```
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
                        "AwsManaged": true,
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
                }
        ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考ListPolicies中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.
```

```
    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- 有关 API 的详细信息，请参阅适用ListPolicies于 Python 的Amazon SDK (Boto3) API 参考。

列出附加到根、OU 或账户的策略

最小权限

要列出附加到您组织中的根、组织部门（OU）或账户的策略，您必须拥有以下权限：

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

Amazon Web Services Management Console

列出直接附加到所指定根、OU 或账户的所有策略

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在Amazon Web Services 账户页面上，选择要查看其策略的根、OU 或账户的名称。您可能需要展开 OUs（选
   择
   ）
   才能找到所需的 OU。

3. 在根、OU 或账户页面上，选择 Policies (策略) 选项卡。

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

Amazon CLI & Amazon SDKs

列出直接附加到所指定根、OU 或账户的所有策略

可以使用以下命令之一列出附加到实体的策略：

- Amazon CLI: list-policies-for-target

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

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

- Amazon SDKs: ListPoliciesForTarget

列出策略所关联的所有根和账户 OUs

最小权限

要列出策略附加到的实体，您必须拥有以下权限：

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

Amazon Web Services Management Console

列出所有关联了指定策略的根和账户 OUs

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

Amazon CLI & Amazon SDKs

列出所有关联了指定策略的根和账户 OUs

可以使用以下命令之一列出具有策略的实体：

- Amazon CLI: list-targets-for-policy

  以下示例显示了指定策略的 root OUs、和账户的所有附件。

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

```
        },
        {
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
        }
    ]
}
```

- Amazon SDKs: ListTargetsForPolicy

获取有关策略的详细信息

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

Amazon Web Services Management Console

获取有关策略的详细信息

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

   策略页面显示有关策略的可用信息，包括 ARN、描述和附加项。

   - Content (内容) 选项卡以 JSON 格式显示策略的当前内容。
   - “目标” 选项卡显示策略所关联的根和账户的列表。 OUs

- Tags (标签) 选项卡显示附加到策略的标签。注意：Tags (标签) 选项卡不可用于 Amazon 托管式策略。

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

Amazon CLI & Amazon SDKs

以下代码示例演示如何使用 `DescribePolicy`。

CLI

Amazon CLI

获取有关策略的信息

以下示例演示如何请求有关策略的信息：

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

输出包括一个策略对象，其中包含有关策略的详细信息：

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DescribePolicy中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- 有关 API 的详细信息，请参阅适用DescribePolicy于 Python 的Amazon SDK (Boto3) API 参考。

使用删除组织政策 Amazon Organizations

当您不再需要某项策略并且将其与所有组织单位 (OUs) 和账户分离后，可以将其删除。

本主题介绍如何使用删除策略 Amazon Organizations。策略定义了您要应用于一组的控制措施 Amazon Web Services 账户。

主题

使用删除策略 Amazon Organizations

当登录到您组织的管理账户时，您可以删除您的组织中不再需要的策略。

必须先将某个策略从所有附加实体中分离，然后才能删除该策略。

> **Note**
>
> - 您无法删除任何 Amazon 托管 SCP，例如名为的 SCP。`FullAWSAccess`
> - 您无法删除任何 Amazon 托管 RCP，例如名为的 RCP。`RCPFullAWSAccess`

> **最小权限**
>
> 要删除策略，您需要有运行以下操作的权限：
>
> - `organizations:DeletePolicy`

Amazon Web Services Management Console

Service control policies (SCPs)

删除 SCP

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

Resource control policies (RCPs)

删除 RCP

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

Declarative policies

删除声明式策略

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

Backup policies

删除备份策略

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

4. 在页面的顶部，选择 Delete (删除)。
5. 在确认对话框上，输入策略的名称，然后选择 Delete (删除)。

Tag policies

删除标签策略

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

Chatbot policies

删除聊天机器人策略

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

AI services opt-out policies

删除 AI 服务选择退出策略

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

2. 在 AI services opt-out policies (AI 服务选择退出策略) 页面上，选择要删除的策略的名称。
3. 您必须先从所有根和账户中分离要删除的策略。 OUs选择 Targets (目标) 选项卡，选择显示在 Targets (目标) 列表中的每个根、OU 或账户旁边的单选按钮，然后选择 Detach (分离)。在确认对话框中，选择 Detach (分离)。重复操作，直到删除所有目标。
4. 在页面的顶部，选择 Delete (删除)。
5. 在确认对话框上，输入策略的名称，然后选择 Delete (删除)。

Amazon CLI & Amazon SDKs

删除策略

以下代码示例演示如何使用 `DeletePolicy`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
```

```
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";

            var request = new DeletePolicyRequest
            {
                PolicyId = policyId,
            };

            var response = await client.DeletePolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted Policy: {policyId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete Policy: {policyId}.");
            }
        }
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考DeletePolicy中的。

CLI

Amazon CLI

删除策略

以下示例演示如何删除组织的策略。该示例假设您之前已将策略与所有实体分离：

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DeletePolicy中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- 有关 API 的详细信息，请参阅适用DeletePolicy于 Python 的Amazon SDK (Boto3) API 参考。

为资源添加标签 Amazon Organizations

标签是一种自定义属性标签，您可以将其添加到 Amazon 资源中，以便于识别、组织和搜索资源。每个标签具有两个部分：

- 标签键（例如，CostCenter、Environment 或 Project）。标签键最大长度可为 128 个字符，且不区分大小写。
- 标签值（例如，111122223333 或 Production）。标签值的最大长度可为 256 个字符，与标签键一样区分大小写。可以将标签的值设为空的字符串，但是不能将其设为空值。省略标签值与使用空字符串效果相同。

有关标签键或值中允许使用哪些字符的详细信息，请参阅《Resource Groups 标记 API 参考》中的标签 API 的标签参数。

您可使用标签，按用途、所有者、环境或其他标准对资源进行分类。有关更多信息，请参阅为Amazon资源添加标签的最佳实践。

> **Tip**
>
> 使用标签策略帮助在组织账户中跨资源标准化标签实现工作。

主题

注意事项

Amazon Organizations 当你登录到管理账户时，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
- 策略

您可以在以下时间添加标签

- 在创建资源时 – 在 Organizations 控制台中指定标签，或将 Tags 参数和一个 Create API 操作一同使用来指定标签。这不适用于组织的根。
- 在创建资源后 – 使用 Organizations 控制台，或调用 TagResource 操作。

其他考虑因素

您可以使用控制台或调用操作 Amazon Organizations 来查看中任何可标记资源的标签。ListTagsForResource

您可以使用控制台指定要删除的键，或者调用 UntagResource 操作，来从资源中删除标签。

使用标签

标签可让您根据对您有用的任何类别对组织内的资源进行分组，从而帮助您整理资源。例如，您可以分配一个跟踪所述部门的“Department”（部门）标签。您可以分配一个“Environment”（环境）标签来跟踪给定资源是否属于 Alpha、Beta、Gamma 或生产环境。

您还可以使用标签执行以下操作：

- 对您的资源强制执行标签标准。
- 控制谁能访问您的资源。

添加、更新和删除标签

当您登录到组织的管理账户时，您可以将标签添加到组织的资源中。

在创建资源时添加标签

最小权限

要在创建资源时向资源添加标签，您需要以下权限：

- 创建指定类型资源的权限
- `organizations:TagResource`
- `organizations:ListTagsForResource` – 仅当使用 Organizations 控制台时才需要

在创建以下资源时，可以添加附加到它们的标签键和值。

- Amazon Web Services 账户
  - 创建账户
  - 邀请账户
- 组织部门 (OU)
- 策略
  - 服务控制策略
  - 资源控制政策
  - 声明性政策
  - 备份策略
  - 标签策略
  - 聊天机器人策略
  - AI 服务选择退出策略

组织根是在您最初创建组织时创建的，因此您只能将标签作为现有资源添加到组织中。

为现有资源添加或更新标签

您还可以添加新标签或更新附加到现有资源的标签值。

最小权限

要向组织中的资源添加或更新标签，您需要拥有以下权限：

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

要从组织中的资源中删除标签，您需要拥有以下权限：

- `organizations:UntagResource`

Amazon Web Services Management Console

添加、更新或删除现有资源的标签

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 导航到并选择账户、根、OU 或策略，并点击其名称以打开其详细信息页面。
3. 在标签选项卡上，选择管理标签。
4. 您可以添加新标签、修改现有标签的值或删除标签。

   要添加标签，选择 Add tag (添加标签)，然后输入标签的 Key (键) 和 Value (值)（可选）。

   要删除标签，请选择移除。

   标签键和值区分大小写。为希望标准化的标签使用大写字母。您还必须遵守适用的任何标签策略的要求。
5. 根据需要，多次重复执行上一步骤。
6. 选择 Save changes（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 SDKs: 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 SDKs: UntagResource

与其他 Amazon Organizations 人一起使用 Amazon Web Services 服务

您可以使用可信访问权限来启用您指定的受支持 Amazon 服务（称为可信服务），以代表您在组织及其账户中执行任务。这涉及向可信服务授予权限，但不会以其他方式影响用户或角色的权限。启用访问权限后，只要需要该IAM角色，可信服务就可以在组织中的每个账户中创建一个名为服务关联角色的角色。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

当该选项可用时，我们强烈建议您仅使用可信服务的控制台或其 Amazon CLI 或API操作等效控制台来启用和禁用可信访问。这使得信任服务在启用信任访问权限时执行任何必需的初始化，例如在禁用信任访问权限时创建任何必需的资源和任何必需的资源清理。
有关如何使用信任服务启用或禁用对组织的信任服务访问的信息，请参阅Amazon Web Services 服务 你可以和它一起使用 Amazon Organizations中了解详情链接下的支持信任访问权限列。
如果您使用 Organizations 控制台、CLI命令或API操作禁用访问权限，则会导致以下操作发生：

- 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。
- 除非附加到您的角色的IAM策略明确允许这些操作，否则该服务无法再在组织中的成员账户中执行任务。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

可信访问需要两个服务的权限： Amazon Organizations 和可信服务。要允许可信访问，请选择以下场景之一：

- 如果您拥有同时拥有同时 Amazon Organizations 拥有可信服务权限的证书，请使用可信服务提供的工具（控制台或 Amazon CLI）启用访问权限。这样，该服务就可以 Amazon Organizations 代表您启用可信访问权限，并创建该服务在您的组织中运行所需的任何资源。

  这些凭证的最低权限如下：

  - `organizations:EnableAWSServiceAccess`。您还可以将 `organizations:ServicePrincipal` 条件键与此操作搭配使用，以将这些操作发出的请求限制为已批准的服务委托人名称列表。有关更多信息，请参阅 条件键。
  - `organizations:ListAWSServiceAccessForOrganization`— 如果您使用 Amazon Organizations 控制台，则为必填项。
  - 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。
- 如果一个人拥有在中具有权限的证书， Amazon Organizations 但其他人拥有在可信服务中拥有权限的证书，请按以下顺序执行这些步骤：

  1. 拥有权限的凭证的人员 Amazon Organizations 应使用 Amazon Organizations 控制台 Amazon CLI、或，为可信服务启用可信访问权限。 Amazon SDK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`— 只有在使用 Amazon Organizations 控制台时才需要

     有关在中启用可信访问的步骤 Amazon Organizations，请参阅如何允许或禁止可信访问。
  2. 拥有在可信服务中具有权限的凭证的人可启用此服务以使用 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Amazon Web Services 服务 你可以和它一起使用 Amazon Organizations处的服务特定说明。

禁止可信访问所需的权限

当您不再需要允许可信服务在您的组织或其账户上运行时，请选择以下场景之一。

> **Important**
>
> 禁止可信服务访问不 会阻止具有相应权限的用户和角色使用该服务。要完全阻止用户和角色访问 Amazon 服务，可以移除授予该访问IAM权限的权限，也可以使用中的服务控制策略 (SCPs) Amazon Organizations。
> 您只能SCPs申请成员账户。 SCPs不适用于管理账户。建议您不要在管理账户中运行服务。取而代之的是，在成员帐户中运行它们，您可以通过使用来控制安全性SCPs。

- 如果您拥有同时 Amazon Organizations 对可信服务具有权限的证书，请使用可信服务可用的工具（控制台或 Amazon CLI）禁用访问权限。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。
  - `organizations:ListAWSServiceAccessForOrganization`— 如果您使用 Amazon Organizations 控制台，则为必填项。
  - 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。
- 如果中具有权限的证书 Amazon Organizations 不是在可信服务中具有权限的证书，请按以下顺序执行以下步骤：

  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Amazon Web Services 服务 你可以和它一起使用 Amazon Organizations处的服务特定说明。
  2. 然后，拥有权限的 Amazon Organizations 人员可以使用 Amazon Organizations 控制台 Amazon CLI、或 Amazon SDK来禁用对可信服务的访问权限。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`— 只有在使用 Amazon Organizations 控制台时才需要

     有关在中禁用可信访问的步骤 Amazon Organizations，请参阅如何允许或禁止可信访问。

如何允许或禁止可信访问

如果您仅拥有其他服务的权限，Amazon Organizations 并且想要代表其他 Amazon 服务的管理员启用或禁用对组织的可信访问权限，请使用以下步骤。

Important

当该选项可用时，我们强烈建议您仅使用可信服务的控制台或其 Amazon CLI 或API操作等效控制台来启用和禁用可信访问。这使得信任服务在启用信任访问权限时执行任何必需的初始化，例如在禁用信任访问权限时创建任何必需的资源和任何必需的资源清理。
有关如何使用信任服务启用或禁用对组织的信任服务访问的信息，请参阅Amazon Web Services 服务 你可以和它一起使用 Amazon Organizations中了解详情链接下的支持信任访问权限列。
如果您使用 Organizations 控制台、CLI命令或API操作禁用访问权限，则会导致以下操作发生：

- 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。
- 除非附加到您的角色的IAM策略明确允许这些操作，否则该服务无法再在组织中的成员账户中执行任务。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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
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. 如果您正在启用访问权限，请告诉其他 Amazon 服务的管理员，他们现在可以启用其他服务了 Amazon Organizations。

禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
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操作来启用或禁用可信服务访问权限：

- Amazon CLI: Amazon 组织 enable-aws-service-access
- Amazon CLI: Amazon 组织 disable-aws-service-access
- Amazon API: E A nableAWSService ccess
- Amazon API: D A isableAWSService ccess

Amazon Organizations 和服务相关角色

Amazon Organizations 使用IAM服务相关角色使可信服务能够在贵组织的成员账户中代表您执行任务。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。服务相关角色具有预定义的IAM权限，允许受信任的服务仅在该账户内执行特定任务。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。只

有 Amazon Organizations 服务本身才能扮演这个角色。该角色具有允许 Amazon Organizations 为其他 Amazon Web Services 服务人创建服务相关角色的权限。此服务相关角色存在于所有组织中。

如果您的组织仅启用了整合账单功能（但我们建议不要这样做），则绝不使用名为 AWSServiceRoleForOrganizations 的服务相关角色并且可删除它。如果您之后要在组织中启用所有功能，则此角色是必需的并且您必须还原它。在您开始启用所有功能的流程时，将进行以下检查：

- 对于已受邀加入组织的每个成员账户 – 账户管理员将收到同意启用所有功能的请求。要成功同意此请求，如果服务相关角色 (organizations:AcceptHandshake) 不存在，此管理员必须同时具有 和iam:CreateServiceLinkedRole AWSServiceRoleForOrganizations 权限。如果 AWSServiceRoleForOrganizations 角色已存在，则管理员只需 organizations:AcceptHandshake 权限即可同意该请求。管理员同意请求后，如果服务相关角色尚不存在，则 Amazon Organizations 创建该角色。
- 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 SCPs永远不会影响与服务相关的角色。这些角色不受任何SCP限制。

使用 AWSServiceRoleForDeclarativePoliciesEC2Report 服务相关角色

Organizations 使用AWSServiceRoleForDeclarativePoliciesEC2Report服务相关角色来描述成员账户的账户属性状态，以创建声明性政策报告。角色的权限在中定义Amazon 托管策略：DeclarativePoliciesEC2Report。

Amazon Web Services 服务 你可以和它一起使用 Amazon Organizations

借助 Amazon Organizations 此功能，您可以 Amazon Web Services 账户 将多个账户整合到一个组织中，从而大规模执行账户管理活动。合并账户可简化您使用其他账户的方式 Amazon Web Services 服务。您可以利用 selec Amazon Web Services 服务 t 中 Amazon Organizations 提供的多账户管理服务，对属于您组织的所有成员账户执行任务。

下表列出了 Amazon Web Services 服务 您可以与一起使用的服务 Amazon Organizations，以及在组织范围内使用每项服务的好处。

可信访问-您可以启用兼容的 Amazon 服务，以便在组织 Amazon Web Services 账户 中的所有部门执行操作。有关更多信息，请参阅 与其他 Amazon Organizations 人一起使用 Amazon Web Services 服务。

的委托管理员 Amazon Web Services 服务-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该组织账户的管理员。有关更多信息，请参阅 与 Organizations 配合使用的 Amazon Web Services 服务委派管理员。

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon 账户管理 管理组织所有内容 Amazon Web Services 账户 的详细信息和元数据。	管理组织 Amazon Web Services 账户 中所有人的账户详情、备用联系人和区域。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Application Migration Service Amazon Application Migration Service 允许公司 lift-and-shift 访问 Amazon 大量物理、虚拟或云服务器，而不会出现兼容性问题、性能中断或转换窗口过长。	您可以管理跨多个账户的大规模迁移任务。	 是 了解更多	 了解更多	是
Amazon Artifact 下载 Amazon 安全合规报告，例如 ISO 和 PCI 报告。	您可以代表您组织内的所有账户接受协议。	 是 了解更多		否

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Audit Manager 自动化持续收集证据，以帮助您审核云服务的使用情况。	持续审计您组织中多个账户的 Amazon 使用情况，以简化评估风险和合规性的方式。	 是 了解更多	 是 了解更多	
Amazon Backup 管理和监控您组织中的所有账户的备份。	您可以为整个组织或组织单位中的账户组配置和管理备份计划（OUs）。您可以集中监控所有账户的备份。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Billing and Cost Management 概述您的 Amazon 云财务管理数据，帮助您更快、更明智地做出决策。	允许拆分成本分配数据检索 Amazon Organizations 信息（如果适用），并收集您选择使用的分割成本分配数据服务的遥测数据。 有关更多信息，请参阅什么是 Amazon Billing and Cost Management？ 在《账单和成本管理》用户指南中。	 是 了解更多	 否	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon CloudFormation Stacksets 通过单个操作跨多个账户和区域创建、更新或删除堆栈。	管理账户或委托管理员账户中的用户可以创建具有服务托管权限的堆栈套，该堆栈套会将堆栈实例部署到您组织中的账户。	 是 了解更多	 了解更多	是
Amazon CloudTrail 允许对您的账户进行监管、合规性检查、操作审核和风险审计。	管理账户或委托管理员账户中的用户可以创建组织跟踪或事件数据存储，记录组织中所有账户的所有事件。	 是 了解更多	 了解更多	是

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon CloudWatch 实时监控您的 Amazon 资源和运行 Amazon 的应用程序。您可以使用 CloudWatch 来收集和跟踪指标，这些指标是您可以衡量资源和应用程序的变量。	CloudWatch 用于从 CloudWatch 控制台的中央视图发现和了解 Amazon 资源的遥测配置状态。通过与 Organizations 集成，您可以修改组织支持的 CloudWatch 配置。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Compute Optimizer 获取 Amazon 计算优化建议。	您可以分析组织账户中的所有资源以获取优化建议。 有关更多信息，请参阅《Amazon Compute Optimizer 用户指南》中的 Compute Optimizer 支持的账户。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Config 评估、审计和评价您的 Amazon 资源的配置。	您可以在组织范围内查看合规性状态。您还可以使用 Amazon Config API 操作来管理组织 Amazon Web Services 账户 中所有部门的 Amazon Config 规则和一致性包。 您可以使用委托管理员账户聚合 Amazon Organizations中组织所有成员账户中的资源配	 是 了解更多	 是 了解更多： Config 规则 一致性包 多账户多区域数据聚合	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
	置和合规性数据。有关更多信息，请参阅 Amazon Config 开发人员指南中的注册委托管理员。			

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Control Tower 设置和管理安全、合规的多账户 Amazon 环境。	您可以为所有 Amazon 资源设置 landing zone，即多账户环境。该环境包括一个组织和组织实体。您可以使用此环境对所有人强制执行合规性法规 Amazon Web Services 账户。 有关更多信息，请参阅《Amazon Control Tower 用户指南》中的 操作方法	 是 了解更多	 否	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
	Amazon Control Tower和通过 Amazon Organizations管理账户。			

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon 成本优化中心 收集各 Amazon 优化产品的成本建议。	您可以轻松识别、筛选和汇总跨 Amazon Organizations 成员账户和 Amazon 地区 Amazon 的成本优化建议。 有关更多信息，请参阅《成本优化中心用户指南》中的 Cost Optimization Hub。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Detective 可从日志数据生成可视化，以分析、调查和快速识别安全结果或可疑活动的根本原因。	您可以将 Amazon D Amazon Organizations etective 与集成，确保您的侦探行为图能够让您了解所有组织账户的活动。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon DevOps Guru 可以分析操作数据以及应用程序指标和事件，以识别偏离正常操作模式的行为。当 DevOps Guru 检测到操作问题或风险时，用户会收到通知。	您可以与集成 Amazon Organizations ，以管理整个组织中所有账户的见解。您可以委托一位管理员来查看、排序和筛选来自所有账户的见解，以获取所有受监控的应用程序在组织范围内的运行状况。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Directory Service 在 Amazon 云端设置和运行目录，或者将你的 Amazon 资源与现有的本地 Microsoft Active Directory 连接起来。	您可以 Amazon Directory Service 与集成，Amazon Organizations 以便在一个区域内的多个账户和任何 VPC 之间实现无缝目录共享。	 是 了解更多	 否	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon EventBridge 实时监控您的 Amazon 资源和运行 Amazon 的应用程序。	您可以允许在组织中的所有账户之间共享所有亚马逊 EventBridge 活动（以前称为 Amazon CloudWatch Events）。 有关更多信息，请参阅《亚马逊 EventBridge 用户指南》Amazon Web Services 账户中的在两者之间发送和接收亚马逊	 否	 否	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
	EventBridge 事件。			
Amazon Elastic Compute Cloud Amazon VPC IP 地址管理器 (IPAM) 在云中提供按需、可扩展的 Amazon 计算容量。	使用声明式策略功能时，让 Organizations 管理员能够创建一份报告，说明其组织中账户的现有配置。	 是 了解更多		否
Amazon Firewall Manager 跨账户和应用程序集中配置和管理 Web 应用程序防火墙规则。	您可以集中配置和管理组织中各个账户的 Amazon WAF 规则。	 是 了解更多	 了解更多	是

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon GuardDuty GuardDuty 是一项持续的安全监控服务，用于分析和处理来自各种数据源的信息。它使用威胁情报源和机器学习来标识您 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 GuardDuty 组织中的所有账户。添加成员帐户会自动启用 GuardDuty 所选帐户中的这些帐户 Amazon Web Services 区域。您还可以自动 GuardDuty 激活添加到组织中的新帐户。 有关更多信息，请参	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
	阅亚马逊 GuardDuty 用户指南中的GuardDut 和 Organizations。			
Amazon Health 轻松了解可能影响资源性能或 Amazon Web Services 服务可用性问题的事件。	您可以汇总组织中各个账户 Amazon Health 的事件。	 是 了解更多	 了解更多	是

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Identity and Access Management 安全地控制对 Amazon 资源的访问。	您可以使用 IAM 中服务上次访问的数据，以帮助您更好地了解组织中的 Amazon 活动。您可以使用这些数据来创建和更新服务控制策略 (SCPs)，这些策略将访问权限仅限于您的组织账户使用的 Amazon 服务。 有关示例，请参阅《IAM 用户指南》中的使用数	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
	据来细化组织部门的权限。 IAM 根访问管理允许您集中管理根用户证书，并对成员账户执行特权任务。			
IAM Access Analyzer 分析您 Amazon 环境中基于资源的策略，以确定向信任区域之外的委托人授予访问权限的任何策略。	您可以指定成员账户作为 IAM 访问分析器的管理员。 有关更多信息，请参阅《IAM 用户指南》中的启用访问分析器。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Inspector 自动扫描您的 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，以发现软件漏洞和意外网络泄露。	可以委托一位管理员来启用或禁用对成员账户的扫描、查看从整个组织汇总的结果数据、创建和管理禁止规则。 有关更多信息，请参阅《Amazon Inspector 用户指南》中的使用 Amazon Organizations管理多个账户。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon License Manager 简化将软件许可证迁移到云中的过程。	您可以在整个组织中启用计算资源的跨账户发现。	 是 了解更多	 了解更多	是

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Macie 使用机器学习发现您的业务关键型内容并对其进行分类，以帮助您满足数据安全和隐私要求。它会持续评估您存储在 Amazon S3 中的内容，并通知您潜在的问题。	您可以为您组织中的所有账户配置 Amazon Macie，以便从指定的 Macie 管理员账户跨所有账户获取 Amazon S3 中所有数据的统一视图。您可以将 Macie 配置为随着组织壮大而自动保护新账户中的资源。系统会提醒您修正整个组织中的 S3 存储桶中的策	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
	略错误配置。			
Amazon Managed Services (AMS) 自助报告 (SSR) 从各种原生 Amazon 服务收集数据，并提供对主要 AMS 产品报告的访问权限。SSR 提供的信息可用于支持运营、配置管理、资产管理、安全管理和合规性。	您可以启用 “聚合 SSR” 功能，该功能允许客户通过您的管理帐户或委派的管理员帐户查看组织中的整合自助服务报告。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Web Services Marketplace 一个精挑细选的数字化产品目录，您通过它可以轻松地查找、购买、部署和管理构建解决方案及运营业务所需的第三方软件、数据和服务。	您可以在组织中的各个账户之间共享 Amazon Web Services Marketplace 订阅和购买的许可证。	 是 了解更多	 否	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Web Services Marketplace 私人市场 为您提供广泛的可用产品目录 Amazon Web Services Marketplace，以及对这些产品的精细控制。	使您能够创建多个私有市场体验，这些体验与您的整个组织、一个或多个账户 OUs、组织中的一个或多个账户相关联，每个账户都有自己的一套经批准的产品。您的 Amazon 管理员还可以通过公司或团队的徽标、消息和配色方案将公司品牌应用于每一次	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
	私人市场体验。			
Amazon Web Services Marketplace 采购见解仪表板 使您能够查看组织中所有 Amazon 账户中所有 Amazon Web Services Marketplace 采购的协议和成本分析数据。	Amazon Web Services Marketplace procurement insights 控制面板监听组织变更，例如加入组织的账户，并汇总相应协议的数据以构建其仪表板。	 是 了解更多	 了解更多	是

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon 网络管理器 使您能够跨 Amazon 账户、区域和本地位置集中管理您的 Amazon Cloud WAN 核心网络和 T Amazon ransit Gateway 网络。	您可以使用组织内的多个 Amazon 账户中的传输网关及其关联资源，集中管理和监控您的全球网络。	 是 了解更多	 是 了解更多	
Amazon Q 开发者版 Amazon Q Developer 是一款由人工智能驱动的生成式对话助手，可以帮助您理解、构建、扩展和操作 Amazon 应用程序。	Amazon Q 开发者版的付费订阅版本需要 Organizations 集成。	 是 了解更多	 否	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Resource Access Manager 与其他账户共享您拥有的指定 Amazon 资源。	您可以在组织内共享资源，而无需交换其他邀请。您可以共享的资源包括 Route 53 Resolver 规则、按需容量预留等。 有关共享容量预留的信息，请参阅《亚马逊 EC2 用户指南》或《亚马逊 EC2 用户指南》。 有关可共享资源的列表，请参阅《Amazon RAM	 是 了解更多	 否	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
	用户指南》中的可共享资源。			
Amazon 资源探索器 使用类似互联网搜索引擎的体验来探索您的资源。	启用多账户搜索。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Security Hub 查看您的安全状态，Amazon 并根据安全行业标准和最佳实践检查您的环境。	您可以为组织的所有账户（包括添加新账户）自动启用 Security Hub。这扩大了 Security Hub 检查和调查结果的覆盖范围，从而可让您更准确地了解您的整体安全状况。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon S3 Storage Lens 存储统计管理工具 通过切实可行的建议，您可以了解 Amazon S3 Storage 使用情况和活动指标。	配置 Amazon S3 Storage Lens，以便了解 Amazon S3 存储使用情况和活动趋势，以及组织中所有成员账户的建议。	 是 了解更多	 了解更多	是
Amazon 安全事件响应 Amazon 安全服务，提供全天候的人工辅助安全事件支持，帮助客户快速响应网络安全事件，例如凭据盗窃和勒索软件攻击。	为整个组织提供安全保障。	 是 了解更多	 了解更多	是

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Security Lake Amazon Security Lake 可将来自云端、本地和自定义源的安全数据，集中到您账户中存储的数据湖中。	创建一个数据湖来收集账户中的日志和事件。	 是 了解更多	 了解更多	是
Amazon Service Catalog 创建和管理获准在 Amazon 上使用的 IT 服务的目录。	无需共享投资组合，即可更轻松地跨账户共享投资组合和复制产品 IDs。	 是 了解更多	 了解更多	是
服务配额 从中央位置查看和管理您的服务配额（也称为限制）。	您可以创建一个配额请求模板，以在创建组织账户时自动请求提升配额。	 是 了解更多		否

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon IAM Identity Center 为您的所有账户和云应用程序提供单一登录访问。	用户可以使用其公司凭据登录 Amazon 访问门户，并访问其分配的管理账户或成员账户中的资源。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Systems Manager 实现对 Amazon 资源的可见性和控制。	您可以使用 Systems Manager Explorer 同步组织 Amazon Web Services 账户 中所有人的操作数据。 通过使用 Systems Manager Change Manager，您可以从委托管理员账户管理组织中所有成员账户的更改模板、批准和报告。	 是 了解更多	 是 了解更多	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon 用户通知服务 Amazon 通知的中心位置。	您可以集中配置和查看组织中各个账户的通知。	 是 了解更多	 了解更多	是
标签策略 在组织账户中跨资源使用标准化标签。	您可以创建标签策略来定义特定资源和资源类型的标记规则，然后将这些策略附加到组织实体和账户，以强制执行这些规则。	 是 了解更多		否

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon Trusted Advisor Trusted Advisor 检查您的 Amazon 环境，并在有机会节省资金、提高系统可用性和性能或帮助填补安全漏洞时提出建议。	对组织 Amazon Web Services 账户 中的所有人进行 Trusted Advisor 检查。	 是 了解更多	 是 了解更多	
Amazon Well-Architected Tool 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 架构最佳实践进行比较。	使 Org Amazon WA Tool anizations 和 Organizations 的客户都能简化与其组织中其他成员共享 Amazon WA Tool 资源的流程。	 是 了解更多	 否	

Amazon 服务	与一起使用的好处 Amazon Organizations	支持可信访问	支持委托管理员	
Amazon VPC IP 地址管理器（IPAM） IPAM 是一项 VPC 功能，可让您更轻松地规划、跟踪和监控工作负载的 IP 地址。Amazon	监控整个组织的 IP 地址使用情况，并在成员账户之间共享 IP 地址池。	 是 了解更多	 了解更多	是
Amazon VPC Reachability Analyzer Reachability Analyzer 是一种配置分析工具，使您能够在虚拟私有云中的源资源和目标资源之间执行连接测试（ ）。VPCs	跟踪组织中各个账户的路径。	 是 了解更多	 了解更多	是

Amazon 账户管理 和 Amazon Organizations

Amazon 账户管理 帮助您管理组织 Amazon Web Services 账户 中所有人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 账户管理 用户指南》中的在您的组织中使用 Amazon 账户管理。

使用以下信息来帮助您集 Amazon 账户管理 成 Amazon Organizations。

启用账户管理可信访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

账户管理需要具有可信访问权限， Amazon Organizations 然后才能将成员账户指定为组织此服务的委托管理员。

您只能使用 Organizations 工具启用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon 账户管理。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon 账户管理” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon 账户管理

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon 账户管理 zations 中启用可信服务。

```
$ 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: E A nableAWSService ccess

禁用账户管理可信访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Amazon Organizations 管理账户中的管理员才能使用禁用可信访问 Amazon 账户管理。

您只能使用 Organizations 工具禁用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon 账户管理。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon 账户管理” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。 Amazon 账户管理

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

运行以下命令在 Organiz Amazon 账户管理 ations 中禁用可信服务。

```
$ 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: D isableAWSService 访问权限

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 管理账户中的用户或角色能够将某个成员账户配置为组织的账户管理委托管理员。

有关如何配置委托策略的一般说明，请参阅 使用创建基于资源的授权策略 Amazon Organizations。

Amazon CLI, Amazon API

如果要使用 Amazon CLI或其中一个配置委派管理员帐户 Amazon SDKs，则可以使用以下命令：

- 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，将账户服务委托人标识`account.amazonaws.com`为参数。

Amazon Application Migration Service （应用程序迁移服务）和 Amazon Organizations

Amazon Application Migration Service 简化、加快了将应用程序迁移到并降低了迁移到的成本。Amazon通过 Organizations 集成，您可以使用全局视图功能来管理跨多个账户的大规模迁移。有关更多信息，请参阅《Application Migration Service 用户指南》中的 Setting up your Amazon Organizations。

使用以下信息来帮助您集 Amazon Application Migration Service 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Application Migration Service 在您组织中的组织账户内执行支持的操作。

只有在禁用 Application Migration Service 与 Organizations 之间的可信访问，或者从组织中移除该成员账户后，才能删除或修改此角色。

- `AWSServiceRoleForApplicationMigrationService`

Application Migration Service 使用的服务主体

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Application Migration Service 使用的服务相关角色为以下服务主体授予访问权限：

- `mgn.amazonaws.com`

启用与 Application Migration Service 的可信访问

启用与 Application Migration Service 的可信访问后，您可以使用全局视图功能，从而管理跨多个账户的大规模迁移。全局视图提供了可见性，并能够在不同 Amazon 账户中的源服务器、应用程序和波浪上执行特定操作。有关更多信息，请参阅Amazon Application Migration Service 用户指南中的设置 Amazon Organ izations。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 Amazon Application Migration Service 控制台或控制台启用可信访问。 Amazon Organizations

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Application Migration Service 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Application Migration Service 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon Application Migration Service提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 Amazon Application Migration Service 控制台或工具启用可信访问，则无需完成这些步骤。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Application Migration Service。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon Application Migration Service” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon Application Migration Service

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Application Migration Service zations 中启用可信服务。

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal mgn.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- Amazon API: E A nableAWSService ccess

禁用与 Application Migration Service 的可信访问

只有 Organizations 管理账户中的管理员才可以禁用与 Application Migration Service 的可信访问。

您可以使用 Amazon Application Migration Service 或 Amazon Organizations 工具禁用可信访问。

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Application Migration Service 控制台或工具来禁用与 Organizations 的集成。这允许 Amazon Application Migration Service 执行它需要的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 Amazon Application Migration Service提供的工具禁用集成时，才会使用这些步骤进行处理。
> 如果您使用 Amazon Application Migration Service 控制台或工具禁用可信访问，则无需完成这些步骤。

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Application Migration Service。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon Application Migration Service” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。 Amazon Application Migration Service

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Application Migration Service ations 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。

- Amazon API: D A isableAWSService ccess

为 Application Migration Service 启用委派管理员账户

将成员账户指定为组织的委派管理员后，该账户中的用户和角色将能够执行本来只能由组织管理账户中的用户或角色执行的 Application Migration Service 管理操作。这有助于将组织的管理与 Application Migration Service 的管理分开。有关更多信息，请参阅《Application Migration Service 用户指南》中的 Setting up your Amazon Organizations。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色才能将某个成员账户配置为组织中的 Application Migration Service 委派管理员。

Amazon CLI, Amazon API

如果要使用 Amazon CLI或其中一个配置委派管理员帐户 Amazon SDKs，则可以使用以下命令：

- Amazon CLI:

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

- Amazon SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，将账户服务标识`mgn.amazonaws.com`为参数。

为 Application Migration Service 禁用委派管理员

只有 Organizations 管理账户中的管理员才能移除 Application Migration Service 的委派管理员。您可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或SDK操作移除委派的管理员。

Amazon Artifact 和 Amazon Organizations

Amazon Artifact 是一项允许您下载 Amazon 安全合规性报告（例如ISO和PCI报告）的服务。使用该功能 Amazon Artifact，即使添加了新的报告和帐户，组织管理账户中的用户也可以自动代表组织中的所有成员账户接受协议。成员账户用户可以查看和下载协议。有关更多信息，请参阅《Amazon Artifact 用户指南》中的 Arti Amazon fact 中管理多个账户的协议。

使用以下信息来帮助您集 Amazon Artifact 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色 Amazon Artifact 允许在组织中的组织账户中执行支持的操作。

只有在禁用 Amazon Artifact 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

尽管您可以在删除组织的成员账户时删除或修改此角色，但我们不建议这样操作。

不鼓励修改角色，因为这可能会导致跨服务混淆代理等安全问题。要了解有关防范混淆代理的更多信息，请参阅Amazon Artifact 《用户指南》中的跨服务代理问题防范。

- `AWSServiceRoleForArtifact`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。使用的服务相关角色向以下服务主体 Amazon Artifact 授予访问权限：

- `artifact.amazonaws.com`

使用 Amazon Artifact启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Organizations 工具启用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Artifact。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon Artifact” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon Artifact

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Artifact zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- Amazon API: E A nableAWSService ccess

使用 Amazon Artifact禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Amazon Organizations 管理账户中的管理员才能使用禁用可信访问权限 Amazon Artifact。

您只能使用 Organizations 工具禁用可信访问。

Amazon Artifact 需要使用可信访问权限 Amazon Organizations 才能使用组织协议。如果您在使用组织协议 Amazon Organizations 时使用禁用可信访问，则它会因为无法访问组织而停止运行。 Amazon Artifact 您接受的任何组织协议都将 Amazon Artifact 保留，但无法被访问 Amazon Artifact。 Amazon Artifact 创造的 Amazon Artifact 角色仍然存在。如果您之后重新允许可信访问，则 Amazon Artifact 将继续像以前一样运行，而无需您重新配置该服务。

从组织中删除的独立账户不再有权访问任何组织协议。

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Artifact。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon Artifact” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。 Amazon Artifact

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Artifact ations 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。

- Amazon API: D A isableAWSService ccess

Amazon Audit Manager 和 Amazon Organizations

Amazon Audit Manager 帮助您持续审计 Amazon 使用情况，以简化评估风险以及对法规和行业标准的合规性的方式。Audit Manager 可自动收集证据，以便更轻松地评估您的策略、过程和活动是否有效运行。当需要进行审计时，Audit Manager 可帮助您管理利益攸关方对控件的审核，并帮助您以更少的人工工作量生成可审计的报告。

将 Audit Manager 与集成后 Amazon Organizations，您可以将来自组织的多个证据纳入评估范围，从而 Amazon Web Services 账户 从更广泛的来源收集证据。

有关更多信息，请参阅《Audit Manager 用户指南》中的 “启用 Amazon 组织”。

使用以下信息来帮助您集 Amazon Audit Manager 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Audit Manager 在您组织中的组织账户内执行支持的操作。

只有在禁用 Audit Manager 和 Organizations 之间的信任访问，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

有关 Audit Manager 如何使用此角色的详细信息，请参阅《Amazon Audit Manager 用户指南》中的使用服务相关角色。

- `AWSServiceRoleForAuditManager`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Audit Manager 使用的服务相关角色为以下服务委托人授予访问权限：

- `auditmanager.amazonaws.com`

使用 Audit Manager 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

Audit Manager 需要可信访问权限， Amazon Organizations 然后才能将成员账户指定为组织的委托管理员。

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

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Audit Manager 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Audit Manager 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon Audit Manager提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 Amazon Audit Manager 控制台或工具启用可信访问，则无需完成这些步骤。

使用 Audit Manager 控制台启用信任访问权限

有关启用信任访问权限的说明，请参阅《Amazon Audit Manager 用户指南》中的设置。

> **Note**
>
> 如果您使用 Amazon Audit Manager 控制台配置委派管理员，则 Amazon Audit Manager 会自动为您启用可信访问权限。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来启用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Audit Manager zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- Amazon API: E A nableAWSService ccess

使用 Audit Manager 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Amazon Organizations 管理账户中的管理员才能使用禁用可信访问权限 Amazon Audit Manager。

您只能使用 Organizations 工具禁用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Audit Manager ations 中禁用可信服务。

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

如果成功，此命令不会产生任何输出。

- Amazon API: D A isableAWSService ccess

为 Audit Manager 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 Audit Manager 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 Audit Manager 的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中具有以下权限的用户或角色才能将成员账户配置为组织中 Audit Manager 的委托管理员：
> `audit-manager:RegisterAccount`

有关为 Audit Manager 启用委托管理员账户的说明，请参阅《Amazon Audit Manager 用户指南》中的设置。

如果您使用 Amazon Audit Manager 控制台配置委派管理员，则 Audit Manager 会自动为您启用可信访问权限。

Amazon CLI, Amazon API

如果要使用 Amazon CLI或其中一个配置委派管理员帐户 Amazon SDKs，则可以使用以下命令：

- Amazon CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- Amazon SDK：调用`RegisterAccount`操作并提供`delegatedAdminAccount`作为参数来委派管理员帐户。

Amazon Backup 和 Amazon Organizations

Amazon Backup 是一项允许您管理和监控组织中 Amazon Backup 作业的服务。使用 Amazon Backup，如果您以组织管理帐户的用户身份登录，则可以启用组织范围的备份保护和监控。它使用备

份策略将 Amazon Backup 计划集中应用于组织中所有客户的资源，从而帮助您实现合规性。当你同时使用两者 Amazon Backup 时，可以获得以下好处： Amazon Organizations

保护

您可以在组织中启用备份策略类型，然后创建备份策略以附加到组织的 root 或帐户。OUs备份策略将 Amazon Backup 计划与自动将计划应用到您的账户所需的其他详细信息相结合。直接关联到账户的策略与从组织根目录和任何上级继承的策略合并，OUs以创建适用于该账户的有效策略。该策略包括有权在您账户中的资源 Amazon Backup 上运行的IAM角色的 ID。 Amazon Backup 使用该IAM角色代表您执行有效策略中备份计划中指定的备份。

监控

当您在组织中为 Amazon Backup启用可信访问时，您可以使用 Amazon Backup 控制台查看有关组织中任何账户的备份、还原和复制作业的详细信息。有关更多信息，请参阅《Amazon Backup 开发人员指南》中的监控备份任务。

有关的更多信息 Amazon Backup，请参阅《Amazon Backup 开发人员指南》。

使用以下信息来帮助您集 Amazon Backup 成 Amazon Organizations。

使用 Amazon Backup启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

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

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Backup 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Backup 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon Backup提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
>
> 如果您使用 Amazon Backup 控制台或工具启用可信访问，则无需完成这些步骤。

要使用启用可信访问 Amazon Backup，请参阅《Amazon Backup 开发人员指南》 Amazon Web Services 账户中的启用多重备份。

使用 Amazon Backup禁用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

Amazon Backup 需要可信访问权限 Amazon Organizations 才能监控组织账户中的备份、还原和复印作业。如果您禁用可信访问权限 Amazon Backup，则无法查看当前账户以外的作业。 Amazon Backup 创造的 Amazon Backup 角色仍然存在。如果您稍后重新启用可信访问，则可以 Amazon Backup 继续像以前一样运行，而无需重新配置服务。

您只能使用 Organizations 工具禁用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Backup ations 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。
- Amazon API: D A isableAWSService ccess

为其启用委派管理员账户 Amazon Backup

请参阅《Amazon Backup 开发人员指南》中的委托管理员。

Amazon Billing and Cost Management 和 Amazon Organizations

Amazon Billing and Cost Management 提供了一套功能，可帮助您设置账单、检索和支付发票，以及分析、整理、计划和优化成本。当您将 Billing and Cost Management 与 Billing and Cost Management 配合使用时， Amazon Organizations 您可以允许拆分成本分配数据检索 Amazon Organizations 信息（如果适用），并收集您选择使用的分割成本分配数据服务的遥测数据。

使用以下信息来帮助您集 Amazon Billing and Cost Management 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许账单和成本管理服务在您组织中的组织账户内执行支持的操作。

只有在禁用账单与成本管理服务和 Organizations 之间的可信访问，或者从组织中移除成员账户后，才能删除或修改此角色。

有关更多信息，请参阅《账单与成本管理用户指南》中的账单和成本管理的服务相关角色权限。

- `AWSServiceRoleForSplitCostAllocationData`

账单与成本管理使用的服务主体

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。账单与成本管理使用的服务相关角色为以下服务主体授予访问权限：

账单与成本管理使用 `billing-cost-management.amazonaws.com` 服务主体。

启用与账单与成本管理的可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

通过管理账户启用可信访问后，客户可以利用账单与成本管理下的拆分成本分配数据功能。当客户使用 Amazon Managed Service for Prometheus 为 Amazon Elastic Kubernetes Service 启用拆分成本分配数据功能时，将调用可信访问为组织内的所有成员账户创建服务相关角色。这样可将拆分成本分配数据功能从客户的 Amazon Managed Service for Prometheus 工作区收集遥测数据，并根据这些指标进行成本分配。

您只能使用 Organizations 工具启用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来启用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Billing and Cost Management zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

禁用可信访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Billing and Cost Management ations 中禁用可信服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: D A isableAWSService ccess

Amazon CloudFormation StackSets 和 Amazon Organizations

Amazon CloudFormation StackSets 使您能够通过单个操作跨多个 Amazon Web Services 账户 堆栈创建、更新或删除堆栈。 Amazon Web Services 区域 StackSets Amazon Organizations 通过与集

成，您可以使用在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管理权限的堆栈集。这可将堆栈实例部署到组织中的成员账户。您不必创建必要的 Amazon Identity and Access Management 角色； StackSets 可以代表IAM您在每个成员账户中创建角色。

您还可以选择为将来添加到组织的账户启用自动部署。启用自动部署后，关联堆栈集实例的角色和部署将自动添加到将来添加到该 OU 的所有账户中。

启用 StackSets 和 Organizations 之间的可信访问权限后，管理账户有权为您的组织创建和管理堆栈集。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。管理账户无法将委派的管理员权限限制为特定堆栈集OUs或执行特定堆栈集操作。

有关 StackSets 与 Organizations 集成的更多信息，请参阅《Amazon CloudFormation 用户指南》Amazon CloudFormation StackSets中的 “使用”。

使用以下信息来帮助您集 Amazon CloudFormation StackSets 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Amazon CloudFormation Stacksets 在组织中的账户中执行支持的操作。

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》 Amazon CloudFormation StackSets中的 “使用”。

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向以下服务主体授予访问权限：

- 管理账户：`stacksets.cloudformation.amazonaws.com`

  只有在 StackSets 和 Organizations 之间禁用了可信访问权限后，才能修改或删除此角色。

- 成员账户：`member.org.stacksets.cloudformation.amazonaws.com`

  只有先禁用 StackSets 和 Organizations 之间的可信访问权限，或者先从目标组织或组织单位 (OU) 中移除该帐户，才能修改或删除账户中的此角色。

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。

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

您只能使用启用可信访问 Amazon CloudFormation StackSets。

要使用 Amazon CloudFormation Stacksets 控制台启用可信访问，请参阅《 Amazon CloudFormation 用户指南》 Amazon Organizations中的 “使用启用可信访问”。

使用 Amazon CloudFormation Stacksets 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Organizations 管理账户中的管理员才有权禁用其他 Amazon 服务的可信访问权限。您只能使用 Organizations 控制台禁用信任访问权限。如果您在使用时禁用 Organizations 的可信访问权限 StackSets，则所有先前创建的堆栈实例都将保留。但是，使用服务相关角色的权限部署的堆栈套无法再对 Organizations 管理的账户执行部署。

您可以使用控制台或 Organizations Amazon CloudFormation 控制台禁用可信访问。

> **Important**
>
> 如果您以编程方式禁用可信访问（例如使用 Amazon CLI 或使用API），请注意这将删除权限。最好使用 Amazon CloudFormation 控制台禁用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon CloudFormation StackSets。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon CloudFormation StackSets” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。 Amazon CloudFormation StackSets

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon CloudFormation StackSets ations 中禁用可信服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal stacksets.cloudformation.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: D A isableAWSService ccess

为 Amazon CloudFormation 堆栈集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管理与 Amazon CloudFormation 堆栈集的管理分开。

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 CloudTrail 和 Amazon Organizations

Amazon CloudTrail 是一项 Amazon 服务，可帮助您实现监管、合规以及运营和风险审计 Amazon Web Services 账户。使用 Amazon CloudTrail管理账户中的用户可以创建组织跟踪，记录该组织 Amazon Web Services 账户 中所有人的所有事件。组织跟踪自动应用到组织中的所有成员账户。成员账户可以查看组织跟踪，但无法修改或删除它。默认情况下，成员账户没有权限访问 Amazon S3 存储桶中组织跟踪的日志文件。这有助于您在组织的账户中统一应用和实施事件日志记录策略。

有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的为组织创建跟踪。

使用以下信息来帮助您集 Amazon CloudTrail 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色 CloudTrail 允许在组织中的组织账户中执行支持的操作。

只有在禁用 CloudTrail 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForCloudTrail`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。使用的服务相关角色向以下服务主体 CloudTrail 授予访问权限：

- `cloudtrail.amazonaws.com`

使用 CloudTrail 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

如果您通过从 Amazon CloudTrail 控制台创建跟踪来启用可信访问，则会自动为您配置可信访问（推荐）。您也可以使用 Amazon Organizations 控制台启用可信访问。您必须使用 Amazon Organizations 管理账户登录才能创建组织跟踪。

如果您选择使用 Amazon CLI 或创建组织跟踪 Amazon API，则必须手动配置可信访问权限。有关更多信息，请参阅《Amazon CloudTrail 用户指南》Amazon Organizations中的 CloudTrail 作为可信服务启用。

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon CloudTrail 控制台或工具来启用与 Organizations 的集成。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来启用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon CloudTrail zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

使用 CloudTrail 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

Amazon CloudTrail 需要使用可信访问权限 Amazon Organizations 才能使用组织跟踪和组织事件数据存储。如果您 Amazon Organizations 在使用时使用禁用可信访问权限 Amazon CloudTrail，则成员账户的所有组织跟踪都将被删除，因为 CloudTrail 无法访问该组织。所有管理账户组织跟踪和组织事件数据存储都将转换为账户级别跟踪和事件数据存储。为两者之间的 CloudTrail 集成而创建的`AWSServiceRoleForCloudTrail`角色将 Amazon Organizations 保留在账户中。如果您重新启用可信访问权限，则 CloudTrail 不会对现有跟踪和事件数据存储执行操作。管理账户必须更新所有账户级别的跟踪和事件数据存储，才能将其应用于组织。

要将账户级别跟踪或事件数据存储转换为组织跟踪或组织事件数据存储，请执行以下操作：

- 在 CloudTrail 控制台中，更新跟踪或事件数据存储，然后选择 “为我的组织中的所有账户启用” 选项。
- 从中 Amazon CLI，执行以下操作：
  - 要更新跟踪，请运行 update-trail命令并包含`--is-organization-trail`参数。
  - 要更新事件数据存储，请运行 update-event-data-store命令并包含`--organization-enabled`参数。

只有 Amazon Organizations 管理账户中的管理员才能使用禁用可信访问权限 Amazon CloudTrail。您只能使用 Organizations 工具禁用可信访问，使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作 Amazon SDKs。

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon CloudTrail。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon CloudTrail” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。 Amazon CloudTrail

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon CloudTrail ations 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。

- Amazon API: D A isableAWSService ccess

为其启用委派管理员账户 CloudTrail

在 CloudTrail 与 Organizations 一起使用时，您可以注册组织内的任何账户，使其成为 CloudTrail 委托管理员，代表组织管理组织的跟踪和事件数据存储。委派管理员是组织中的成员帐户，可以在中执行与管理帐户 CloudTrail 相同的管理任务。

> **最小权限**
>
> 只有 Organizations 管理账户中的管理员才能为其注册委托管理员 CloudTrail。

您可以使用 CloudTrail 控制台或使用 Organizations `RegisterDelegatedAdministrator` CLI 或SDK操作注册委派管理员帐户。要使用 CloudTrail 控制台注册委派管理员，请参阅添加 CloudTrail 委派管理员。

禁用委派的管理员 CloudTrail

只有 Organizations 管理账户中的管理员才能移除其委派的管理员 CloudTrail。您可以使用 CloudTrail 控制台或使用 Organizations `DeregisterDelegatedAdministrator` CLI 或SDK操作来移除委派的管理员。有关如何使用 CloudTrail 控制台移除委派管理员的信息，请参阅移除 CloudTrail 委派管理员。

亚马逊 CloudWatch 和 Amazon Organizations

您可以使用 Organizations for Amazon CloudWatch 从 CloudWatch 控制台的中央视图发现和了解 Amazon 资源的遥测配置状态。这简化了审核组织或账户中多种资源类型的遥测采集配置的过程。Amazon

通过与 Organizations 集成，您可以修改亚马逊 CloudWatch 组织支持的配置。您必须启用可信访问权限才能在整个组织中使用遥测配置。

有关更多信息，请参阅 Amazon CloudWatch 用户指南中的审计遥测配置。

使用以下信息来帮助您将Amazon CloudWatch 与之集成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

在贵组织的管理账户中创建以下服务相关角色。启用可信访问权限后，服务相关角色将在成员账户中自动创建。此角色 CloudWatch 允许在组织中的组织账户中执行支持的操作。只有在 CloudWatch 和 Organizations 之间禁用可信访问权限或从组织中移除成员帐户后，才能删除或修改此角色。

- `AWSServiceRoleForObservabilityAdmin`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。使用的服务相关角色向以下服务主体 CloudWatch 授予访问权限：

- `observabilityadmin.amazonaws.com`

使用 CloudWatch 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

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

> **Important**
>
> 我们强烈建议您尽可能使用亚马逊 CloudWatch 控制台或工具来启用与 Organizations 的集成。这样，Amazon 就可以 CloudWatch 执行其所需的任何配置，例如创建服务所需的资源。只有在无法使用 Amazon 提供的工具启用集成时，才能继续执行这些步骤 CloudWatch。有关更多信息，请参阅此说明。

如果您使用 Amazon CloudWatch 控制台或工具启用可信访问，则无需完成这些步骤。

使用 CloudWatch 控制台启用可信访问

请参阅《Amazon CloudWatch 用户指南》中的开启 CloudWatch 遥测审计。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用 API 操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表 CloudWatch中选择 Amazon。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “为 Amazon 启用可信访问 CloudWatch” 对话框中，键入 enab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告诉 Amazon CloudWatch 管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。

Amazon CLI, Amazon API

使用 OrganizationsCLI/SDK 启用信任服务访问权限

使用以下 Amazon CLI 命令或 API 操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令将 Amazon 启用 CloudWatch 为 Organizations 的可信服务。

```
$ aws organizations enable-aws-service-access \
    --service-principal observabilityadmin.amazonaws.com
```

  如果成功，此命令不会产生任何输出。

- Amazon API：启用AWSService访问权限

使用 CloudWatch 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您可以使用 Amazon CloudWatch 或 Amazon Organizations 工具禁用可信访问。

> **Important**
>
> 我们强烈建议您尽可能使用亚马逊 CloudWatch 控制台或工具来禁用与 Organizations 的集成。这样，Amazon 就可以 CloudWatch 执行其所需的任何清理工作，例如删除服务不再需要的资源或访问角色。只有当您无法使用 Amazon 提供的工具禁用集成时，才能继续执行这些步骤 CloudWatch。
> 如果您使用 Amazon CloudWatch 控制台或工具禁用可信访问，则无需完成这些步骤。

使用 CloudWatch 控制台禁用可信访问

请参阅《Amazon CloudWatch 用户指南》中的关闭 CloudWatch 遥测审计

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 禁用信任服务访问权限

使用以下 Amazon CLI 命令或 API 操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令将 Amazon 禁用 Organization CloudWatch s 作为可信服务。

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

  如果成功，此命令不会产生任何输出。
- Amazon API：禁用AWSService访问权限

为其启用委派管理员账户 CloudWatch

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 CloudWatch 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 CloudWatch 的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中的管理员才能将成员账户配置为组织 CloudWatch 中的委托管理员。

您可以使用 CloudWatch 控制台，也可以使用 Organizations `RegisterDelegatedAdministrator` CLI 或 SDK 操作来注册委派管理员帐户。有关如何使用 CloudWatch 控制台注册委托管理员的信息，请参阅 Amazon CloudWatch 用户指南中的开启 CloudWatch 遥测审计。

禁用委派的管理员 CloudWatch

> **最小权限**
>
> 只有 Organizations 管理账户中的管理员才能删除组织 CloudWatch 中的委托管理员。

您可以使用 CloudWatch 控制台，也可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作来移除委派的管理员。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的关闭 CloudWatch 遥测审计。

Amazon Compute Optimizer 和 Amazon Organizations

Amazon Compute Optimizer 是一项分析 Amazon 资源的配置和利用率指标的服务。资源示例包括亚马逊弹性计算云 (AmazonEC2) 实例和 Auto Scaling 组。Compute Optimizer 报告您的资源是否处于最佳状态并生成优化建议，以降低成本并提高工作负载的性能。有关 Compute Optimizer 的更多信息，请参阅 Amazon Compute Optimizer 用户指南。

使用以下信息来帮助您集 Amazon Compute Optimizer 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Compute Optimizer 在您组织中的组织账户内执行支持的操作。

只有在禁用 Compute Optimizer 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForComputeOptimizer`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Compute Optimizer 使用的服务相关角色为以下服务委托人授予访问权限：

- `compute-optimizer.amazonaws.com`

使用 Compute Optimizer 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 Amazon Compute Optimizer 控制台或控制台启用可信访问。 Amazon Organizations

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Compute Optimizer 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Compute Optimizer 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon Compute Optimizer提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 Amazon Compute Optimizer 控制台或工具启用可信访问，则无需完成这些步骤。

使用 Compute Optimizer 控制台启用信任访问权限

您必须使用组织的管理账户登录 Compute Optimizer 控制台。代表您的组织选择启用，方法是按照《Amazon Compute Optimizer 用户指南》中的选择启用账户中的说明操作。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Compute Optimizer。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon Compute Optimizer” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon Compute Optimizer

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Compute Optimizer zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- Amazon API: E A nableAWSService ccess

使用 Compute Optimizer 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Amazon Organizations 管理账户中的管理员才能使用禁用可信访问权限 Amazon Compute Optimizer。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Compute Optimizer ations 中禁用可信服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: D A isableAWSService ccess

为 Compute Optimizer 启用委托管理员账户

当您将某个成员账户指定为组织的委托管理员时，来自指定账户的用户和角色将可以管理组织内其他成员账户的 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 管理账户中的用户或角色才能将某个成员账户配置为组织的 Compute Optimizer 委托管理员。

有关为 Compute Optimizer 启用委托管理员账户的说明，请参阅Amazon Compute Optimizer 用户指南中的 https://docs.amazonaws.cn/compute-optimizer/latest/ug/delegate-administrator-account.html。

Amazon CLI, Amazon API

如果要使用 Amazon CLI或其中一个配置委派管理员帐户 Amazon SDKs，则可以使用以下命令：

- Amazon CLI:

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

- Amazon SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，将账户服务委托人标识`account.amazonaws.com`为参数。

为 Compute Optimizer 禁用委托管理员账户

只有组织管理账户中的管理员才能为 Compute Optimizer 配置委托管理员。

要使用 Compute Optimizer 控制台禁用委托管理员 Compute Optimizer 账户，请参阅 Amazon Compute Optimizer 用户指南中的 https://docs.amazonaws.cn/compute-optimizer/latest/ug/delegate-administrator-account.html。

要使用移除委派的管理员 Amazon Amazon CLI，请参阅《Amazon Amazon CLI 命令参考》deregister-delegated-administrator中的。

Amazon Config 和 Amazon Organizations

中的多账户、多区域数据聚合 Amazon Config 使您可以将来自多个账户 Amazon Config 的数据聚合 Amazon Web Services 区域 到单个账户中。多账户、多区域数据聚合用于中心 IT 管理员监控企业中多个 Amazon Web Services 账户 的合规性。聚合器是一种资源类型 Amazon Config ，用于从多个源账户和地区收集 Amazon Config 数据。在要查看聚合 Amazon Config 数据的区域中创建聚合器。在创建聚合器时，您可以选择添加个人帐户IDs或组织。有关的更多信息 Amazon Config，请参阅《Amazon Config 开发人员指南》。

您还可以使用Amazon Config APIs来管理组织 Amazon Web Services 账户 中所有部门的 Amazon Config 规则。有关更多信息，请参阅《Amazon Config 开发者指南》中的在组织中的所有账户中启用 Amazon Config 规则。

使用以下信息来帮助您集 Amazon Config 成 Amazon Organizations。

服务相关角色

以下服务相关角色 Amazon Config 允许您在组织中的账户中执行支持的操作。

- `AWSServiceRoleForConfig`

要详细了解如何创建此角色，请参阅Amazon Config 开发人员指南 Amazon Config中分配给IAM角色的权限

要详细了解如何 Amazon Config 使用服务相关角色，请参阅开发人员指南 Amazon Config中的Amazon Config 使用服务相关角色

只有在禁用 Amazon Config 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

使用 Amazon Config启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

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

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Config 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Config 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用Amazon Config提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。如果您使用 Amazon Config 控制台或工具启用可信访问，则无需完成这些步骤。

使用 Amazon Config 控制台启用可信访问

要启用可信访问 Amazon Organizations 使用 Amazon Config，请创建多账户聚合器并添加组织。有关如何配置多账户聚合器的信息，请参阅《Amazon Config 开发人员指南》中的 Creating Aggregators。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Config。
4. 选择 Enable trusted access (启用可信访问)。

5. 在 “启用可信访问 Amazon Config” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon Config

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Config zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

使用 Amazon Config禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Config ations 中禁用可信服务。

  ```
  $ aws organizations disable-aws-service-access \
  ```

```
    --service-principal config.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- Amazon API: D isableAWSService 访问权限

Amazon 成本优化中心 和 Amazon Organizations

Amazon 成本优化中心 是一项 B Amazon illing and Cost Management 功能，可帮助您整合不同 Amazon 账户和 Amazon 地区的成本优化建议并确定其优先顺序，从而最大限 Amazon 度地利用支出。当您使用成本优化中心时， Amazon Organizations 您可以轻松识别、筛选和汇总您的 Organizations 成员账户和 Amazon 地区 Amazon 的成本优化建议。

有关更多信息，请参阅《Amazon Cost Management 用户指南》中的 Cost Optimization Hub。

使用以下信息来帮助您集 Amazon 成本优化中心 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许成本优化中心在您组织中的组织账户内执行支持的操作。

只有在成本优化中心与 Organizations 之间禁用可信访问，或者您从组织中移除该成员账户后，才能删除或修改此角色。

有关更多信息，请参阅《Amazon Cost Management 用户指南》中的 Service-linked role permissions for Cost Optimization Hub。

- `AWSServiceRoleForCostOptimizationHub`

成本优化中心使用的服务主体

成本优化中心使用 `cost-optimization-hub.bcm.amazonaws.com` 服务主体。

启用与成本优化中心的可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

当您选择加入组织的管理账户并包括组织内的所有成员账户时，您的组织账户中将自动启用成本优化中心的可信访问权限。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon 成本优化中心。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon 成本优化中心” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon 成本优化中心

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon 成本优化中心 zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

禁用可信访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用可信访问。

> **Important**
>
> 如果您在选择加入后禁用成本优化中心可信访问，则成本优化中心会拒绝访问组织成员账户的建议。此外，组织内的成员账户不会选择加入成本优化中心。要了解更多信息，请参阅《Amazon Cost Management 用户指南》中的 Cost Optimization Hub and Organizations trusted access。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon 成本优化中心 ations 中禁用可信服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- Amazon API: D A isableAWSService ccess

为成本优化中心启用委派管理员账户

当您将某个成员账户指定为组织的委派管理员时，该指定账户将可以检索组织内所有账户的成本优化中心建议并管理成本优化中心首选项，从而让您可以更灵活地集中识别资源优化机会。

> **最小权限**
>
> 只有 Organizations 管理账户中具有以下权限的用户或角色才能将成员账户配置为组织中的成本优化中心委派管理员：

有关如何为成本优化中心启用委派管理员账户的说明，请参阅《Amazon Cost Management 用户指南》中的 Delegate an administrator account。

为成本优化中心禁用委派管理员

只有 Organizations 管理账户中的管理员才能移除成本优化中心的委派管理员。

要使用成本优化中心控制台禁用成本优化中心的委派管理员账户，请参阅《Amazon Cost Management 用户指南》中的 Delegate an administrator account。

要使用移除委派管理员 Amazon CLI，请参阅 “Amazon Config CLI参考” `deregister-delegated-administrator`中的。

Amazon Control Tower 和 Amazon Organizations

Amazon Control Tower 遵循规范性最佳实践，提供了一种设置和管理 Amazon 多账户环境的简单方法。 Amazon Control Tower 编排扩展了的功能。 Amazon Organizations Amazon Control Tower 应用预防和侦查控制（护栏），以帮助防止您的组织和客户偏离最佳实践（偏离）。

Amazon Control Tower 编排扩展了的功能。 Amazon Organizations

有关更多信息，请参阅《Amazon Control Tower 用户指南》。

使用以下信息来帮助您集 Amazon Control Tower 成 Amazon Organizations。

集成所需的角色

`AWSControlTowerExecution` 角色必须存在于所有注册的账户中。它 Amazon Control Tower 允许管理您的个人账户，并将有关这些账户的信息报告给您的审计和日志存档账户。

要了解有关所用角色的更多信息 Amazon Control Tower，请参阅Amazon Control Tower 如何使用角色来创建和管理账户，以及使用基于身份的策略（IAM策略） Amazon Control Tower

使用的服务主体 Amazon Control Tower

Amazon Control Tower 使用`controltower.amazonaws.com`服务主体。

使用 Amazon Control Tower启用信任访问权限

Amazon Control Tower 使用可信访问来检测偏差以进行预防性控制，并跟踪导致偏差的账户和 OU 更改。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Organizations 工具启用可信访问。

要从 Organizations 控制台启用可信访问，请选择 Amazon Control Tower 旁边的 **Enable access**。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来启用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Control Tower zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

使用 Amazon Control Tower禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用可信访问。

> **Important**
>
> 禁用可 Amazon Control Tower信访问权限会导致您的着 Amazon Control Tower 陆区域出现偏差。修复偏差的唯一方法是使用 Amazon Control Tower的登录区修复。在 Organizations 中重新启用可信访问权限并不能解决偏差。在《Amazon Control Tower 用户指南》中了解有关偏差的更多信息。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Control Tower ations 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。

- Amazon API: D A isableAWSService ccess

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 可以确保 Detective 行为图可以查看所有组织帐户的活动。

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。

使用以下信息来帮助您将 Amazon Detective 与集成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Detective 在您组织中的组织账户内执行受支持的操作。

只有在禁用 Detective 与 Organizations 之间的信任访问权限后，或是从组织中删除成员账户后，您才能删除或修改此角色。

- `AWSServiceRoleForDetective`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Detective 使用的服务相关角色为以下服务主体授予访问权限：

- `detective.amazonaws.com`

使用 Detective 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

> **Note**
>
> 当您为 Amazon Detective 指定委托管理员时，Detective 会自动为您的组织启用 Detective 信任访问权限。
> Detective 需要获得可信访问权限， Amazon Organizations 然后才能将成员账户指定为组织中该服务的委托管理员。

您只能使用 Organizations 工具启用可信访问。

您可以使用 Amazon Organizations 控制台启用可信访问。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Detective。
4. 选择 Enable trusted access (启用可信访问)。
5. 在为 Amazon Detective 启用可信访问对话框中，键入启用进行确认，然后选择启用可信访问。
6. 如果您仅是的管理员 Amazon Organizations，请告诉 Amazon Detective 的管理员，他们现在可以 Amazon Organizations 从服务控制台启用该服务。

使用 Detective 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Amazon Organizations 管理账户中的管理员才能禁用 Amazon Detective 的可信访问权限。

您只能使用 Organizations 工具禁用可信访问。

您可以使用 Amazon Organizations 控制台禁用可信访问。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Detective。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用 Amazon Detective 的可信访问” 对话框中，键入 “禁用” 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告诉 Amazon Detective 的管理员，他们现在 Amazon Organizations 可以使用服务控制台或工具禁用该服务；。

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。

您可以从 Detective 控制台或使用 Organi API zations CLI 或SDK操作指定委托管理员帐户。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色能够将某个成员账户配置为组织的 Detective 委托管理员。

要使用 Detective 控制台或配置委托管理员API，请参阅《Amazon Detective 管理指南》中的为组织指定侦探管理员账户。

Amazon CLI, Amazon API

如果要使用 Amazon CLI或其中一个配置委派管理员帐户 Amazon SDKs，则可以使用以下命令：

- 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，将账户服务委托人标识`account.amazonaws.com`为参数。

为 Detective 禁用委托管理员

您可以使用 Detective 控制台或API，或者使用 Organizations `DeregisterDelegatedAdministrator` CLI 或SDK操作移除委托的管理员。有关如何使用 Detective 控制台或 API Org anizations 移除委派管理员的信息API，请参阅《Amazon Detective 管理指南》中的为组织指定侦探管理员账户。

Amazon DevOps Guru 和 Amazon Organizations

Amazon DevOps Guru 分析运营数据和应用程序指标及事件，以识别与正常操作模式不同的行为。当 DevOps Guru 检测到操作问题或风险时，用户会收到通知。

使用 DevOps Guru 可实现多账户支持 Amazon Organizations，因此您可以指定一个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内的账户。

使用以下信息来帮助您将 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 在组织中的账户中执行支持的操作。

只有在禁用 DevOps Guru 和 Organizations 之间的可信访问权限或从组织中删除成员帐户后，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。 DevOpsGuru 使用的服务相关角色向以下服务主体授予访问权限：

- `devops-guru.amazonaws.com`

有关更多信息，请参阅 A ma DevOps zon Guru 用户指南中的为 DevOps Guru 使用服务相关角色。

通过 DevOps Guru 启用可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

> **Note**
>
> 当您为 Amazon DevOps Guru 指定委托管理员时， DevOpsGuru 会自动为您的组织启用 DevOps Guru 的可信访问权限。
> DevOpsGuru 需要获得可信访问权限， Amazon Organizations 然后才能指定成员账户作为贵组织此服务的委托管理员。

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon DevOps Guru 控制台或工具来启用与 Organizations 的集成。这允许 Amazon DevOps Guru 执行其所需的任何配置，例如创建服务所需的资源。只有当您无法使用 Amazon DevOps Guru 提供的工具启用集成时，才能继续执行这些步骤。有关更多信息，请参阅此说明。

您可以使用控制台或 DevOps Guru Amazon Organizations 控制台启用可信访问。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在 “服务” 页面上，找到 Amazon DevOps Guru 所在的行，选择该服务的名称，然后选择 “启用可信访问”。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您仅是的管理员 Amazon Organizations，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。 Amazon Organizations

DevOps Guru console

使用 DevOps Guru 控制台启用可信服务访问

1. 以管理员身份登录管理账户并打开 DevOps Guru 控制台：Amazon DevOps G uru 控制台
2. 选择 Enable trusted access (启用可信访问)。

使用 DevOps Guru 禁用可信访问

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Amazon Organizations 管理账户中的管理员才能禁用 Amazon DevOps Guru 的可信访问权限。

您只能使用 Organizations 工具禁用可信访问。

您可以使用 Amazon Organizations 控制台禁用可信访问。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon DevOps Guru。

4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用 Amazon DevOps Guru 的可信访问” 对话框中，键入 “禁用” 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告诉 Amazon DevOps Guru 的管理员，他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务；。

为 DevOps Guru 启用委托管理员账户

DevOpsGuru 的委托管理员账户可以查看来自组织加入 DevOps Guru 的所有成员账户的见解数据。有关委派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 配置委派管理员。

您可以从 DevOps Guru 控制台指定委托管理员帐户，也可以使用 Organizations `RegisterDelegatedAdministrator` CLI 或SDK操作来指定委托管理员帐户。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色才能将成员账户配置为组织中 DevOps Guru 的委托管理员

DevOps Guru console

在 DevOps Guru 控制台中配置委派管理员

1. 以管理员身份登录管理账户并打开 DevOps Guru 控制台：Amazon DevOps G uru 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或其中一个配置委派管理员帐户 Amazon SDKs，则可以使用以下命令：

- 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，将账户服务委托人标识`account.amazonaws.com`为参数。

禁用 DevOps Guru 的委托管理员

您可以使用 DevOps Guru 控制台或使用 Organizations `DeregisterDelegatedAdministrator` CLI 或SDK操作来移除委派的管理员。有关如何使用 DevOps Guru 控制台移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 Directory Service 和 Amazon Organizations

Amazon Directory Service 适用于微软 Active Directory Amazon Managed Microsoft AD，或者，允许你将微软 Active Directory (AD) 作为托管服务运行。 Amazon Directory Service 可以轻松地在 Amazon 云端设置和运行目录，或者将您的 Amazon 资源与现有的本地 Microsoft Active Directory 连接起来。Amazon Managed Microsoft AD 还与紧密集成 Amazon Organizations ，允许在一个区域VPC中的多个 Amazon Web Services 账户 和任意区域之间无缝共享目录。有关更多信息，请参阅 Amazon Directory Service 管理指南。

要在 Amazon Directory Service 整个组织中共享，组织必须启用所有功能，并且目录必须位于组织管理帐户中。

使用以下信息来帮助您集 Amazon Directory Service 成 Amazon Organizations。

使用 Amazon Directory Service启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 Amazon Directory Service 控制台或控制台启用可信访问。 Amazon Organizations

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Directory Service 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Directory Service 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon Directory Service提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 Amazon Directory Service 控制台或工具启用可信访问，则无需完成这些步骤。

使用 Amazon Directory Service 控制台启用可信访问

要共享自动启用信任访问权限的目录，请参阅《Amazon Directory Service 管理指南》中的共享您的目录。有关 step-by-step说明，请参阅教程：共享您的 Amazon 托管 Microsoft AD 目录。

您可以使用 Amazon Organizations 控制台启用可信访问。

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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Directory Service。
4. 选择 Enable trusted access (启用可信访问)。
5. 在为 Amazon Directory Service启用可信访问对话框中，键入启用进行确认，然后选择启用可信访问。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon Directory Service

使用 Amazon Directory Service禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

如果您 Amazon Organizations 在使用时使用禁用可信访问 Amazon Directory Service，则以前共享的所有目录将继续正常运行。但是，在重新启用信任访问权限前，您将无法再在组织内共享新目录。

您只能使用 Organizations 工具禁用可信访问。

您可以使用 Amazon Organizations 控制台禁用可信访问。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。

3. 在服务列表中选择 Amazon Directory Service。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon Directory Service” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务;。 Amazon Directory Service

Amazon Elastic Compute Cloud 和 Amazon Organizations

Amazon 弹性计算云在 Amazon 云中提供按需、可扩展的计算容量。当你将 Amazon EC2 with Organizations 使用时，你允许组织管理员在使用亚马逊的声明性政策功能后创建一份报告，说明其组织中账户EC2的现有配置情况。

使用以下信息来帮助您将 Amazon 弹性计算云与集成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Amazon EC2 在贵组织中的账户中执行支持的操作。

只有在您禁用 Amazon EC2 和 Organizations 之间的可信访问权限或从组织中删除成员账户的情况下，您才能删除或修改此角色。

- `AWSServiceRoleForDeclarativePoliciesEC2Report`

Amazon 使用的服务主体 EC2

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 使用的服务相关角色向以下服务委托人EC2授予访问权限：

- `report.declarative-policies-ec2.amazonaws.com`

通过 Amazon 启用可信访问 EC2

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。

要使 Organizations 管理员能够为其组织中的账户创建现有配置的报告，您必须启用可信访问权限。

您只能使用 Organizations 工具启用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon 弹性计算云。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “为 Amazon Elastic Compute Cloud 启用可信访问” 对话框中，键入 enable 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告诉 Amazon Elastic Compute Cloud 的管理员，他们现在可以 Amazon Organizations 从服务控制台启用该服务。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令将亚马逊弹性计算云启用为 Organizations 的可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal report.declarative-policies-ec2.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

禁用可信访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令禁用 Amazon 弹性计算云作为 Organizations 的可信服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal report.declarative-policies-ec2.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: D A isableAWSService ccess

Amazon Firewall Manager 和 Amazon Organizations

Amazon Firewall Manager 是一项安全管理服务，用于集中配置和管理组织中的 Amazon Web Services 账户 和应用程序中的防火墙规则和其他保护。使用 Firewall Manager，您可以发布 Amazon WAF 规则、创建 Amazon Shield Advanced 保护措施、配置和审核亚马逊虚拟私有云 (AmazonVPC) 安全组以及部署 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。有关的更多信息 Amazon Firewall Manager，请参阅《Amazon Firewall Manager 开发人员指南》。

使用以下信息来帮助您集 Amazon Firewall Manager 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Firewall Manager 在您组织中的组织账户内执行支持的操作。

只有在禁用 Firewall Manager 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForFMS`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Firewall Manager 使用的服务相关角色为以下服务委托人授予访问权限：

- `fms.amazonaws.com`

使用 Firewall Manager 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

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

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Firewall Manager 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Firewall Manager 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 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。
> 如果您使用 Amazon Firewall Manager 控制台或工具启用可信访问，则无需完成这些步骤。

您必须使用您的 Amazon Organizations 管理账户登录，并将组织内的一个账户配置为 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、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Firewall Manager。

4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon Firewall Manager” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon Firewall Manager

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Firewall Manager zations 中启用可信服务。

  ```
  $ 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: E A nableAWSService ccess

使用 Firewall Manager 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您可以使用 Amazon Firewall Manager 或 Amazon Organizations 工具禁用可信访问。

> **Important**
>
> 我们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。这允许 Amazon Firewall Manager 执行它需要的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 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 控制台或工具禁用可信访问，则无需完成这些步骤。

使用 Firewall Manager 控制台禁用信任访问权限

您可以按照《Amazon Firewall Manager 开发者指南》中将其他账户指定为 Amazon Firewall Manager 管理员账户中的说明更改或撤消 Amazon Firewall Manager 管理员帐户。

如果您撤消管理员帐户，则必须登录 Amazon Organizations 管理账户并为设置新的管理员帐户。Amazon Firewall Manager

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Firewall Manager。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon Firewall Manager” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。 Amazon Firewall Manager

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Firewall Manager ations 中禁用可信服务。

  ```
  $ 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: D A isableAWSService ccess

为 Firewall Manager 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 Firewall Manager 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 Firewall Manager 的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色才能将成员账户配置为组织中 Firewall Manager 的委托管理员。

有关如何将成员帐户指定为组织的 Firewall Manager 管理员的说明，请参阅《Amazon Firewall Manager 开发者指南》中的设置 Amazon Firewall Manager 管理员帐户。

亚马逊 GuardDuty 和 Amazon Organizations

Amazon GuardDuty 是一项持续的安全监控服务，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 环境中意外的、可能未经授权的恶意活动。这可能包括诸如权限升级、使用暴露的证书、与恶意 IP 地址或域的通信，或者您的 Amazon Elastic Compute Cloud 实例和容器工作负载上存在恶意软件等问题。URLs

您可以使用 Organi GuardDuty zations 管理组织中的 GuardDuty 所有账户，从而帮助简化管理。

有关更多信息，请参阅 Amazon GuardDuty 用户指南 Amazon Organizations中的使用管理 GuardDuty 账户

使用以下信息来帮助您将Amazon GuardDuty 与之集成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

当您启用信任访问权限后，您组织的管理账户中会自动创建以下服务相关角色。这些角色 GuardDuty 允许在组织中的组织账户中执行支持的操作。只有在和 Organizations GuardDuty 之间禁用可信访问权限或从组织中删除成员帐户后，才能删除角色。

- `AWSServiceRoleForAmazonGuardDuty`服务相关角色是在已与 Organizations 集 GuardDuty 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 Organizations GuardDuty 账户

- AmazonGuardDutyMalwareProtectionServiceRolePolicy服务相关角色是在启用 GuardDuty 恶意软件防护的帐户中自动创建的。有关更多信息，请参阅 Amazon GuardDuty 用户指南中的 GuardDuty 恶意软件防护服务相关角色权限

服务相关角色使用的服务委托人

- guardduty.amazonaws.com，由 AWSServiceRoleForAmazonGuardDuty 服务相关角色使用。
- malware-protection.guardduty.amazonaws.com，由 AmazonGuardDutyMalwareProtectionServiceRolePolicy 服务相关角色使用。

使用 GuardDuty 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Amazon 启用可信访问 GuardDuty。

Amazon Organizations 在您将成员账户指定为组织 GuardDuty 管理员之前，Amazon GuardDuty 需要获得可信访问权限。如果您使用 GuardDuty 控制台配置委派管理员，则 GuardDuty 会自动为您启用可信访问权限。

但是，如果要使用 Amazon CLI 或其中一个配置委派管理员帐户 Amazon SDKs，则必须显式调用 E A nableAWSService cces s 操作并提供服务主体作为参数。然后，您可以EnableOrganizationAdminAccount致电委派 GuardDuty 管理员帐户。

使用 GuardDuty 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令将 Amazon 禁用 Organization GuardDuty s 作为可信服务。

  ```
  $ 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: D A isableAWSService ccess

为其启用委派管理员账户 GuardDuty

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 GuardDuty 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 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

请参见指定委派管理员并添加成员账户（控制台）和指定委派管理员并添加成员账户（API）

Amazon Health 和 Amazon Organizations

Amazon Health 提供对您的资源绩效以及 Amazon Web Services 服务 和账户可用性的持续可见性。Amazon Health 当您的 Amazon 资源和服务受到问题影响或将受到即将发生的变更影响时，会发送事件。启用组织视图后，组织管理账户中的用户可以汇总组织中所有账户 Amazon Health 的事件。组织视图仅显示启用该功能后交付 Amazon Health 的事件，并将其保留 90 天。

您可以使用 Amazon Health 控制台、 Amazon Command Line Interface (Amazon CLI) 或，启用组织视图 Amazon Health API。

有关更多信息，请参阅《Amazon Health 用户指南》中的聚合 Amazon Health 事件。

使用以下信息来帮助您集 Amazon Health 成 Amazon Organizations。

用于集成的服务相关角色

AWSServiceRoleForHealth_Organizations服务相关角色 Amazon Health 允许在组织中的账户中执行支持的操作。

当您通过调用EnableHealthServiceAccessForOrganizationAPI操作启用可信访问权限时，将在您组织的管理账户中自动创建此角色。否则，请使用 Amazon Health 控制台或创建角色CLI，如IAM用户指南中的创建服务相关角色中所述。API

只有在 Amazon Health 和 Organizations 之间禁用可信访问权限或从组织中移除成员帐户后，才能删除或修改此角色。

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。使用的服务相关角色向以下服务主体 Amazon Health 授予访问权限：

- health.amazonaws.com

使用 Amazon Health启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

当您启用组织视图功能时 Amazon Health，还会自动为您启用可信访问权限。

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

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Health 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Health 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon Health提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。如果您使用 Amazon Health 控制台或工具启用可信访问，则无需完成这些步骤。

使用 Amazon Health 控制台启用可信访问

您可以使用 Amazon Health 和以下选项之一来启用可信访问：

- 使用控制 Amazon Health 台。有关更多信息，请参阅《Amazon Health 用户指南》中的组织视图（控制台）。
- 使用 Amazon CLI。有关更多信息，请参阅《Amazon Health 用户指南》中的 “组织视图” (CLI)。
- 调用该EnableHealthServiceAccessForOrganizationAPI操作。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来启用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Health zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

使用 Amazon Health禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

禁用组织视图功能后，将 Amazon Health 停止聚合组织中所有其他账户的事件。这也会自动禁用您的信任访问权限。

您可以使用 Amazon Health 或 Amazon Organizations 工具禁用可信访问。

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Health 控制台或工具来禁用与 Organizations 的集成。这允许 Amazon Health 执行它需要的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 Amazon Health提供的工具禁用集成时，才会使用这些步骤进行处理。

如果您使用 Amazon Health 控制台或工具禁用可信访问，则无需完成这些步骤。

使用 Amazon Health 控制台禁用可信访问

您可以使用以下选项之一禁用信任访问权限：

- 使用控制 Amazon Health 台。有关更多信息，请参阅《Amazon Health 用户指南》中的禁用组织视图（控制台）。
- 使用 Amazon CLI。有关更多信息，请参阅《Amazon Health 用户指南》中的禁用组织视图 (CLI)。
- 调用该DisableHealthServiceAccessForOrganizationAPI操作。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Health ations 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。
- Amazon API: D A isableAWSService ccess

为其启用委派管理员账户 Amazon Health

将成员账户指定为组织的委托管理员后，该账户中的用户和角色将能够对 Amazon Health 执行本来只能由组织管理账户中的用户或角色执行的管理操作。这有利于将组织的管理与 Amazon Health的管理分开。

指定一个成员账户作为 Amazon Health 的委托管理员

请参阅为您的组织视图注册委派管理员

移除 Amazon Health 的委派管理员

请参阅从您的组织视图中移除委派管理员

Amazon Identity and Access Management 和 Amazon Organizations

Amazon Identity and Access Management 是一项用于安全控制服务访问的 Web Amazon 服务。

您可以使用 IAM 中服务上次访问的数据，以帮助您更好地了解组织中的 Amazon 活动。您可以使用这些数据来创建和更新服务控制策略 (SCPs)，这些策略将访问权限仅限于您的组织账户使用的 Amazon 服务。

有关示例，请参阅《IAM 用户指南》中的使用数据来细化组织部门的权限。

IAM 允许您集中管理根用户证书，并对成员账户执行特权任务。在您启用根访问权限管理（在中为 IAM 启用可信访问权限）后 Amazon Organizations，您可以集中保护成员账户的根用户证书。成员账户不能登录到他们的根用户或为其根用户执行密码恢复。IAM 的管理账户或委托管理员账户也可以使用短期根访问权限对成员账户执行一些特权任务。短期特权会话为您提供临时凭证，您可以限定这些凭证的范围，以对组织中的成员账户执行特权操作。

有关更多信息，请参阅 IAM 用户指南中的集中管理成员账户的根访问权限。

使用以下信息来帮助您集 Amazon Identity and Access Management 成 Amazon Organizations。

通过 IAM 启用可信访问

启用根访问管理后，将在中为 IAM 启用可信访问权限 Amazon Organizations。

使用 IAM 禁用可信访问

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Amazon Organizations 管理账户中的管理员才能使用禁用可信访问权限 Amazon Identity and Access Management。

您只能使用 Organizations 工具禁用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Identity and Access Management。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon Identity and Access Management” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。 Amazon Identity and Access Management

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 操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Identity and Access Management ations 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。
- Amazon API：禁用AWSService访问权限

为 IAM 启用委托管理员账户

当您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成员账户执行特权任务，否则这些任务只能由组织管理账户中的用户或角色执行。有关更多信息，请参阅 IAM 用户指南中的对 Organizations 成员账户执行特权任务。

只有组织管理账户中的管理员才能为 IAM 配置委托管理员。

您可以从 IAM 控制台或 API 中指定委托管理员账户，也可以使用 Organizations CLI 或 SDK 操作来指定委托管理员账户。

禁用 IAM 的委托管理员

只有 Organizations 管理账户或 IAM 委托管理员账户中的管理员才能从组织中移除委派管理员账户。您可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作禁用委托管理。

亚马逊 Inspector 和 Amazon Organizations

Amazon Inspector 是一项自动漏洞管理服务，可持续扫描亚马逊EC2和容器工作负载，以查找软件漏洞和意外网络泄露。

使用 Amazon Inspector，您只需为亚马逊 Inspector 委派一个管理员账户，即可管理 Amazon Organizations 通过关联的多个账户。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。

使用以下信息来帮助您将 Amazon Inspector 与集成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Amazon Inspector 在您组织中的组织账户内执行受支持的操作。

只有在禁用 Amazon Inspector 与 Organizations 之间的信任访问权限后，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForAmazonInspector2`

有关更多信息，请参阅《Amazon Inspector 用户指南》中的将服务相关角色用于 Amazon Inspector。

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Amazon Inspector 使用的服务相关角色为以下服务委托人授予访问权限：

- `inspector2.amazonaws.com`

使用 Amazon Inspector 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

Amazon Inspector 需要可信访问权限， Amazon Organizations 然后您才能指定成员账户作为贵组织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，如果要使用 Amazon CLI或其中一个配置委派管理员帐户 Amazon SDKs，则必须显式调用该`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 命令或在其中一个中调用 Organizations API 操作来启用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令将 Amazon Inspector 启用为 Organizations 的可信服务。

  ```
  $ 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: E A nableAWSService ccess

> **Note**
>
> 如果您使用的是 EnableAWSServiceAccessAPI，则还需要致电委EnableDelegatedAdminAccount托 Inspector 管理员帐户。

使用 Amazon Inspector 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Amazon Organizations 管理账户中的管理员才能禁用 Amazon Inspector 的可信访问权限。

您只能使用 Organizations 工具禁用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令将 Amazon Inspector 禁用 Organizations 作为可信服务。

  ```
  $ 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: D A isableAWSService ccess

为 Amazon Inspector 启用委托管理员账户

借助 Amazon Inspector，您可以使用具有 Amazon Organizations 服务的委托管理员来管理组织中的多个账户。

Amazon Organizations 管理账户将组织内的一个账户指定为 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。

您可以从 Amazon Inspector 控制台或API使用 Organizations CLI 或SDK操作指定委托管理员账户。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色能够将某个成员账户配置为组织中 Amazon Inspector 的委托管理员。

要使用 Amazon Inspector 控制台配置委托管理员，请参阅《Amazon Inspector 用户指南》中的步骤 1：启用 Amazon Inspector - 多账户环境。

> **Note**
>
> 您必须在使用 Amazon Inspector 的每个区域调用 `inspector2:enableDelegatedAdminAccount`。

Amazon CLI, Amazon API

如果要使用 Amazon CLI或其中一个配置委派管理员帐户 Amazon SDKs，则可以使用以下命令：

- 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，将账户服务委托人标识`account.amazonaws.com`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移除委派的管理员账户。

您可以使用 Amazon Inspector 控制台或API，或者使用 Organizations `DeregisterDelegatedAdministrator` CLI 或SDK操作移除委托的管理员。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引入云端的流程。在构建云基础架构时 Amazon，您可以通过使用 bring-your-own-license (BYOL) 机会来节省成本，也就是说，重新利用现有许可证库存以用于云资源。通过基于规则的许可证消耗控制，管理员可以对新的和现有的云部署设置硬限制或软限制，在发生不合规的服务器之前停止使用它。

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

通过将 License Manager 与关联起来 Amazon Organizations，您可以：

- 在整个组织中启用计算资源的跨账户发现。
- 查看和管理您拥有并在 Amazon上运行的商用 Linux 订阅。有关更多信息，请参阅 Amazon License Manager中的 Linux 订阅。

使用以下信息来帮助您集 Amazon License Manager 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

当您启用信任访问权限后，您组织的管理账户中会自动创建以下服务相关角色。这些角色允许 License Manager 在您组织中的组织账户内执行支持的操作。

只有在禁用 License Manager 和 Organizations 之间的信任访问权限，或者您从组织中删除成员账户时，您才能删除或修改这些角色。

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

有关更多信息，请参阅 License Manager – 管理账户角色、License Manager – 成员账户角色和 License Manager – Linux 订阅角色。

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。License Manager 使用的服务相关角色为以下服务委托人授予访问权限：

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

使用 License Manager 启用信任访问权限

您只能使用启用可信访问 Amazon License Manager。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

使用 License Manager 启用信任访问权限

您必须使用您的 Amazon Organizations 管理帐户登录许可证管理器控制台，并将其与您的许可证管理器帐户关联。有关更多信息，请参阅中的设置 Amazon License Manager。

使用 License Manager 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  您可以运行以下命令在 Organization Amazon License Manager s 中禁用可信服务。

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal license-manager.amazonaws.com
```

如果成功，此命令不会产生任何输出。

要禁用 Linux 订阅的信任访问权限，请执行以下操作：

```
$  aws organizations disable-aws-service-access \
    --service-principal license-manager-linux-subscriptions.amazonaws.com
```

- Amazon API: D A isableAWSService ccess

为 License Manager 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 License Manager 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 License Manager 的管理分开。

要将成员账户委托为 License Manager 的管理员，请按照《License Manager 用户指南》中注册委托管理员内的步骤操作。

Amazon Managed Services (AMS) 自助报告 (SSR) 和 Amazon Organizations

Amazon Managed Services (AMS) 自助报告 (SSR) 从各种本地 Amazon 服务收集数据，并提供对主要 AMS 产品报告的访问权限。SSR 提供的信息可用于支持运营、配置管理、资产管理、安全管理和合规性。

与集成后 Amazon Organizations，您可以启用聚合自助服务报告 (SSR)。这是一项 AMS 功能，它允许 Advanced 和 Accelerate 客户查看在组织层面、跨账户汇总的现有自助服务报告。这使您可以了解关键运营指标，例如补丁合规性、备份覆盖范围以及其中的所有 AMS 管理的账户的事件。 Amazon Organizations

使用以下信息来帮助您集成 Amazon Managed Services (AMS) 自助报告 (SSR)。 Amazon Organizations

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 AMS 在组织中的账户中执行支持的操作。

只有在禁用 AMS 和 Organizations 之间的可信访问权限或从组织中删除成员账户时，才能删除或修改此角色。

- `AWSServiceRoleForManagedServices_SelfServiceReporting`

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。AMS 使用的服务相关角色向以下服务主体授予访问权限：

- `selfservicereporting.managedservices.amazonaws.com`

通过 AMS 启用可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来启用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 启用信任服务访问权限

使用以下 Amazon CLI 命令或 API 操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令将 Amazon Managed Services (AMS) 自助报告 (SSR) 作为可信服务启用 Organizations。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal selfservicereporting.managedservices.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API：启用AWSService访问权限

使用 AMS 禁用可信访问

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Organizations 工具禁用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 Organizations CLI/SDK 禁用信任服务访问权限

使用以下 Amazon CLI 命令或 API 操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令将 Amazon Managed Services (AMS) 自助报告 (SSR) 禁用 Organizations 的可信服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal selfservicereporting.managedservices.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- Amazon API：禁用AWSService访问权限

为 AMS 启用委托管理员账户

委派的管理员账户可以在 AMS 控制台的单个聚合视图中查看所有账户的 AMS 报告（例如补丁和备份）。

您可以使用 AMS 控制台或 API，也可以使用 Organizations `RegisterDelegatedAdministrator` CLI 或 SDK 操作来添加委派管理员。

禁用 AMS 的委派管理员

只有组织管理账户中的管理员才能为 AMS 配置委派管理员。

您可以使用 AMS 控制台或 API，也可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作来移除委派的管理员。

Amazon Macie 和 Amazon Organizations

Amazon Macie 是一个完全托管式数据安全和数据隐私服务，它使用机器学习和模式匹配来发现、监控并帮助您保护 Amazon Simple Storage Service（Amazon S3）中的敏感数据。Macie 可自动发现敏感数据，例如个人身份信息 (PII) 和知识产权，让您更好地了解您的组织存储在 Amazon S3 中的数据。

有关更多信息，请参阅《Amazon Macie 用户指南》中的使用 Amazon Organizations管理多个 Amazon Macie 账户。

使用以下信息来帮助您将 Amazon Macie 与集成。 Amazon Organizations

启用集成时，创建了一个服务相关角色

在启用可信访问权限时，系统自动在组织的委托 Macie 管理员账户中创建以下服务相关角色。此角色将允许 Macie 为您组织中的账户执行支持的操作。

只有在禁用 Macie 和 Organizations 之间的可信访问权限，或者您将该成员账户从组织中删除时，才能删除此角色。

- `AWSServiceRoleRorAmazonMacie`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Macie 使用的服务相关角色为以下服务委托人授予访问权限：

- `macie.amazonaws.com`

使用 Macie 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

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

> **Important**
>
> 强烈建议您尽可能使用 Amazon Macie 控制台或工具来实现与 Organizations 的集成。这可让 Amazon Macie 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon Macie 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。

如果您使用 Amazon Macie 控制台或工具启用信任访问权限，则您无需完成这些步骤。

要使用 Macie 控制台启用信任访问权限，请执行以下操作：

Amazon Macie 需要可信访问权限 Amazon Organizations 才能将成员账户指定为贵组织的 Macie 管理员。如果您使用 Macie 管理控制台配置委托管理员，Macie 会自动为您启用信任访问权限。

有关更多信息，请参阅《Amazon Macie 用户指南》中的在 Amazon Macie 中集成和配置组织。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来启用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令将 Amazon Macie 启用为 Organizations 的可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal macie.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

为 Macie 启用委托管理员账户

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 Macie 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 Macie 的管理分开。

最小权限

只有 Organizations 管理账户中具有以下权限的用户或角色才能将成员账户配置为组织中 Macie 的委托管理员：

- `organizations:EnableAWSServiceAccess`

- `macie:EnableOrganizationAdminAccount`

指定一个成员账户作为 Macie 的委托管理员

Amazon Macie 需要可信访问权限 Amazon Organizations 才能将成员账户指定为贵组织的 Macie 管理员。如果您使用 Macie 管理控制台配置委托管理员，Macie 会自动为您启用信任访问权限。

有关更多信息，请参阅 https://docs.amazonaws.cn/macie/latest/user/macie-organizations.html#register-delegated-admin

Amazon Web Services Marketplace 和 Amazon Organizations

Amazon Web Services Marketplace 是一个精心策划的数字目录，可用于查找、购买、部署和管理构建解决方案和运营业务所需的第三方软件、数据和服务。

Amazon Web Services Marketplace 使用 Amazon License Manager 在中购买时创建和管理许可证 Amazon Web Services Marketplace。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。

使用以下信息来帮助您集 Amazon Web Services Marketplace 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色 Amazon Web Services Marketplace 允许在组织中的组织账户中执行支持的操作。

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。使用的服务相关角色向以下服务主体 Amazon Web Services Marketplace 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。

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

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Web Services Marketplace 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Web Services Marketplace 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 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。
> 如果您使用 Amazon Web Services Marketplace 控制台或工具启用可信访问，则无需完成这些步骤。

使用 Amazon Web Services Marketplace 控制台启用可信访问

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。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Web Services Marketplace。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon Web Services Marketplace” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。

6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon Web Services Marketplace

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Web Services Marketplace zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

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。

您只能使用 Organizations 工具启用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Web Services Marketplace ations 中禁用可信服务。

  ```
  $ 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: D A isableAWSService ccess

Amazon Web Services Marketplace 私有市场 Amazon Organizations

Amazon Web Services Marketplace 是一个精心策划的数字目录，可用于查找、购买、部署和管理构建解决方案和运营业务所需的第三方软件、数据和服务。私人市场为您提供广泛的可用产品目录 Amazon Web Services Marketplace，以及对这些产品的精细控制。

Amazon Web Services Marketplace Private Marketplace 使您能够创建多个私有市场体验，这些体验与您的整个组织OUs、一个或多个账户、组织中的一个或多个账户相关联，每个账户都有自己的一套经批准的产品。您的 Amazon 管理员还可以通过公司或团队的徽标、消息和配色方案将公司品牌应用于每一次私人市场体验。

有关更多信息，请参阅《Amazon Web Services Marketplace 买家指南》中的 Using roles to configure Private Marketplace in Amazon Web Services Marketplace。

使用以下信息来帮助您将P Amazon Web Services Marketplace rivate Marketplace与集成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

当您使用 P Amazon Web Services Marketplace rivate Marketplace 控制台启用可信访问时，将在您组织的管理账户中自动创建以下服务相关角色。此角色允许 Private Marketplace 在您组织中的组织账户内执行支持的操作。只有在您禁用 Private Marketplace 和 Organization Amazon Web Services Marketplace s 之间的可信访问权限并取消组织中所有私有市场体验的关联后，您才能删除或修改此角色。

如果您直接从 Organizations 控制台启用可信访问SDK，CLI或者，服务相关角色不会自动创建。

- `AWSServiceRoleForPrivateMarketplaceAdmin`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Private Marketplace 使用的服务相关角色将为以下服务主体授予访问权限：

- `private-marketplace.marketplace.amazonaws.com`

启用与 Private Marketplace 的可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

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

> **Important**
>
> 我们强烈建议您尽可能使用 P Amazon Web Services Marketplace rivate Marketplace 控制台或工具来启用与 Organizations 的集成。这允许 P Amazon Web Services Marketplace rivate Marketplace 执行其所需的任何配置，例如创建服务所需的资源。只有当你无法使用 P Amazon Web Services Marketplace rivate Marketplace 提供的工具启用集成时，才能继续执行这些步骤。有关更多信息，请参阅此说明。
> 如果您使用 P Amazon Web Services Marketplace rivate Marketplace 控制台或工具启用可信访问，则无需完成这些步骤。

使用 Private Marketplace 控制台启用可信访问

请参阅《Amazon Web Services Marketplace 买家指南》中的 Getting started with Private Marketplace。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Web Services Marketplace Private Marketplace。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “为 P Amazon Web Services Marketplace rivate Marketplace 启用可信访问” 对话框中，键入 enable 进行确认，然后选择 “启用可信访问”。

6. 如果您只是 Private Marketplace 的管理员 Amazon Organizations，请告诉 P Amazon Web Services Marketplace rivate Marketplace 的管理员，他们现在可以 Amazon Organizations 从服务控制台启用该服务。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令将 P Amazon Web Services Marketplace rivate Marketplace 启用为 Organizations 的可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

禁用与 Private Marketplace 的可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Organizations 工具禁用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令将 P Amazon Web Services Marketplace rivate Marketplace 禁用 Organizations 作为可信服务。

```
$ aws organizations disable-aws-service-access \
    --service-principal private-marketplace.marketplace.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- Amazon API: D A isableAWSService ccess

为 Private Marketplace 启用委派管理员账户

管理账户的管理员可以将 Private Marketplace 的管理权限委派给被称为委派管理员的指定成员账户。要将账户注册为私有市场的委托管理员，管理账户管理员必须确保启用可信访问权限和服务相关角色，选择注册新管理员，提供 12 位 Amazon 账号，然后选择提交。

管理账户和委派管理员账户可以执行 Private Marketplace 管理任务，例如创建体验、更新品牌设置、关联受众或将其取消关联、添加或移除产品以及批准或拒绝待处理的请求。

要使用 Private Marketplace 控制台配置委派管理员，请参阅《Amazon Web Services Marketplace 买家指南》中的 Creating and managing a private marketplace。

您也可以使用 Organizations 配置委派管理员`RegisterDelegatedAdministrator`API。有关更多信息，请参阅 Organizati ons 命令参考 RegisterDelegatedAdministrator中的。

为 Private Marketplace 禁用委派管理员

只有组织管理账户中的管理员才能为 Private Marketplace 配置委派管理员。

您可以使用 Private Marketplace 控制台或API，或者使用 Organizations `DeregisterDelegatedAdministrator` CLI 或SDK操作移除委托的管理员。

要使用 Private Marketplace 控制台禁用 Private Marketplace 委派管理员账户，请参阅《Amazon Web Services Marketplace 买家指南》中的 Creating and managing a private marketplace

Amazon Web Services Marketplace 采购见解仪表板和 Amazon Organizations

您可以使用 Amazon Web Services Marketplace 采购见解控制面板查看组织中所有 Amazon 账户的协议和成本分析数据。与 Organizations 集成后， Amazon Web Services Marketplace 采购见解控制面板会监听组织变更，例如加入组织的账户，并汇总相应协议的数据以构建其仪表板。

有关更多信息，请参阅《Amazon Web Services Marketplace 买家指南》中的 Procurement insights。

使用以下信息来帮助您将 Amazon Web Services Marketplace 采购见解仪表板与集成 Amazon Organizations。

启用集成时创建的服务相关角色和托管式策略

激活 Amazon Web Services Marketplace 采购见解控制面板后，将创建AWSServiceRoleForProcurementInsightsPolicy服务相关角色和AWSServiceRoleForProcurementInsightsPolicy Amazon 托管策略。

启用与 Amazon Web Services Marketplace 采购详情的可信访问

启用可信访问权限使 Amazon Web Services Marketplace 采购见解控制面板能够与客户的 Organizations 服务集成。 Amazon Web Services Marketplace 采购见解仪表板监听组织变更，例如加入组织的账户，并汇总相应协议的数据以构建仪表板。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 Amazon Web Services Marketplace 采购见解控制面板控制台或控制台启用可信访问。 Amazon Organizations

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Web Services Marketplace 采购见解控制面板控制台或工具来实现与 Organizations 的集成。这使 Amazon Web Services Marketplace 采购见解仪表板可以执行其所需的任何配置，例如创建服务所需的资源。只有当你无法使用 Amazon Web Services Marketplace 采购见解控制面板提供的工具启用集成时，才能继续执行这些步骤。有关更多信息，请参阅此说明。
>
> 如果您使用 Amazon Web Services Marketplace 采购见解控制面板控制台或工具启用可信访问，则无需完成这些步骤。

通过启用 Amazon Web Services Marketplace 采购见解仪表板实现可信访问

请参阅《Amazon Web Services Marketplace 买家指南》中的 “启用 Amazon Web Services Marketplace 采购见解控制面板”。

使用 Organizations 工具启用可信访问

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Web Services Marketplace 采购详情控制面板。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “为 Amazon Web Services Marketplace 采购见解启用可信访问控制面板” 对话框中，键入 enab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告诉 Amazon Web Services Marketplace 采购见解仪表板的管理员，他们现在可以 Amazon Organizations 从服务控制台启用该服务。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令，将 Amazon Web Services Marketplace 采购见解仪表板启用为 Organizations 的可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal procurement-insights.marketplace.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- Amazon API: E A nableAWSService ccess

禁用与 Amazon Web Services Marketplace 采购详情控制面板的可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Organizations 工具禁用可信访问。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令将 Amazon Web Services Marketplace 采购见解仪表板作为 Organizations 的可信服务禁用。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal procurement-insights.marketplace.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- Amazon API: D isableAWSService 访问权限

启用委托管理员账户以获取 Amazon Web Services Marketplace 采购见解

要在 Amazon Web Services Marketplace 采购见解控制台中配置委派管理员，请参阅《Amazon Web Services Marketplace 买家指南》中的注册委托管理员>。

您也可以使用 Organizations 配置委派管理员`RegisterDelegatedAdministrator`API。有关更多信息，请参阅 Organizati ons 命令参考 RegisterDelegatedAdministrator中的。

禁用委派管理员获取 Amazon Web Services Marketplace 采购见解

只有组织管理账户中的管理员才能为 Amazon Web Services Marketplace 采购见解配置委派管理员。

要通过 Amazon Web Services Marketplace 采购见解控制台移除委派管理员，请参阅《Amazon Web Services Marketplace 买家指南》中的取消注册委托管理员。

您也可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或SDK操作移除委派的管理员。

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.amazonaws.com。
- 对于 AWSServiceRoleForCloudFormationStackSetsOrgMember 服务相关角色，唯一拥有访问权限的服务主体是 member.org.stacksets.cloudformation.amazonaws.com。
- 对于 AWSServiceRoleForCloudFormationStackSetsOrgAdmin 服务相关角色，唯一拥有访问权限的服务主体是 stacksets.cloudformation.amazonaws.com。
- 对于 AWSServiceRoleForCloudWatchCrossAccount 服务相关角色，唯一拥有访问权限的服务主体是 cloudwatch-crossaccount.amazonaws.com。

如果删除这些角色，则将影响 Network Manager 的多账户功能。

使用 Network Manager 启用可信访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

只有 Organizations 管理账户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。

使用 Network Manager 禁用可信访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Organizations 管理账户的管理员有权禁用对其他Amazon服务的可信访问权限。

> **Important**
>
> 我们强烈建议您使用 Network Manager 控制台禁用可信访问权限。如果通过任何其他方式（例如使用 Amazon CLI、API 或 Amazon CloudFormation 控制台）禁用可信访问权限，则可能无法正确清理已部署的 Amazon CloudFormation StackSets 和自定义 IAM 角色。要禁用可信服务访问权限，请登录 Network Manager 控制台。

为 Network Manager 启用委托管理员账户

将成员账户指定为组织的委托管理员后，该账户中的用户和角色将能够对 Network Manager 执行本来只能由组织管理账户中的用户或角色执行的管理操作。这有利于将组织的管理与 Network Manager 的管理分开。

有关如何将成员账户指定为组织中的 Network Manager 委托管理员的说明，请参阅《Amazon VPC 用户指南》中的注册委托管理员。

Amazon Q 开发者版与 Amazon Organizations

Amazon Q Developer 是一款由人工智能驱动的生成式对话助手，可以帮助您理解、构建、扩展和操作 Amazon 应用程序。这也是一款基于机器学习的通用代码生成器，可实时提供代码建议。Amazon Q 开发者版的付费订阅版本需要 Organizations 集成。有关更多信息，请参阅 Amazon Q 用户指南中的账户、IAM身份中心和组织设置。

使用以下信息来帮助您集成 Amazon Q Developer Amazon Organizations。

服务相关角色

`AWSServiceRoleForAmazonQDeveloper` 服务相关角色允许 Amazon Q 开发者版在您的组织内执行受支持的操作。使用 Amazon Q 开发者控制台创建角色 APICLI，或者，如IAM用户指南中的创建服务相关角色中所述。

如果您使用的是成员账户，则只有在 Amazon Q 开发者版与 Organizations 之间禁用可信访问，或者您从组织中移除该成员账户后，才能删除或修改此角色。

Amazon Q 开发者版使用的服务主体

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Amazon Q 开发者版使用的服务相关角色为以下服务主体授予访问权限：

- `q.amazonaws.com`

启用与 Amazon Q 开发者版的可信访问

Amazon Q 开发者版专业套餐使用可信访问，将组织管理账户中的设置与同一组织中的成员账户共享。

例如，Amazon Q 开发者版专业套餐管理员在 Organizations 管理账户中工作时，可以启用带代码参考的建议。如果启用了可信访问，则还会为该组织中的所有成员账户启用带代码参考的建议。

您只能使用 Amazon Q Developer 启用可信访问。

要为 Amazon Q 开发者版启用可信访问，请完成以下过程。

1. 在 Amazon Q 开发者版的设置页面中，选择成员账户设置下的编辑。
2. 在弹出窗口中，选择开启。
3. 选择保存。

有关更多信息，请参阅《Amazon Q 开发者版用户指南》中的 Enabling trusted access。

禁用与 Amazon Q 开发者版的可信访问

您只能使用 Amazon Q 开发者工具禁用可信访问。

要为 Amazon Q 开发者版禁用可信访问，请完成以下过程。

1. 在 Amazon Q 开发者版的设置页面中，选择成员账户设置下的编辑。
2. 在弹出窗口中，选择关闭。
3. 选择保存。

有关更多信息，请参阅《Amazon Q 开发者版用户指南》中的 Enabling trusted access。

Amazon Resource Access Manager 和 Amazon Organizations

Amazon Resource Access Manager (Amazon RAM) 使您能够与其他人共享您拥有的指定 Amazon 资源 Amazon Web Services 账户。这是一项集中式服务，可为跨多个账户共享不同类型的 Amazon 资源提供一致的体验。

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

使用以下信息来帮助您集 Amazon Resource Access Manager 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色 Amazon RAM 允许在组织中的组织账户中执行支持的操作。

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。使用的服务相关角色向以下服务主体 Amazon RAM 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。

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

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Resource Access Manager 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Resource Access Manager 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 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。

如果您使用 Amazon Resource Access Manager 控制台或工具启用可信访问，则无需完成这些步骤。

使用 Amazon RAM 控制台启用可信访问或 CLI

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

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Resource Access Manager。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon Resource Access Manager” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon Resource Access Manager

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Resource Access Manager zations 中启用可信服务。

```
$ 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: E A nableAWSService ccess

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。

您可以使用 Amazon Resource Access Manager 或 Amazon Organizations 工具禁用可信访问。

> **Important**
>
> 我们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。这允许 Amazon Resource Access Manager 执行它需要的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 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 控制台或工具禁用可信访问，则无需完成这些步骤。

使用 Amazon Resource Access Manager 控制台禁用可信访问或 CLI

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

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Resource Access Manager。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon Resource Access Manager” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。 Amazon Resource Access Manager

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Resource Access Manager ations 中禁用可信服务。

  ```
  $ 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: D A isableAWSService ccess

Amazon 资源探索器 和 Amazon Organizations

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

当你将 Resource Explorer 与 Amazon Organizations集成时，你可以将 Amazon Web Services 账户来自组织的多个证据纳入评估范围，从而从更广泛的来源收集证据。

使用以下信息来帮助您集 Amazon 资源探索器 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许资源管理器在您组织中的组织账户内执行支持的操作。

只有在禁用资源管理器和 Organizations 之间的信任访问权限时，或者如果您从组织中删除成员账户，才能删除或修改此角色。

有关资源管理器如何使用此角色的详细信息，请参阅《Amazon 资源探索器 用户指南》中的使用服务相关角色。

- `AWSServiceRoleForResourceExplorer`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。资源管理器使用的服务相关角色将为以下服务主体授予访问权限：

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

使用 Amazon 资源探索器启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

Resource Explorer 需要具有可信访问权限， Amazon Organizations 然后才能将成员帐户指定为组织的委派管理员。

您可以使用资源管理器控制台或 Organizations 控制台启用信任访问权限。强烈建议您尽可能使用资源管理器控制台或工具来实现与 Organizations 的集成。这允许 Amazon 资源探索器 执行它需要的任何配置，例如创建服务所需的资源。

使用资源管理器控制台启用可信访问权限

有关启用可信访问权限的说明，请参阅《Amazon 资源探索器 用户指南》中的使用资源管理器的先决条件。

> **Note**
>
> 如果您使用 Amazon 资源探索器 控制台配置委派管理员，则 Amazon 资源探索器 会自动为您启用可信访问权限。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来启用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon 资源探索器 zations 中启用可信服务。

```
$ aws organizations enable-aws-service-access \
    --service-principal resource-explorer-2.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- Amazon API: E A nableAWSService ccess

使用资源管理器禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Amazon Organizations 管理账户中的管理员才能使用禁用可信访问权限 Amazon 资源探索器。

您可以使用 Amazon 资源探索器 或 Amazon Organizations 工具禁用可信访问。

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon 资源探索器 控制台或工具来禁用与 Organizations 的集成。这允许 Amazon 资源探索器 执行它需要的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 Amazon 资源探索器提供的工具禁用集成时，才会使用这些步骤进行处理。
>
> 如果您使用 Amazon 资源探索器 控制台或工具禁用可信访问，则无需完成这些步骤。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon 资源探索器 ations 中禁用可信服务。

```
$ aws organizations disable-aws-service-access \
    --service-principal resource-explorer-2.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- Amazon API: D A isableAWSService ccess

为资源管理器启用委托管理员账户

使用您的委托管理员账户创建多账户资源视图，并将其范围限定为一个组织单位或整个组织。通过 Amazon Resource Access Manager 创建资源共享，您可以与组织中的任何账户共享多账户视图。

> **最小权限**
>
> 只有 Organizations 管理账户中具有以下权限的用户或角色才能将成员账户配置为组织中资源管理器的委托管理员：`resource-explorer:RegisterAccount`

有关为资源管理器启用委托管理员账户的说明，请参阅《Amazon 资源探索器 用户指南》中的设置。

如果您使用 Amazon 资源探索器 控制台配置委派管理员，则资源管理器会自动为您启用可信访问权限。

Amazon CLI, Amazon API

如果要使用 Amazon CLI或其中一个配置委派管理员帐户 Amazon SDKs，则可以使用以下命令：

- Amazon CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- Amazon SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，将账户服务标识`resource-explorer-2.amazonaws.com`为参数。

为资源管理器禁用委托管理员

只有 Organizations 管理账户中或资源管理器委托管理员账户中的管理员才能删除资源管理器的委托管理员。您可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或SDK操作禁用可信访问。

Amazon Security Hub 和 Amazon Organizations

Amazon Security Hub 为您提供 Amazon 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 可跨 Amazon Web Services 账户、您使用的 Amazon Web Services 服务以及受支持的第三方合作伙伴产品收集安全数据。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。

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。

禁用与 Security Hub 的可信访问

有关禁用可信访问所需权限的详细信息，请参阅《Amazon Organizations 用户指南》中的禁用可信访问所需的权限。

在禁用可信访问权限之前，可以选择与组织的委托管理员合作，禁用成员账户的 Security Hub，并清理这些账户的 Security Hub 资源。

您可以使用 Amazon Organizations 控制台、Organizations API 或 Amazon CLI 来禁用可信访问。只有 Organizations 管理账户中的管理员可以禁用与 Security Hub 的可信访问。

有关禁用与 Security Hub 的可信访问的说明，请参阅 Disabling Security Hub integration with Amazon Organizations。

为 Security Hub 启用委派管理员

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，选择常规下的设置。
3. 在 Delegated Administrator (委托管理员) 中，输入账户 ID。

为 Security Hub 禁用委派管理员

仅组织管理账户可以移除 Security Hub 委派管理员账户。

要更改 Security Hub 委派管理员，必须首先移除当前委派管理员账户，然后指定新的委派管理员账户。

如果您使用 Security Hub 控制台删除一个区域的委托管理员，该管理员将在所有区域中被自动删除。

Security Hub API 仅会从发出 API 调用或命令的区域中移除 Security Hub 委派管理员账户。您必须在其他区域重复执行此操作。

如果您使用 Organizations API 移除委托 Security Hub 管理员账户，则该账户将在所有区域中被自动移除。

有关禁用 Security Hub 委派管理员的说明，请参阅 Removing or changing the delegated administrator。

Amazon S3 Storage Lens 和 Amazon Organizations

通过向您的组织授予 Amazon S3 Storage Lens 可信访问权限，即允许其收集和汇总组织 Amazon Web Services 账户 内所有部门的指标。S3 Storage Lens 通过访问属于您组织的账户列表来实现此目的，并收集和分析所有账户的存储和使用情况以及活动指标。

有关更多信息，请参阅《Amazon S3 Storage Lens 用户指南》中的将服务相关角色用于 Amazon S3 Storage Lens。

使用以下信息来帮助您将 Amazon S3 存储镜头与集成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

在启用可信访问权限且 Storage Lens 配置已应用到您的企业时，系统自动在您企业的委托管理员账户中创建以下服务相关角色。此角色允许 Amazon S3 Storage Lens 在您组织中的组织账户内执行支持的操作。

只有在禁用 Amazon S3 Storage Lens 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForS3StorageLens`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Amazon S3 Storage Lens 使用的服务相关角色为以下服务委托人授予访问权限：

- `storage-lens.s3.amazonaws.com`

为 Amazon S3 Storage Lens 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 Amazon S3 Storage Lens 控制台或 Amazon Organizations 控制台启用信任访问权限。

> **Important**
>
> 强烈建议您尽可能使用 Amazon S3 Storage Lens 控制台或工具来实现与 Organizations 的集成。这可让 Amazon S3 Storage Lens 执行所需的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon S3 Storage Lens 提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
>
> 如果您使用 Amazon S3 Storage Lens 控制台或工具启用信任访问权限，则您无需完成这些步骤。

使用 Amazon S3 控制台启用信任访问权限

请参阅《Amazon Simple Storage Service 用户指南》中的为 S3 Storage Lens 存储统计管理工具启用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon S3 Storage Lens 存储统计管理工具。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “为 Amazon S3 存储镜头启用可信访问” 对话框中，键入 “启用” 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告诉 Amazon S3 Storage Lens 的管理员，他们现在可以 Amazon Organizations 从服务控制台启用该服务。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令将 Amazon S3 存储镜头启用为 Organizations 的可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal storage-lens.s3.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

为 Amazon S3 Storage Lens 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用 Amazon S3 存储镜头工具禁用可信访问。

您可以使用 Amazon S3 控制台、 Amazon CLI 或任一控制台禁用可信访问 Amazon SDKs。

使用 Amazon S3 控制台禁用信任访问权限

请参阅《Amazon Simple Storage Service 用户指南》中的为 S3 Storage Lens 存储统计管理工具禁用可信访问。

为 Amazon S3 Storage Lens 启用委托管理员账户。

将成员账户指定为组织的委托管理员时，该账户中的用户和角色可以对 Amazon S3 Storage Lens 执行管理操作，否则只能由组织管理账户中的用户或角色执行操作。这可以帮助您将组织的管理与 Amazon S3 Storage Lens 的管理分开。

> 最小权限
>
> 只有 Organizations 管理账户中具有以下权限的用户或角色才能将成员账户配置为组织中 Amazon S3 Storage Lens 存储统计管理工具的委托管理员：`organizations:RegisterDelegatedAdministrator`

```
    organizations:DeregisterDelegatedAdministrator
```

Amazon S3 Storage Lens 在您的组织中最多支持 5 个委托管理员账户。

指定一个成员账户作为 Amazon S3 Storage Lens 的委托管理员

您可以使用 Amazon S3 控制台、 Amazon CLI 或任意控制台注册委托管理员 Amazon SDKs。要使用 Amazon S3 控制台将某个成员账户注册为组织的委派管理员账户，请参阅《Amazon Simple Storage Service 用户指南》中的为 S3 Storage Lens 存储统计管理工具注册委派管理员。

为 Amazon S3 Storage Lens 取消注册委托管理员

您可以使用 Amazon S3 控制台、 Amazon CLI 或任意控制台取消注册委托管理员。 Amazon SDKs要使用 Amazon S3 控制台取消注册委派管理员，请参阅《Amazon Simple Storage Service 用户指南》中的取消注册 S3 Storage Lens 存储统计管理工具的委派管理员。

Amazon 安全事件响应和 Amazon Organizations

Amazon Security Incident Response 是一项安全服务，可提供全天候的人工辅助安全事件支持，以帮助客户快速响应证书盗用和勒索软件攻击等网络安全事件。通过与 Organizations 集成，您可以为整个组织提供安全保障。有关更多信息，请参阅《Amazon 安全事件响应用户指南》 Amazon Organizations中的 “使用管理安全事件响应帐户”。

使用以下信息来帮助您将 Amazon 安全事件响应与集成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

当您启用信任访问权限后，您组织的管理账户中会自动创建以下服务相关角色。

- `AWSServiceRoleForSecurityIncidentResponse`-用于创建安全事件响应会员资格-您通过订阅该服务 Amazon Organizations。
- `AWSServiceRoleForSecurityIncidentResponse_Triage`-仅在注册期间启用分类功能时使用。

安全事件响应使用的服务主体

上一节中的服务相关角色只能由通过为该角色定义的信任关系授权的服务主体担任。安全事件响应使用的服务相关角色向以下服务主体授予访问权限：

- `security-ir.amazonaws.com`

启用对安全事件响应的可信访问权限

启用对安全事件响应的可信访问权限使该服务能够跟踪您的组织结构，并确保组织中的所有账户都有有效的安全事件保障。当您启用会审功能时，它还允许服务使用成员账户中的服务关联角色来实现分类功能。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 Amazon 安全事件响应控制台或控制台启用可信访问。 Amazon Organizations

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon 安全事件响应控制台或工具来启用与 Organizations 的集成。这允许 Amazon 安全事件响应执行其所需的任何配置，例如创建服务所需的资源。只有在无法使用 Amazon 安全事件响应提供的工具启用集成时，才能继续执行这些步骤。有关更多信息，请参阅此说明。
> 如果您使用 Amazon 安全事件响应控制台或工具启用可信访问，则无需完成这些步骤。

当您使用安全事件响应控制台进行设置和管理时，Organizations 会自动启用 Organizations 的可信访问权限。如果您使用安全事件响应CLI/，SDK则必须使用 E Access 手动启用可信nableAWSService访问API。要了解如何通过安全事件响应控制台启用可信访问，请参阅《安全事件响应用户指南》中的“为 Amazon 账户管理启用可信访问”。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 “Amazon 安全事件响应”。
4. 选择 Enable trusted access (启用可信访问)。

5. 在 “为 Amazon 安全事件响应启用可信访问” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知 Amazon 安全事件响应的管理员，他们现在可以 Amazon Organizations 从服务控制台启用该服务。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令，将 “ Amazon 安全事件响应” 作为 Organizations 的可信服务启用。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal security-ir.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

使用 “安全事件响应” 禁用可信访问

只有 Organizations 管理帐户中的管理员才能通过 “安全事件响应” 禁用可信访问权限。

您只能使用 Organizations 工具禁用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 “Amazon 安全事件响应”。

4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “为 Amazon 安全事件响应禁用可信访问” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告诉 “ Amazon 安全事件响应” 的管理员，他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令将 Amazon 安全事件响应作为 Organizations 的可信服务禁用。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal security-ir.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: D A isableAWSService ccess

为安全事件响应启用委派管理员帐户

当您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安全事件响应执行管理操作，否则只能由组织管理账户中的用户或角色执行这些操作。这可以帮助您将组织管理与安全事件响应管理分开。有关更多信息，请参阅《Amazon 安全事件响应用户指南》 Amazon Organizations中的 “使用管理安全事件响应帐户”。

> 最小权限
>
> 只有 Organizations 管理账户中的用户或角色才能将成员账户配置为组织中安全事件响应的委托管理员

要了解如何通过安全事件响应控制台配置委派管理员，请参阅《安全事件响应用户指南》中的指定委派安全事件响应管理员帐户。

Amazon CLI, Amazon API

如果要使用 Amazon CLI或其中一个配置委派管理员帐户 Amazon SDKs，则可以使用以下命令：

- Amazon CLI:

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

- Amazon SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，将账户服务标识`security-ir.amazonaws.com`为参数。

禁用安全事件响应的委托管理员

> **Important**
>
> 如果成员资格是通过委派的管理员帐户创建的，则取消注册委派管理员是一种破坏性操作，并且会导致服务中断。要重新注册 DA，请执行以下操作：
>
> 1. 登录安全事件响应控制台，网址为 https://console.aws.amazon.com/security-ir/ home#/membership/settings
> 2. 从服务控制台取消成员资格。会员资格在账单周期结束之前一直有效。
> 3. 取消成员资格后，通过 Organizations 控制台禁用服务访问权限，CLI或者SDK。

只有 Organizations 管理账户中的管理员才能移除安全事件响应的委派管理员。您可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或SDK操作移除委派的管理员。

Amazon Security Lake 和 Amazon Organizations

Amazon Security Lake 将来自云端、本地和自定义源的安全数据集中到存储在您的账户的数据湖中。通过与 Organizations 集成，您可以创建一个数据湖来收集账户中的日志和事件。有关更多信息，请参阅《Amazon Security Lake 用户指南》中的使用 Amazon Organizations管理多个账户。

使用以下信息来帮助您将 Amazon Security Lake 与集成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

当您调用时，将在您组织的管理账户中自动创建以下服务相关角色。RegisterDataLakeDelegatedAdministratorAPI此角色允许 Amazon Security Lake 在您组织中的组织账户内执行支持的操作。

只有在 Amazon Security Lake 与 Organizations 之间禁用可信访问，或者您从组织中移除该成员账户后，才能删除或修改此角色。

- `AWSServiceRoleForSecurityLake`

> ⚠ 建议：使用 Security La RegisterDataLakeDelegatedAdministrator API ke 允许 Security Lake 访问您的组织并注册组织的委托管理员
>
> 如果您使用 Organi APIs zations 注册委托管理员，则可能无法成功创建组织的服务相关角色。为确保全部功能，请使用安全湖APIs。

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Amazon Security Lake 使用的服务相关角色将为以下服务主体授予访问权限：

- `securitylake.amazonaws.com`

启用与 Amazon Security Lake 的可信访问

当您授予对安全数据湖的信任访问权限时，安全数据湖可以自动应对组织成员资格的更改。委派的管理员可以在任何组织账户中启用从支持的服务收集 Amazon 日志。有关更多信息，请参阅《Amazon Security Lake 用户指南》中的亚马逊安全数据湖的服务相关角色。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Organizations 工具启用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Security Lake。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “为 Amazon Security Lake 启用可信访问” 对话框中，键入 enable 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告诉 Amazon Security Lake 的管理员，他们现在可以 Amazon Organizations 从服务控制台启用该服务。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令将 Amazon Security Lake 启用为 Organizations 的可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

禁用与 Amazon Security Lake 的可信访问

只有 Organizations 管理账户中的管理员可以禁用与 Amazon Security Lake 的可信访问。

您只能使用 Organizations 工具禁用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Security Lake。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用 Amazon Security Lake 的可信访问” 对话框中，键入 “禁用” 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告诉 Amazon Security Lake 的管理员，他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令将 Amazon Security Lake 禁用 Organizations 作为可信服务。

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

  如果成功，此命令不会产生任何输出。

- Amazon API: D A isableAWSService ccess

为 Amazon Security Lake 启用委派管理员账户

Amazon Security Lake 委派管理员可将组织中的其他账户添加为成员账户。委派管理员可为成员账户启用 Amazon Security Lake 并配置 Amazon Security Lake 设置。委派的管理员可以在启用了 Amazon Security Lake 的所有 Amazon 区域（无论您当前使用的是哪个区域终端节点）收集整个组织的日志。

您还可以将委托管理员设置为自动将组织中的新帐户添加为成员。Amazon Security Lake 委派管理员有权访问关联成员账户中的日志和事件。因此，您可以设置 Amazon Security Lake 来收集关联成员账户拥有的数据。您还可以授予订阅用户使用关联成员账户所拥有数据的权限。

有关更多信息，请参阅《Amazon Security Lake 用户指南》中的使用 Amazon Organizations管理多个账户。

> **最小权限**
>
> 只有 Organizations 管理账户中的管理员才能将某个成员账户配置为组织中的 Amazon Security Lake 委派管理员。

您可以使用 Amazon Security Lake 控制台、Amazon Security Lake `CreateDatalakeDelegatedAdmin` API 操作或`create-datalake-delegated-admin`CLI命令来指定委托管理员账户。或者，您可以使用 Organizati `RegisterDelegatedAdministrator` CLI ons 或SDK操作。有关为 Amazon Security Lake 启用委派管理员账户的说明，请参阅《Amazon Security Lake 用户指南》中的 Designating the delegated Security Lake administrator and adding member accounts。

Amazon CLI, Amazon API

如果要使用 Amazon CLI或其中一个配置委派管理员帐户 Amazon SDKs，则可以使用以下命令：

- Amazon CLI:

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

- Amazon SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，将账户服务委托人标识`account.amazonaws.com`为参数。

为 Amazon Security Lake 禁用委派管理员

只有 Organizations 管理账户或 Amazon Security Lake 委派管理员账户中的管理员才能从组织中移除委派管理员账户。

您可以使用 Amazon Security Lake `DeregisterDataLakeDelegatedAdministrator` API 操作、`deregister-data-lake-delegated-administrator`CLI命令或使用 Organizations `DeregisterDelegatedAdministrator` CLI 或SDK操作删除委托管理员账户。要使用 Amazon

Security Lake 移除委派管理员，请参阅《Amazon Security Lake 用户指南》中的 Removing the Amazon Security Lake delegated administrator。

Amazon Service Catalog 和 Amazon Organizations

借助 Service Catalog，您可以创建和管理获准在 Amazon上使用的 IT 服务的目录。

Service Catalog 与 Service Catalog 的集成 Amazon Organizations 简化了整个组织内的产品组合共享和产品复制。Service Catalog 管理员可以在共享产品组合 Amazon Organizations 时引用现有组织，也可以与组织树结构中的任何可信组织单位 (OU) 共享该产品组合。这样就无需共享投资组合IDs，也无需收款账户在导入投资组合时手动引用投资组合 ID。在 Service Catalog 中，通过此机制共享的产品组合将管理员的 Imported Portfolio（导入的产品组合）视图的共享目标账户中列出。

有关 Service Catalog 的更多信息，请参阅 服务目录管理员指南。

使用以下信息来帮助您集 Amazon Service Catalog 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

Amazon Service Catalog 不会创建任何与服务相关的角色作为启用可信访问的一部分。

用于授予权限的服务委托人

要启用信任访问权限，您必须指定以下服务委托人：

- `servicecatalog.amazonaws.com`

使用 Service Catalog 启用可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 Amazon Service Catalog 控制台或控制台启用可信访问。 Amazon Organizations

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Service Catalog 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Service Catalog 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon Service Catalog提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
>
> 如果您使用 Amazon Service Catalog 控制台或工具启用可信访问，则无需完成这些步骤。

使用 Service Catalog 启用可信访问CLI或 Amazon SDK

调用下列命令或操作之一：

- Amazon CLI: a ws 服务目录 enable-aws-organizations-access
- Amazon SDKs:: AWSServiceCatalog: E Access nableAWSOrganizations

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Service Catalog。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon Service Catalog” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon Service Catalog

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Service Catalog zations 中启用可信服务。

```
$ aws organizations enable-aws-service-access \
    --service-principal servicecatalog.amazonaws.com
```

  如果成功，此命令不会产生任何输出。

- Amazon API: E A nableAWSService ccess

使用 Service Catalog 禁用可信访问

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

如果您 Amazon Organizations 在使用 Service Catalog 时使用禁用可信访问，它不会删除您当前的共享，但会阻止您在整个组织中创建新的共享。如果在您调用此操作后当前共享发生更改，则它将不会与您的组织结构同步。

使用 Service Catalog 禁用可信访问CLI或 Amazon SDK

调用下列命令或操作之一：

- Amazon CLI: a ws 服务目录 disable-aws-organizations-access
- Amazon SDKs: D A isableAWSOrganizations ccess

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Service Catalog。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon Service Catalog” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。 Amazon Service Catalog

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Service Catalog ations 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。

- Amazon API: D A isableAWSService ccess

Service Quotas 和 Amazon Organizations

Service Quotas 是一项 Amazon 服务，可让您从中央位置查看和管理您的配额。配额（也称为限制）是 Amazon Web Services 账户中资源、操作和项目的最大值。

与 Service Quotas 关联后 Amazon Organizations，您可以创建配额请求模板，以便在创建账户时自动请求增加配额。

有关 Service Quotas 的更多信息，请参阅 Service Quotas 用户指南。

使用以下信息来帮助您将 Service Quotas 与集成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Service Quotas 在您组织中的组织账户内执行支持的操作。

只有在禁用 Service Quotas 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForServiceQuotas`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Service Quotas 使用的服务相关角色为以下服务委托人授予访问权限：

- `servicequotas.amazonaws.com`

启用其他 Service Quotas 服务的信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Service Quotas 启用可信访问。

您可以使用 Service Quotas 控制台启用可信访问， Amazon CLI 或者SDK：

- 使用 Service Quotas 控制台启用信任访问权限

  使用您的 Amazon Organizations 管理账户登录，然后在 Service Quotas 控制台上配置模板。有关更多信息，请参阅《Service Quotas 用户指南》中的使用 Service Quotas 模板。
- 使用 Service Quotas 启用可信访问 Amazon CLI 或 SDK

  调用以下命令或操作：
  - Amazon CLI: aw s 服务配额 associate-service-quota-template
  - Amazon SDKs: AssociateServiceQuotaTemplate

Amazon IAM Identity Center 和 Amazon Organizations

Amazon IAM Identity Center 为您的所有应用程序 Amazon Web Services 账户 和云应用程序提供单点登录访问权限。它通过 Amazon Directory Service 与 Microsoft Active Directory 连接，允许该目录中的用户使用其现有的 Active Directory 用户名和密码登录个性化 Amazon 访问门户。通过 Amazon 访问门户，用户可以访问他们有权访问的所有 Amazon Web Services 账户 和云应用程序。

有关 Ident IAM ity Center 的更多信息，请参阅《Amazon IAM Identity Center 用户指南》。

使用以下信息来帮助您集 Amazon IAM Identity Center 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 IAM Identity Center 在组织中的账户中执行支持的操作。

只有在禁用 Ident IAM ity Center 和 Organizations 之间的可信访问权限或从组织中删除成员帐户时，才能删除或修改此角色。

- AWSServiceRoleForSSO

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Ident IAM ity Center 使用的服务相关角色向以下服务主体授予访问权限：

- sso.amazonaws.com

使用IAM身份中心启用可信访问

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您可以使用 Amazon IAM Identity Center 控制台或控制台启用可信访问。 Amazon Organizations

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon IAM Identity Center 控制台或工具来启用与 Organizations 的集成。这允许 Amazon IAM Identity Center 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 Amazon IAM Identity Center提供的工具启用集成时执行这些操作步骤。有关更多信息，请参阅此说明。
> 如果您使用 Amazon IAM Identity Center 控制台或工具启用可信访问，则无需完成这些步骤。

IAMIdentity Center 需要可信访问权限 Amazon Organizations 才能正常运行。设置IAM身份中心时，会启用可信访问。有关更多信息，请参阅《Amazon IAM Identity Center 用户指南》中的入门 – 步骤 1：启用 Amazon IAM Identity Center。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。

3. 在服务列表中选择 Amazon IAM Identity Center。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon IAM Identity Center” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon IAM Identity Center

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon IAM Identity Center zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- Amazon API: E A nableAWSService ccess

使用IAM身份中心禁用可信访问

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

IAMIdentity Center 需要可信访问权限 Amazon Organizations 才能运行。如果您 Amazon Organizations 在使用 Ident IAM ity Center 时使用禁用可信访问，则它会因为无法访问组织而停止运行。用户无法使用 IAM Identity Center 访问账户。Ident IAM ity Center 创建的所有角色都将保留，但IAM身份中心服务无法访问它们。IAM身份中心服务相关角色仍然存在。如果您重新启用可信访问，Ident IAM ity Center 将继续像以前一样运行，而无需重新配置服务。

如果您从组织中删除帐户，Ident IAM ity Center 会自动清理所有元数据和资源，例如其服务相关角色。从组织中移除的独立账户将无法再在 Ident IAM ity Center 中使用。

您只能使用 Organizations 工具禁用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon IAM Identity Center。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon IAM Identity Center” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。 Amazon IAM Identity Center

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon IAM Identity Center ations 中禁用可信服务。

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

  如果成功，此命令不会产生任何输出。
- Amazon API: D A isableAWSService ccess

为 Ident IAM ity Center 启用委派管理员账户

当您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 Ident IAM ity Center 执行管理操作，否则这些操作只能由组织管理账户中的用户或角色执行。这可以帮助您将组织的管理与 Ident IAM ity Center 的管理分开。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色才能将成员账户配置为组织中 Ident IAM ity Center 的委派管理员。

有关如何为 Ident IAM ity Center 启用委派管理员帐户的说明，请参阅Amazon IAM Identity Center 用户指南中的委托管理。

Amazon Systems Manager 和 Amazon Organizations

Amazon Systems Manager 是一系列可实现 Amazon 资源可见性和控制的功能。以下 Systems Manager 功能可跨您组织中的所有 Amazon Web Services 账户 与 Organizations 配合工作：

- Systems Manager Explorer 是一个可自定义的操作控制面板，用于报告有关您的 Amazon 资源的信息。您可以使用 Organizations and Systems Manager Explorer 同步组织 Amazon Web Services 账户 中所有人的操作数据。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。
- Systems Manager OpsCenter 提供了一个中心位置，运营工程师和 IT 专业人员可以在其中查看、调查和解决与 Amazon 资源相关的运营工作项目 (OpsItems)。当您 OpsCenter 与 Organizations 一起使用时，它支持在单个会话 OpsItems 中使用管理帐户（组织管理帐户或 Systems Manager 委托的管理员帐户）和另一个帐户。配置后，用户可以执行以下类型的操作：
  - OpsItems 在另一个账户中创建、查看和更新。
  - 查看有关在其他账户 OpsItems 中指定的 Amazon 资源的详细信息。
  - 启动 Systems Manager Automation 运行手册以修复其他 Amazon 账户中的资源问题。

  有关更多信息，请参阅《Amazon Systems Manager 用户指南》中的 Amazon Systems Manager OpsCenter。
- 使用快速设置可根据推荐的最佳做法快速配置常用 Amazon 服务和功能。有关更多信息，请参阅《Amazon Systems Manager 用户指南》中的 Amazon Systems Manager Quick Setup。

  在 Systems Manager 注册 Amazon Organizations 委托管理员帐户时，您可以创建、更新、查看和删除针对组织中组织单位的快速设置配置管理器。要了解更多信息，请参阅《Amazon Systems Manager 用户指南》中的 “使用委托管理员进行快速设置”。

- 在为 Systems Manager 设置集成控制台时，需要输入委派的管理员帐户。此帐户用于在 “快速设置”、“资源管理器” 和 “资源管理器” 中注册 Amazon Organizations 委派的管理员帐户。CloudFormation StackSets要了解更多信息，请参阅为组织设置 Systems Manager 集成控制台Amazon Systems Manager 用户指南。

使用以下信息来帮助您集 Amazon Systems Manager 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色允许 Systems Manager 在您组织中的组织账户内执行支持的操作。

只有在禁用 Systems Manager 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Systems Manager 使用的服务相关角色为以下服务委托人授予访问权限：

- `ssm.amazonaws.com`

使用 Systems Manager 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用 Organizations 工具启用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。

2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Systems Manager。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon Systems Manager” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon Systems Manager

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Systems Manager zations 中启用可信服务。

  ```
  $ 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: E A nableAWSService ccess

使用 Systems Manager 禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

Systems Manager 需要可信访问权限才能同步组织 Amazon Web Services 账户 中的运营数据。Amazon Organizations 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。

您只能使用 Organizations 工具禁用可信访问。

您可以使用 Amazon Organizations 控制台、运行 Organizations Amazon CLI 命令或在其中一个中调用 Organizations API 操作来禁用可信访问 Amazon SDKs。

Amazon Web Services Management Console

使用 Organizations 控制台禁用信任服务访问权限

1. 登录 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Systems Manager。
4. 选择 Disable trusted access（禁用信任访问权限）。
5. 在 “禁用可信访问 Amazon Systems Manager” 对话框中，键入 dis able 进行确认，然后选择 “禁用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以使用服务控制台或工具禁止 Amazon Organizations 使用该服务。 Amazon Systems Manager

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

您可以使用以下 Amazon CLI 命令或API操作来禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Systems Manager ations 中禁用可信服务。

  ```
  $ 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: D A isableAWSService ccess

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。该帐户已被指定为在 Amazon Web Services 账户 变更管理器中管理变更模板、变更请求、变更运行手册和批准工作流的帐户。委托账户

管理整个组织的变更活动。当您设置您的组织以便使用 Change Manager 时，您要指定您的哪个账户在此角色中使用服务。它不必是组织的管理账户。如果您只对单个账户使用 Change Manager，则不需要委托管理员账户。

要将成员帐户指定为委托管理员，请参阅《Amazon Systems Manager 用户指南》中的以下主题：

- 对于 Explorer 和 OpsCenter，请参阅配置委派管理员。
- 有关 Change Manager 的信息，请参阅为 Change Manager 设置组织和委托账户。
- 有关快速设置，请参阅注册授权管理员进行快速设置。

禁用 Systems Manager 的委派管理员帐户

要取消注册委派管理员，请参阅《Amazon Systems Manager 用户指南》中的以下主题：

- 对于 Explorer 和 OpsCenter，请参阅注销 Explorer 授权的管理员。
- 有关 Change Manager 的信息，请参阅为 Change Manager 设置组织和委托账户。
- 有关快速设置，请参阅取消注册授权管理员以进行快速设置。

Amazon 用户通知服务 和 Amazon Organizations

Amazon 用户通知服务是您 Amazon 接收通知的中心位置。

与集成后 Amazon Organizations，您可以集中配置和查看组织中各个账户的通知。

使用以下信息来帮助您集 Amazon 用户通知服务 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色 用户通知服务 允许在组织中的组织账户中执行支持的操作。

只有在禁用 用户通知服务 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。

- `AWSServiceRoleForAWSUserNotifications`

有关更多信息，请参阅Amazon 用户通知服务 用户指南中的使用服务相关角色。

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。使用的服务相关角色向以下服务主体 用户通知服务 授予访问权限：

- notifications.amazon.com

使用 用户通知服务启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用启用可信访问 Amazon 用户通知服务。

要使用 用户通知服务 控制台启用可信访问，请参阅《用户通知服务 用户指南》 Amazon Organizations Amazon 用户通知服务中的 “启用”。

使用 用户通知服务禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您只能使用启用可信访问 Amazon 用户通知服务。

要使用 用户通知服务 控制台禁用可信访问，请参阅《用户通知服务 用户指南》 Amazon Organizations Amazon 用户通知服务中的 “启用”。

为其启用委派管理员账户 用户通知服务

管理账户管理员可以将 用户通知服务 管理权限委托给名为委派管理员的指定成员账户。要将账户注册为私有市场的委托管理员，管理账户管理员必须确保启用可信访问权限和服务相关角色，选择注册新管理员，提供 12 位 Amazon 账号，然后选择提交。

管理账户和授权管理员帐户可以执行 用户通知服务 管理任务，例如创建体验、更新品牌设置、关联或取消受众关联、添加或删除产品以及批准或拒绝待处理的请求。

要使用 用户通知服务 控制台配置委派管理员，请参阅用户通知服务 用户指南 Amazon 用户通知服务中的注册委托管理员。

您还可以使用 Organizations RegisterDelegatedAdministrator API 配置委派管理员。有关更多信息，请参阅 Organizati ons 命令参考 RegisterDelegatedAdministrator中的。

禁用委派的管理员 用户通知服务

只有组织管理账户中的管理员才能为其配置委派管理员 用户通知服务。

您可以使用 用户通知服务 控制台或 API，也可以使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作来移除委派的管理员。

要使用 用户通知服务 控制台禁用委派管理员 用户通知服务 帐户，请参阅《用户通知服务 用户指南》Amazon 用户通知服务中的删除委托管理员。

标签策略和 Amazon Organizations

标签策略是一种策略 Amazon Organizations ，可以帮助您标准化组织账户中各个资源的标签。有关标签策略的更多信息，请参阅标签策略。

使用以下信息来帮助您将标签策略与集成 Amazon Organizations。

服务相关角色使用的服务委托人

Organizations 使用以下服务委托人与附加到资源的标签进行交互。

- `tagpolicies.tag.amazonaws.com`

为标签策略启用信任访问权限

您可以通过在组织中启用标签策略或使用 Amazon Organizations 控制台来启用可信访问。

> **Important**
>
> 强烈建议您通过启用标签策略来启用信任访问权限。这使 Organizations 能够执行必需的设置任务。

您可以为标签策略启用信任访问权限，方法是在 Amazon Organizations 控制台中启用标签策略类型。有关更多信息，请参阅 启用策略类型。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须在组织的管理账户中以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）。

2. 在导航窗格中，选择服务。
3. 在服务列表中选择标签策略。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “为标签策略启用可信访问” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告诉标签策略的管理员，他们现在可以 Amazon Organizations 从服务控制台启用该服务。

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令将标签策略作为可信服务启用 Organizations。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal tagpolicies.tag.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: E A nableAWSService ccess

使用标记策略禁用信任访问权限

您可以通过在 Amazon Organizations 控制台中禁用标签策略类型来禁用标签策略的可信访问。有关更多信息，请参阅 禁用策略类型。

Amazon Trusted Advisor 和 Amazon Organizations

Amazon Trusted Advisor 检查您的 Amazon 环境，并在有机会节省资金、提高系统可用性和性能或帮助填补安全漏洞时提出建议。与 Organizations 集成后，您可以接收组织中所有账户的 Trusted Advisor 检查结果，并下载报告以查看支票摘要和任何受影响的资源。

有关更多信息，请参阅《Amazon Web Services 支持 用户指南》中的 Amazon Trusted Advisor的组织视图。

使用以下信息来帮助您集 Amazon Trusted Advisor 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色 Trusted Advisor 允许在组织中的组织账户中执行支持的操作。

只有在禁用 Trusted Advisor 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForTrustedAdvisorReporting`

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。使用的服务相关角色向以下服务主体 Trusted Advisor 授予访问权限：

- `reporting.trustedadvisor.amazonaws.com`

使用 Trusted Advisor启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

您只能使用启用可信访问 Amazon Trusted Advisor。

使用 Trusted Advisor 控制台启用可信访问

请参阅《Amazon Web Services 支持 用户指南》中的启用组织视图。

使用 Trusted Advisor禁用信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

禁用此功能后，将 Trusted Advisor 停止记录组织中所有其他账户的支票信息。您无法查看或下载现有报告或创建新报告。

您可以使用 Amazon Trusted Advisor 或 Amazon Organizations 工具禁用可信访问。

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Trusted Advisor 控制台或工具来禁用与 Organizations 的集成。这允许 Amazon Trusted Advisor 执行它需要的任何清理，例如删除服务不再需要的资源

或访问角色。仅当您无法使用 Amazon Trusted Advisor提供的工具禁用集成时，才会使用这些步骤进行处理。
如果您使用 Amazon Trusted Advisor 控制台或工具禁用可信访问，则无需完成这些步骤。

使用 Trusted Advisor 控制台禁用可信访问

请参阅《Amazon Web Services 支持 用户指南》中的禁用组织视图。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Trusted Advisor ations 中禁用可信服务。

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。
- Amazon API: D isableAWSService 访问权限

为其启用委派管理员账户 Trusted Advisor

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 管理账户中的用户或角色才能将成员账户配置为组织 Trusted Advisor 中的委托管理员

有关为其启用委派管理员账户的说明 Trusted Advisor，请参阅《Amazon Web Services 支持 用户指南》中的注册委派管理员。

Amazon CLI, Amazon API

如果要使用 Amazon CLI或其中一个配置委派管理员帐户 Amazon SDKs，则可以使用以下命令：

- Amazon CLI:

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

- Amazon SDK：调用 Organizations `RegisterDelegatedAdministrator` 操作和成员账户的 ID 号，将账户服务委托人标识`account.amazonaws.com`为参数。

禁用委派的管理员 Trusted Advisor

您可以使用 Trusted Advisor 控制台或使用 Organizations `DeregisterDelegatedAdministrator` CLI 或SDK操作来移除委派的管理员。有关如何使用 Trusted Advisor 控制台禁用委派管理员 Trusted Advisor 帐户的信息，请参阅Amazon Web Services 支持 用户指南中的取消注册委派管理员。

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 架构最佳实践进行比较。

Amazon Well-Architected Tool 与 Organizations 一起使用可以让 Amazon Well-Architected Tool 和组织客户简化与组织中其他成员共享 Amazon Well-Architected Tool 资源的流程。

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。

使用以下信息来帮助您集 Amazon Well-Architected Tool 成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

以下服务相关角色会在您启用信任访问权限时自动在组织的管理账户中创建。此角色 Amazon WA Tool 允许在组织中的组织账户中执行支持的操作。

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。使用的服务相关角色向以下服务主体 Amazon WA Tool 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结构变化。

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

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

> **Important**
>
> 我们强烈建议您尽可能使用 Amazon Well-Architected Tool 控制台或工具来启用与 Organizations 的集成。这允许 Amazon Well-Architected Tool 执行它需要的任何配置，例如创建服务所需的资源。请仅在您无法使用 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。
> 如果您使用 Amazon Well-Architected Tool 控制台或工具启用可信访问，则无需完成这些步骤。

使用 Amazon WA Tool 控制台启用可信访问

请参阅《Amazon Well-Architected Tool 用户指南》中的共享 Amazon Well-Architected Tool 资源。

您可以使用 Amazon Organizations 控制台、运行 Amazon CLI 命令或在其中一个中调用API操作来启用可信访问 Amazon SDKs。

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 Amazon Organizations 控制台。您必须以IAM用户身份登录、代入IAM角色或以 root 用户身份登录（不推荐）在组织的管理账户中登录。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon Well-Architected Tool。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “启用可信访问 Amazon Well-Architected Tool” 对话框中，键入 en ab le 进行确认，然后选择 “启用可信访问”。
6. 如果您仅是的管理员 Amazon Organizations，请告知管理员他们现在可以 Amazon Organizations 从服务控制台启用该服务。 Amazon Well-Architected Tool

Amazon CLI, Amazon API

使用 OrganizationsCLI/启用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作启用可信服务访问权限：

- Amazon CLI: enable-aws-service-access

  运行以下命令以在 Organi Amazon Well-Architected Tool zations 中启用可信服务。

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  如果成功，此命令不会产生任何输出。

- Amazon API: E A nableAWSService ccess

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。

您可以使用 Amazon Well-Architected Tool 或 Amazon Organizations 工具禁用可信访问。

> **Important**
>
> 我们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。这允许 Amazon Well-Architected Tool 执行它需要的任何清理，例如删除服务不再需要的资源或访问角色。仅当您无法使用 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 控制台或工具禁用可信访问，则无需完成这些步骤。

使用 Amazon WA Tool 控制台禁用可信访问

请参阅《Amazon Well-Architected Tool 用户指南》中的共享 Amazon Well-Architected Tool 资源。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令在 Organiz Amazon Well-Architected Tool ations 中禁用可信服务。

  ```
  $ 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: D A isableAWSService ccess

亚马逊 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，可让您更轻松地规划、跟踪和监控 Amazon 工作负载的 IP 地址。

使用 Amazon Organizations 允许您监控整个组织的 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 Amazon Organizations中的IPAM与集成。

使用以下信息来帮助您将 Amazon VPC IP 地址管理器 (IPAM) 与集成 Amazon Organizations。

启用集成时，创建了一个服务相关角色

当您使用IPAM控制台或使用IPAM控制台与组织管理账户和每个成员账户集成IPAM时，会自动在组织的管理账户和每个成员账户中创建以下服务相关角色。 Amazon Organizations `EnableIpamOrganizationAdminAccount` API

- `AWSServiceRoleForIPAM`

有关更多信息，请参阅 Amazon VPC IPAM 用户指南IPAM中的服务相关角色。

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为以下服务委托人授予访问权限：

- `ipam.amazonaws.com`

使用 IPAM 启用信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

> **Note**
>
> 当您为其指定委派管理员时IPAM，它会自动IPAM为您的组织启用可信访问权限。IPAM需要获得可信访问权限， Amazon Organizations 然后才能将成员账户指定为组织中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。

如果您使用IPAM控制台或 Amazon Organizations 使用IPAM进行集成 IPAM `EnableIpamOrganizationAdminAccount`API，则会自动向授予可信访问权限IPAM。授予可信访问权限会在管理账户和组织中的所有成员账户中创建服务相关角色 `Amazon ServiceRoleForIPAM`。 IPAM使用服务相关角色监控组织中与EC2网络资源CIDRs关联的并将相

关指标存储在 Amazon IPAM CloudWatch 中。有关更多信息，请参阅 Amazon VPC IPAM 用户指南 IPAM中的服务相关角色。

有关启用可信访问的说明，请参阅 Amazon VPC IPAM 用户指南 Amazon Organizations中的IPAM与集成。

> **Note**
>
> 您无法使用 Amazon Organizations 控制台或IPAM使用来启用可信访问EnableAWSServiceAccessAPI。

使用禁用可信访问 IPAM

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

只有 Amazon Organizations 管理账户中的管理员才能IPAM使用禁用可信访问 Amazon Organizations `disable-aws-service-access`API。

有关禁用IPAM账户权限和删除服务相关角色的信息，请参阅 A mazon VPC IPAM 用户指南IPAM中的服务相关角色。

您可以通过运行 Organizations Amazon CLI 命令或在其中一个中调用 Organization API s 操作来禁用可信访问 Amazon SDKs。

Amazon CLI, Amazon API

使用 OrganizationsCLI/禁用可信服务访问权限 SDK

使用以下 Amazon CLI 命令或API操作禁用可信服务访问权限：

- Amazon CLI: disable-aws-service-access

  运行以下命令禁用 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: D A isableAWSService ccess

为 IPAM 启用委托管理员账户

的委托管理员账户IPAM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 Amazon Organizations中的IPAM与集成。

只有组织管理账户中的管理员才能为其配置委派管理员IPAM。

您可以通过IPAM控制台指定委派管理员帐户，也可以使用`enable-ipam-organization-admin-account`API。有关更多信息，请参阅《 Amazon Amazon CLI 命令enable-ipam-organization-admin参考》中的- account。

> **最小权限**
>
> 只有 Organizations 管理账户中的用户或角色才能将某个成员账户配置为组织的 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 Amazon Organizations中的IPAM与集成。

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其配置委派管理员IPAM。

要使用删除委派管理员 Amazon Amazon CLI，请参阅《Amazon Amazon CLI 命令参考》中的disable-ipam-organization-admin- account。

要使用IPAM控制台禁用委托管理员IPAM账户，请参阅 Amazon VPC IPAM 用户指南 Amazon Organizations中的IPAM与集成。

Amazon VPC Reachability Analyzer 和 Amazon Organizations

Reachability Analyzer 是一种配置分析工具，使您能够在虚拟私有云（VPC）中的源资源和目标资源之间执行连接测试。

Amazon Organizations 与 Reachability Analyzer 一起使用可让您跟踪组织中各个账户的路径。

有关更多信息，请参阅《Reachability Analyzer 用户指南》中的 Manage delegated administrator accounts in Reachability Analyzer。

使用以下信息可帮助您将 Reachability Analyzer 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 Reachability Analyzer 在您组织中的组织账户内执行支持的操作。

只有在禁用 Reachability Analyzer 和 Organizations 之间的信任访问权限，或者如果您从组织中删除成员账户，您才能删除或修改此角色。

- `AWSServiceRoleForReachabilityAnalyzer`

有关更多信息，请参阅 Reachability Analyzer 用户指南中的 Cross-account analyses for Reachability Analyzer（Reachability Analyzer 的跨账户分析）。

服务相关角色使用的服务委托人

上一部分中的服务相关角色只能由为角色定义的信任关系授权的服务委托人担任。Reachability Analyzer 使用的服务相关角色为以下服务主体授予访问权限：

- `reachabilityanalyzer.networkinsights.amazonaws.com`

启用 Reachability Analyzer 信任访问权限

有关启用信任访问权限所需权限的信息，请参阅允许可信访问所需的权限。

当您为 Reachability Analyzer 指定委托管理员时，它会自动为您的组织启用 Reachability Analyzer 信任访问权限。

Reachability Analyzer 需要具有 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**
>
> - 您可以使用 Reachability Analyzer 控制台或 Organizations 控制台启用信任访问权限。但是，强烈建议您使用 Reachability Analyzer 控制台或 `EnableMultiAccountAnalysisForAwsOrganization` API 来实现与 Organizations 的集成。这可让 Reachability Analyzer 执行所需的任何配置，例如创建服务所需的资源。

- 授予可信访问权限将会在组织的管理账户和所有成员账户中创建服务相关角色 `AWSServiceRoleForReachabilityAnalyzer`。Reachability Analyzer 使用服务相关角色来支持管理，并允许委托管理员在组织中的任何资源之间运行连接分析。Reachability Analyzer 能够拍摄组织中账户的网络元素的快照，以回答连接查询。
- 有关更多信息以及有关通过 Reachability Analyzer 启用信任访问权限的说明，请参阅 Reacability Analyzer 用户指南中的 Cross-account analyses for Reachability Analyzer（Reachability Analyzer 的跨账户分析）。

您可以使用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 Amazon Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在服务页面上，找到 VPC Reachability Analyzer 行，选择服务的名称，然后选择启用可信访问权限。
3. 在确认对话框中，启用 Show the option to enable trusted access (显示启用信任访问权限的选项)，在框中输入 **`enable`**，然后选择 Enable trusted access (启用信任访问权限)。
4. 如果您只是 Amazon Organizations 的管理员，请告诉 Reachability Analyzer 的管理员，他们现在可以使用其控制台启用该服务来处理 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 Reachability Analyzer 作为 Organizations 的信任服务。

```
$ aws organizations enable-aws-service-access \
    --service-principal reachabilityanalyzer.networkinsights.amazonaws.com
```

如果成功，此命令不会产生任何输出。

- Amazon API：EnableAWSServiceAccess

禁用 Reachability Analyzer 信任访问权限

有关禁用信任访问所需权限的信息，请参阅禁止可信访问所需的权限。

您可以使用 Reachability Analyzer 控制台（建议）或 Organizations 控制台禁用信任访问权限。要使用 Reachability Analyzer 控制台禁用信任访问权限，请参阅 Reachability Analyzer 用户指南中的 Reachability Analyzer user guide（Reachability Analyzer 的跨账户分析）。

为 Reachability Analyzer 启用委托管理员账户

委托管理员账户能够对组织中的任何资源运行连接分析。有关更多信息，请参阅《Reachability Analyzer 用户指南》中的 将 Reachability Analyzer 与 Amazon Organizations 集成）。

只有组织管理账户中的管理员才能为 Reachability Analyzer 配置委托管理员。

您可以通过 Reachability Analyzer 控制台或使用 `RegisterDelegatedAdministrator` API 指定委托管理员账户。有关更多信息，请参阅 Organizations Command Reference（Organizations 命令参考）中的 RegisterDelegatedAdministrator。

> 最小权限
>
> 只有 Organizations 管理账户中的用户或角色才能将某个成员账户配置为组织的 Reachability Analyzer 委托管理员

要使用 Reachability Analyzer 控制台配置委托管理员，请参阅《Reachability Analyzer 用户指南》中的将 Reachability Analyzer 与 Amazon Organizations 集成。

禁用 Reachability Analyzer 的委托管理员

只有组织管理账户中的管理员才能为 Reachability Analyzer 配置委托管理员。

您可以使用 Reachability Analyzer 控制台或 API，或者通过使用 Organizations `DeregisterDelegatedAdministrator` CLI 或 SDK 操作，来删除委托管理员。

要使用 Reachability Analyzer 控制台禁用 Reachability Analyzer 委托管理员账户，请参阅 Reachability Analyzer 用户指南中的 Cross-account analyses for Reachability Analyzer（Reachability Analyzer 的跨账户分析）。

与 Organizations 配合使用的 Amazon Web Services 服务委派管理员

我们建议您将 Amazon Organizations 管理账户及其用户和角色仅用于必须由该账户执行的任务。此外，我们还建议您将所有的 Amazon 资源存储在组织的其他成员账户中，而非保存在管理账户中。这是因为，Organizations 服务控制策略（SCP）等安全功能不会限制管理账户中的用户或角色。将资源与管理账户分离还可帮助您了解发票上的费用。

许多与 Organizations 集成的 Amazon Web Services 服务可帮助您减少对管理账户的使用。这些服务允许您将一个或多个成员账户注册为管理员，用来管理该服务中使用的所有组织账户。这些账户被称为该特定服务的委托管理员。通过将成员账户注册为 Amazon 服务的委托管理员，您可以使该账户拥有该服务的某些管理权限以及 Organizations 只读操作权限。

在将账户注册为服务的委托管理员之前：

- 确认该服务支持委托管理员。请参阅 Amazon Web Services 服务 你可以和它一起使用 Amazon Organizations 中的表格，了解哪些服务支持委托管理员。
- 为该服务启用可信访问。

> **Note**
>
> 要了解如何为某个服务启用委托管理员，请参阅 Amazon Web Services 服务 你可以和它一起使用 Amazon Organizations 中的表格，然后在该服务的支持委托管理员列中选择了解详情链接。

授予委托管理员账户的权限

每个特定服务的委托管理员账户都具有该服务授予的权限。要了解更多信息，请参阅 Amazon Web Services 服务 你可以和它一起使用 Amazon Organizations 中的表格，然后在该服务的支持委托管理员列中选择了解详情链接。

委托管理员账户还具有以下只读权限：

- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy

借助这些权限，您可以查看但不能更改下列控制台项目：

- 组织结构、所有账户和 OU 以及组织策略
- 成员资格
- 所有账户和 OU。
- 组织策略

安全性 Amazon Organizations

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

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

- 云安全 — Amazon 负责保护在 Amazon 云 Amazon Web Services 服务 中运行的基础架构。Amazon 还为您提供可以安全使用的服务。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。要了解适用于的合规计划 Amazon Organizations，请参阅Amazon Web Services 服务 按合规计划划分的范围。
- 云端安全-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。您还将学习如何使用其他方法来帮助您监控和保护您 Amazon Web Services 服务 的 Organizations 资源。

主题

Amazon PrivateLink 对于 Amazon Organizations

使用 Amazon PrivateLink for Amazon Organizations，您无需通过公共互联网即可从虚拟私有云 (VPC) 内访问该 Amazon Organizations 服务。

Amazon VPC 允许您在自定义虚拟网络中启动 Amazon 资源。可以使用 VPC 控制您的网络设置，例如 IP 地址范围、子网、路由表和网络网关。有关更多信息 VPCs，请参阅 Amazon VPC 用户指南。

要将您的 Amazon VPC 连接到 Amazon Organizations，您必须先定义接口 VPC 终端节点（接口终端节点）。接口终端节点由一个或多个弹性网络接口 (ENIs) 表示，这些接口 () 是从您的 VPC 中的

子网中分配的私有 IP 地址。从您的 VPC 发往 Amazon Organizations 接口终端节点的请求将保留在 Amazon 网络上。

有关接口终端节点的一般信息，请参阅 Amazon VPC 用户指南中的使用接口 VPC 终端节点访问 Amazon 服务。

主题

- for 的 Amazon PrivateLink 限制和限制 Amazon Organizations
- 为创建 VPC 终端节点 Amazon Organizations
- 为 Amazon Organizations创建 VPC 端点策略

for 的 Amazon PrivateLink 限制和限制 Amazon Organizations

VPC 限制适用 Amazon PrivateLink 于 Amazon Organizations。有关更多信息，请参阅 Amazon VPC 用户指南中的使用接口 VPC 终端节点和Amazon PrivateLink 配额访问 Amazon 服务。此外，以下限制将适用：

- 仅在 us-east-1 区域中可用。
- 不支持传输层安全性协议（TLS）1.1

为创建 VPC 终端节点 Amazon Organizations

您可以使用 Amazon VPC 控制台 Amazon Command Line Interface （Amazon CLI）或，在您的 VPC 中创建 Amazon Organizations 终端节点 Amazon CloudFormation。

有关使用 Amazon VPC 控制台或创建和配置终端节点的信息 Amazon CLI，请参阅 Amazon VPC 用户指南中的创建 VPC 终端节点。有关使用创建和配置终端节点的信息 Amazon CloudFormation，请参阅Amazon CloudFormation 用户指南中的 AWSEC2::: VPCEndpoint 资源。

创建 Amazon Organizations 终端节点时，请使用以下内容作为服务名称：

```
com.amazonaws.us-east-1.organizations
```

如果您在访问时需要经过 FIPS 140-2 验证的加密模块 Amazon，请使用以下 Amazon Organizations FIPS 服务名称：

```
com.amazonaws.us-east-1.organizations-fips
```

为 Amazon Organizations创建 VPC 端点策略

您可以将端点策略附加到 VPC 端点，以控制对 Organizations 的访问。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用端点策略控制对 VPC 端点的访问。

示例： Amazon Organizations 操作的 VPC 端点策略

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

适用于 Identity and Access 管理 Amazon Organizations

Amazon Identity and Access Management (IAM) Amazon Web Services 服务 可帮助管理员安全地控制对 Amazon 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和获得授权（具有权限）以使用 Organizations 资源。您可以使用 IAM Amazon Web Services 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 如何 Amazon Organizations 与 IAM 配合使用
- 使用管理组织的访问权限 Amazon Organizations

- 适用于 Amazon Organizations的基于身份的策略示例
- 基于资源的策略示例 Amazon Organizations
- Amazon 的托管策略 Amazon Organizations
- 使用 Amazon Organizations 的标签进行基于属性的访问控制
- 对 Amazon Organizations 身份和访问进行故障排除

受众

您的使用方式 Amazon Identity and Access Management (IAM) 会有所不同，具体取决于您在 Organizations 中所做的工作。

服务用户 - 如果您使用 Organizations 服务来完成工作，则管理员会为您提供所需的凭证和权限。随着您使用更多 Organizations 功能来完成工作，您可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Organizations 中的功能，请参阅对 Amazon Organizations 身份和访问进行故障排除。

服务管理员 – 如果您在公司负责管理 Organizations 资源，您可能对 Organizations 具有完全访问权限。您有责任确定您的服务用户应访问哪些 Organizations 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解您的公司如何将 IAM 与 Organizations 结合使用，请参阅如何 Amazon Organizations 与 IAM 配合使用。

IAM 管理员 - 如果您是 IAM 管理员，您可能希望详细了解如何编写策略以管理对 Organizations 的访问。要查看您可在 IAM 中使用的 Organizations 基于身份的策略示例，请参阅适用于 Amazon Organizations的基于身份的策略示例。

使用身份进行身份验证

身份验证是您 Amazon 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 Amazon Web Services 账户根用户任 IAM 角色进行身份验证（登录 Amazon）。

如果您 Amazon 以编程方式访问，则会 Amazon 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 Amazon 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的Amazon 签名版本 4。

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

Amazon Web Services 账户 root 用户

创建时 Amazon Web Services 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 Amazon Web Services 服务 和资源。此身份被称为 Amazon Web Services 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 IAM 用户指南中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 Amazon Web Services 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C 或者任何使用 Amazon Web Services 服务 通过身份源提供的凭据进行访问的用户。 Amazon Directory Service当联合身份访问时 Amazon Web Services 账户，他们将扮演角色，角色提供临时证书。

IAM 用户和群组

I AM 用户是您 Amazon Web Services 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 Amazon Web Services 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 Amazon Web Services Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 Amazon Web Services 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 Amazon Web Services 服务 使用其他 Amazon Web Services 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 Amazon，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 Amazon Web Services 服务 向下游服务发出请求的请求。 Amazon Web Services 服务只有当服务收到需要与其他 Amazon Web Services 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 Amazon Web Services 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种链接到的服务角色。 Amazon Web Services 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 Amazon Web Services 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 Amazon 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含角色并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 Amazon 通过创建策略并将其附加到 Amazon 身份或资源来控制中的访问权限。策略是其中的一个对象 Amazon ，当与身份或资源关联时，它会定义其权限。 Amazon 在委托人（用户、root 用

户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 Amazon 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

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

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 Amazon Web Services 账户。托管策略包括 Amazon 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 Amazon Web Services 服务。

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

访问控制列表 (ACLs)

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

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 Amazon WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

Amazon 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs) — SCPs 是 JSON 策略，用于指定中组织或组织单位 (OU) 的最大权限 Amazon Organizations。 Amazon Organizations 是一项用于对您的企业拥有的多 Amazon Web Services 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中的实体（包括每个 Amazon Web Services 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 Amazon Web Services 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 Amazon Web Services 服务 该支持的列表 RCPs，请参阅《Amazon Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 Amazon 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 Amazon Organizations 与 IAM 配合使用

在使用 IAM 管理对 Organizations 的访问之前，您应该了解哪些 IAM 功能可与 Organizations 结合使用。

IAM 特征	Organizations 支持
基于身份的策略	是
基于资源的策略	是
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACLs	否
ABAC（策略中的标签）	是
临时凭证	否
转发访问会话（FAS）	是
服务角色	是
服务相关角色	是

要全面了解 Organizations 和其他 Amazon 服务如何使用大多数 IAM 功能，请参阅 IAM 用户指南中与 IAM 配合使用的Amazon 服务。

适用于 Organizations 的基于身份的策略

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

适用于 Organizations 的基于身份的策略示例

要查看 Organizations 基于身份的策略示例，请参阅适用于 Amazon Organizations的基于身份的策略示例。

Organizations 中基于资源的策略

支持基于资源的策略：是

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 Amazon Web Services 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 Amazon Web Services 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

Organizations 服务仅支持一种基于资源的策略（称为基于资源的委派策略），这种策略会指定哪些成员账户可以对策略执行操作。您可以在策略中添加多个语句来表示成员账户的不同权限集。

有关更多信息，请参阅 的委派管理员 Amazon Organizations。

Organizations 中基于资源的策略示例

要查看 Organizations 基于资源的策略示例，请参阅基于资源的策略示例 Amazon Organizations。

Organizations 的策略操作

支持策略操作：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 Amazon API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Organizations 操作的列表，请参阅《服务授权参考》中的 Actions defined by Amazon Organizations。

Organizations 中的策略操作在操作前使用以下前缀：

```
organizations
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "organizations:action1",
      "organizations:action2"
         ]
```

要查看 Organizations 基于身份的策略示例，请参阅适用于 Amazon Organizations的基于身份的策略示例。

Organizations 策略资源

支持策略资源：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 Organizations 资源类型及其列表 ARNs，请参阅《服务授权参考》 Amazon Organizations中定义的资源。要了解可以在哪些操作中指定每个资源的 ARN，请参阅 Amazon Organizations定义的操作。

要查看 Organizations 基于身份的策略示例，请参阅适用于 Amazon Organizations的基于身份的策略示例。

Organizations 的策略条件键

支持特定于服务的策略条件键：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 Amazon 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 Amazon 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

Amazon 支持全局条件密钥和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅 IAM 用户指南中的Amazon 全局条件上下文密钥。

有关 Organizations 条件键的列表，请参阅《服务授权参考》中的 Condition keys for Amazon Organizations。要了解可以使用条件键的操作和资源，请参阅由定义的操作 Amazon Organizations。

要查看 Organizations 基于身份的策略示例，请参阅适用于 Amazon Organizations的基于身份的策略示例。

ACLs 在组织中

支持 ACLs：否

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

将 ABAC 与 Organizations 结合使用

支持 ABAC（策略中的标签）：是

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 Amazon，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 Amazon 资源附加标签。标记实体和资源

是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时凭证用于 Organizations

支持临时凭证：否

当你使用临时证书登录时，有些 Amazon Web Services 服务 不起作用。有关更多信息，包括哪些 Amazon Web Services 服务 适用于临时证书，请参阅 IAM 用户指南中的Amazon Web Services 服务与 IAM 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 Amazon Web Services Management Console 使用的是临时证书。例如，当您 Amazon 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 Amazon CLI 或 Amazon API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 Amazon。 Amazon 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Organizations 的转发访问会话

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在中执行操作时 Amazon，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 Amazon Web Services 服务 向下游服务发出请求的请求。 Amazon Web Services 服务只有当服务收到需要与其他 Amazon Web Services 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Organizations 的服务角色

支持服务角色：是

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 Amazon Web Services 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会破坏 Organizations 的功能。只有在 Organizations 提供相关操作指导时，才能编辑服务角色。

Organizations 的服务相关角色

支持服务相关角色：是

服务相关角色是一种链接到的服务角色。 Amazon Web Services 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 Amazon Web Services 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的Amazon 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

使用管理组织的访问权限 Amazon Organizations

所有 Amazon 资源，包括组织中的根 OUs、账户和策略，均归属于 Amazon Web Services 账户，创建或访问资源的权限受权限策略的约束。对于一个组织，其管理账户拥有所有资源。账户管理员可以通过向 IAM 身份（用户、群组和角色）附加权限策略来控制对 Amazon 资源的访问权限。

> **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《Amazon 账户管理 参考指南》中的 IAM 安全最佳实践。

在授予权限时，您要决定谁获得权限，获得对哪些资源的权限，以及您允许对这些资源执行的具体操作。

默认情况下，IAM 用户、组和角色没有权限。作为组织管理账户的管理员，您可以执行管理任务或将管理员权限委派给管理账户中的其他 IAM 用户或角色。为此，您可以将 IAM 权限策略附加到 IAM 用户、组或角色。默认情况下，用户没有权限；这有时称为隐式拒绝。该策略将使用显式允许 覆盖隐式拒绝，这将指定用户可以执行哪些操作以及可对哪些资源执行这些操作。如果将权限授予了角色，则组织中其他账户的用户可以代入该角色。

Amazon Organizations 资源和运营

本节讨论 Amazon Organizations 概念如何映射到其等同于 IAM 的概念。

资源

在中 Amazon Organizations，您可以控制对以下资源的访问权限：

- 组织层次结构 OUs 的根源和构成组织层次结构的根源
- 组织的成员账户
- 您附加到组织中实体的账户
- 用于更改组织状态的握手

其中，每种资源均有一个与之关联的唯一 Amazon 资源名称 (ARN)。您可以通过在 IAM 权限策略的 `Resource` 元素中指定资源的 ARN 来控制对资源的访问。有关中使用的资源的 ARN 格式的完整列表 Amazon Organizations，请参阅《服务授权参考》 Amazon Organizations中定义的资源类型。

运营

Amazon 提供了一组操作来使用组织中的资源。利用这些操作，您可以对资源进行创建、列出、修改、访问其内容以及删除。可在 IAM policy 的 `Action` 元素中引用大多数操作来控制可使用操作的人员。有关可在 IAM 策略中用作权限的 Amazon Organizations 操作列表，请参阅《服务授权参考》中的 Actions defined by organizations。

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 提供了条件键，您可以通过查询这些条件键来对某些操作进行更精细的控制。您可以在 IAM policy 的 `Condition` 元素中参考这些条件密钥，以指定将语句视为匹配必须满足的其他条件。

以下条件键在以下情况下特别有用 Amazon Organizations：

- aws:PrincipalOrgID – 简化在基于资源的策略中指定 Principal 元素的过程。此全局密钥提供了一种替代方法，而不是列出组织 Amazon Web Services 账户 中所有人的所有账户 IDs 。您可以在元素中指定组织 IDCondition，而不是列出作为组织成员的所有账户。

  > **Note**
  >
  > 此全局条件也适用于组织的管理账户。

  有关更多信息，请参阅《IAM 用户指南》中的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 I A M 用户指南PrincipalOrgPaths中的 aws:。

  例如，以下条件元素匹配同一组织 OUs 中两个成员中任一的成员。

  ```
          "Condition": {
              "ForAnyValue:StringLike": {
                  "aws:PrincipalOrgPaths": [
                      "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
                      "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
                  ]
              }
          }
  ```

- organizations:PolicyType – 您可以使用此条件键限制与 Organizations 策略相关的 API 操作以仅处理指定类型的 Organizations 策略。您可以将此条件键应用于任何包含与 Organizations 策略交互的操作的策略语句。

  可以将以下值与此条件键结合使用：

  - SERVICE_CONTROL_POLICY
  - RESOURCE_CONTROL_POLICY
  - DECLARATIVE_POLICY_EC2
  - BACKUP_POLICY
  - TAG_POLICY

- CHATBOT_POLICY
- AISERVICES_OPT_OUT_POLICY

例如，以下示例策略允许用户执行任何 Organizations 操作。但是，如果用户执行采用策略参数的操作，则仅当指定的策略是标记策略时才允许该操作。如果用户指定任何其他类型的策略，则该操作将失败。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
    ]
}
```

- organizations:ServicePrincipal— 如果您使用 “启用AWSService访问” 或 “禁用访问” 操作启用或禁用AWSService对其他 Amazon 服务的可信访问，则可用作条件。您可以使用 organizations:ServicePrincipal 来将这些操作发出的请求限制为已批准的服务委托人名称列表。

  例如，以下策略允许用户仅在启用和禁用可信访问 Amazon Firewall Manager 时进行指定 Amazon Organizations。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

有关可用作 IAM 策略中权限的所有 Amazon Organizations特定条件密钥的列表，请参阅《服务授权参考》 Amazon Organizations中的条件密钥。

了解资源所有权

Amazon Web Services 账户 拥有在账户中创建的资源，无论谁创建了这些资源。具体而言，资源所有者是 Amazon Web Services 账户 对资源创建请求进行身份验证的委托人实体（即根用户、IAM 用户或 IAM 角色）。对于组织，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。（在中 Amazon Organizations，资源是 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**
>
> 本节讨论在的上下文中使用 IAM Amazon Organizations。这里不提供有关 IAM 服务的详细信息。有关完整的 IAM 文档，请参阅 IAM 用户指南。有关 IAM 策略语法和描述的信息，请参阅《IAM 用户指南》中的 IAM JSON 策略参考。

附加到 IAM 身份的策略称作基于身份的策略 (IAM policy)。附加到资源的策略称作基于资源的策略。Amazon Organizations 仅支持基于身份的策略 (IAM policy)。

主题

基于身份的权限策略 (IAM policy)

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，您可以执行以下操作：

- 将@@ 权限策略附加到您账户中的用户或群组-要向用户授予创建 Amazon Organizations 资源（例如服务控制策略 (SCP) 或 OU）的权限，您可以将权限策略附加到该用户所属的用户或群组。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。如果您想向 Amazon 服务授予担任该角色的权限，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 委托权限的更多信息，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 IAM 身份（用户、用户组和角色）。

基于资源的策略

一些服务（如 Amazon S3）支持基于资源的权限策略。例如，您可以将策略附加到 Amazon S3 存储桶，以管理对该存储桶的访问权限。 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

对于每种 Amazon Organizations 资源，该服务都定义了一组 API 操作或操作，这些操作或操作可以以某种方式与该资源交互或操纵该资源。要授予这些操作的权限，请 Amazon Organizations 定义一组可以在策略中指定的操作。例如，对于 OU 资源， Amazon Organizations 定义如下所示的操作：

- `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`允许或拒绝用户执行 Amazon Organizations `CreateAccount`操作的权限。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：影响。
- Principal – 在基于身份的策略 (IAM policy) 中，附加了策略的用户会自动成为隐式委托人。对于基于资源的策略，您可以指定要获得权限的用户、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，不支持基于资源的策略。

有关 IAM 策略语法和描述的信息，请参阅《IAM 用户指南》中的 IAM JSON 策略参考。

适用于 Amazon Organizations的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Organizations 资源的权限。他们也无法使用 Amazon Web Services Management Console、 Amazon Command Line Interface (Amazon CLI) 或 Amazon API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关 Organizations 定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》 Amazon Organizations中的操作、资源和条件密钥。 ARNs

主题

策略最佳实践

基于身份的策略用于确定某个人是否可以创建、访问或删除您账户中的 Organizations 资源。这些操作可能会使 Amazon Web Services 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 Amazon 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的Amazon 托管策略。它们在你的版本中可用 Amazon Web Services 账户。我们建议您通过定义针对您的用例的 Amazon 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略或工作职能的Amazon 托管式策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。

- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 Amazon Web Services 服务，例如 Amazon CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 Amazon Web Services 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 Organizations 控制台

要访问 Amazon Organizations 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 Organizations 资源的详细信息 Amazon Web Services 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 Amazon CLI 或 Amazon API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Organizations 控制台，还需要将 Organization `AWSOrganizationsReadOnlyAccess` Amazon s `AWSOrganizationsFullAccess`或托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 Amazon CLI 或 Amazon API 以编程方式完成此操作的权限。

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

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam/。
2. 在左侧的导航窗格中，选择策略。

   如果这是您首次选择策略，则会显示欢迎访问托管式策略页面。选择开始使用。
3. 在页面的顶部，选择创建策略。
4. 在策略编辑器部分，选择 JSON 选项。
5. 输入以下 JSON 策略文档：

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

6. 选择下一步。

> **Note**
>
> 您可以随时在可视化和 JSON 编辑器选项卡之间切换。不过，如果您进行更改或在可视化编辑器中选择下一步，IAM 可能会调整策略结构以针对可视化编辑器进行优化。有关更多信息，请参阅《IAM 用户指南》中的调整策略结构。

7. 在查看并创建页面上，为您要创建的策略输入策略名称和描述（可选）。查看此策略中定义的权限以查看策略授予的权限。
8. 选择创建策略可保存新策略。

要了解有关创建 IAM 策略的更多信息，请参阅《IAM 用户指南》中的创建 IAM 策略。

按操作授予有限访问权

如果只是授予有限权限而非完全权限，则可以创建一个策略，列出您打算在 IAM 权限策略的 `Action` 元素中允许的各个权限。如以下示例中所示，您可以使用通配符 (*) 字符来仅授予 `Describe*` 和 `List*` 权限，这实际上提供对组织的只读访问权限。

> **Note**
>
> 在服务控制策略 (SCP) 中，`Action` 元素中的通配符 (*) 字符只能由自身使用或用在字符串结尾处。它不能出现在字符串的开头或中间部分。因此，`"servicename:action*"`有效，但`"servicename:*action"`和在中`"servicename:some*action"`均无效 SCPs。

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

```
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "organizations:Describe*",
            "organizations:List*"
        ],
        "Resource": "*"
    }
}
```

有关可在 IAM 策略中分配的所有权限的列表，请参阅《服务授权参考》中的 Organi Amazon zations 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。这不适用于任何孩子 OUs。未授予账单访问权。请注意，这不会授予您对 OU Amazon Web Services 账户 中的的管理权限。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 控制台或致电获取 OU 和组织的信息`List*` APIs。IDs 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。

有关各种资源的更多信息，请参阅《 ARNs 服务授权参考》 Amazon Organizations中定义的资源类型。

向有限服务委托人授予允许可信访问的功能

您可以使用策略语句的 `Condition` 元素对策略语句匹配的情况做进一步限制。

示例：授予对一个指定服务允许可信访问的权限

以下语句显示如何将允许可信访问的功能局限于您指定的哪些服务。如果用户尝试使用与的服务主体不同的服务主体调用 API Amazon IAM Identity Center，则此策略不匹配，请求将被拒绝：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

有关各种资源的更多信息，请参阅《 ARNs 服务授权参考》 Amazon Organizations中定义的资源类型。

基于资源的策略示例 Amazon Organizations

以下代码示例说明如何使用基于资源的委托策略。有关更多信息，请参阅 的委派管理员 Amazon Organizations。

主题

示例：查看组织 OUs、账户和政策

在委托策略管理之前，您必须委派权限才能浏览组织结构并查看组织单位 (OUs)、账户和附加到它们的策略。

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

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

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:root"
      },
      "Action": [
```

```
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

示例：创建、读取、更新和删除策略

您可以创建基于资源的委派策略，允许管理账户委派任何策略类型的 `create`、`read`、`update` 和 `delete` 操作。此示例说明如何将服务控制策略的这些操作委托给成员账户*MemberAccountId*。示例中显示的两个资源分别授予对客户托管和托 Amazon 管服务控制策略的访问权限。

> **Important**
>
> 此策略允许委派管理员对组织中任何账户（包括管理账户）创建的策略执行指定操作。
> 此策略不允许委派管理员附加或分离策略，因为未包含执行
> `organizations:AttachPolicy` 和 `organizations:DetachPolicy` 操作所需的权限。

此示例委托策略授予 Amazon 通过 API 或 Amazon CLI以编程方式完成操作所需的权限。将*MemberAccountId*、*ManagementAccountId*和的 Amazon 占位符文本*OrganizationId*替换为您自己的信息。然后，按照 的委派管理员 Amazon Organizations 中的说明进行操作。

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

```
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "SERVICE_CONTROL_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingMinimalActionsForSCPs",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:CreatePolicy",
        "organizations:DescribePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy"
      ],
      "Resource": [
```

```
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
service_control_policy/*",
        "arn:aws:organizations::aws:policy/service_control_policy/*"
      ]
    }
  ]
}
```

示例：标记和取消标记策略

此示例展示了如何创建基于资源的委派策略，以允许委派管理员标记或取消标记备份策略。它授予 Amazon 通过 API 或 Amazon CLI以编程方式完成操作所需的权限。

要使用此委托策略，请将*MemberAccountIdManagementAccountId*、和*OrganizationId*的 Amazon 占位符文本替换为您自己的信息。然后，按照 的委派管理员 Amazon Organizations 中的说明进行操作。

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

```
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "BACKUP_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingTaggingBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:TagResource",
        "organizations:UntagResource"
      ],
      "Resource": "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
    }
  ]
}
```

示例：将策略附加到单个 OU 或账户

此示例展示了如何创建基于资源的委派策略，以允许来自指定组织单位（OU）或指定账户的委派管理员 `attach` 或 `detach` Organizations 策略。在委派这些操作之前，必须委派浏览组织结构并查看组织结构下账户的权限。有关详细信息，请参阅 示例：查看组织 OUs、账户和政策

> **Important**
>
> - 虽然此政策允许将策略与指定 OU 或账户关联或分离，但不包括子账号 OUs 和子账号。OUs
> - 此策略允许委托管理员对组织中任何账户（包括管理账户）创建的策略执行指定操作。

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AttachDetachPoliciesSpecifiedAccountOU",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/ou-OUId",
        "arn:aws:organizations::ManagementAccountId:account/
o-OrganizationId/TargetAccountId",
```

```
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

要将附加和分离策略的责任委派给组织中的任何 OU 或账户，请将上一个示例中的资源替换为以下资源：

```
"Resource": [
    "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/backup_policy/
*"
]
```

示例：管理组织备份策略所需的合并权限

此示例说明如何创建基于资源的委托策略，该策略允许管理账户委托管理组织内部备份策略所需的全部权限，包括 `create`、`read`、`update` 和 `delete` 操作以及 `attach` 和 `detach` 策略操作。

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

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
```

```
      },
      "Action": [
            "organizations:DescribeOrganization",
            "organizations:DescribeOrganizationalUnit",
            "organizations:DescribeAccount",
            "organizations:ListRoots",
            "organizations:ListOrganizationalUnitsForParent",
            "organizations:ListParents",
            "organizations:ListChildren",
            "organizations:ListAccounts",
            "organizations:ListAccountsForParent",
            "organizations:ListTagsForResource"
        ],
      "Resource": "*"
    },
    {
      "Sid": "DelegatingNecessaryDescribeListActionsForSpecificPolicyType",
      "Effect": "Allow",
      "Principal": {
            "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
            "organizations:DescribePolicy",
            "organizations:DescribeEffectivePolicy",
            "organizations:ListPolicies",
            "organizations:ListPoliciesForTarget",
            "organizations:ListTargetsForPolicy"
      ],
      "Resource": "*",
      "Condition": {
            "StringLikeIfExists": {
                "organizations:PolicyType": "BACKUP_POLICY"
            }
      }
    },
    {
      "Sid": "DelegatingAllActionsForBackupPolicies",
      "Effect": "Allow",
      "Principal": {
      "AWS": "arn:aws:iam::MemberAccountId:root"
    },
      "Action": [
            "organizations:CreatePolicy",
            "organizations:UpdatePolicy",
```

```
            "organizations:DeletePolicy",
            "organizations:AttachPolicy",
            "organizations:DetachPolicy",
            "organizations:EnablePolicyType",
            "organizations:DisablePolicyType"
      ],
      "Resource": [
            "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/
r-RootId",
            "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
            "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
            "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ],
      "Condition": {
            "StringLikeIfExists": {
                "organizations:PolicyType": "BACKUP_POLICY"
            }
      }
    }
  ]
}
```

Amazon 的托管策略 Amazon Organizations

本节列出了为 Amazon管理组织而提供的托管策略。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将其分离到组织中的实体。

Amazon Organizations 与 Amazon Identity and Access Management (IAM) 一起使用的托管策略

IAM托管策略由提供和维护 Amazon。托管策略提供常见任务的权限，您可以通过将托管策略附加到相应的用户或角色对象来分配给您的IAM用户。您不必自己编写政策，当根据需要 Amazon 更新政策以支持新服务时，您会自动立即从更新中受益。您可以在IAM控制台的 “策略” 页面中查看 Amazon 托管策略列表。使用 Filter policies (筛选策略) 下拉菜单，选择 Amazon managed (亚马逊云科技托管)。

您可以使用这些托管策略向组织中的用户授予权限。

Amazon 托管策略：AWSOrganizationsFullAccess

提供创建和完全管理组织所需的所有权限。

查看策略：AWSOrganizationsFullAccess。

Amazon 托管策略：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。

查看策略：AWSOrganizationsReadOnlyAccess。

Amazon 托管策略：DeclarativePoliciesEC2Report

AWSServiceRoleForDeclarativePoliciesEC2Report服务相关角色使用此策略来描述成员账户的账户属性状态。

查看策略：DeclarativePoliciesEC2Report。

对组织托 Amazon 管政策的更新

下表详细说明了自该服务开始跟踪这些更改以来对 Amazon 托管策略的更新。要获得有关此页面变更的自动提醒，请在 “Amazon Organizations 文档历史记录” 页面上订阅 RSS Feed。

更改	描述	日期
新的托管策略-DeclarativePoliciesEC2Report	添加了启用 AWSServiceRoleForDeclarativePoliciesEC2Report 服务相关角色功能的DeclarativePoliciesEC2Report 策略。	2024 年 11 月 22 日
AWSOrganizationsReadOnlyAccess— 更新为允许查看根用户电子邮件地址所需的账户API权限。	Organizations 增加了 account:GetPrimaryEmail 操作，以授予查看组织中任何成员账户的根用户电子邮件地址的访问权限，此外还增加了 account:GetRegionOptStatus 操作，以授予查看组织中任何成员账户的已启用区域的访问权限。	2024 年 6 月 6 日
AWSOrganizationsFullAccess— 更新为包括描述政策声明的Sid元素。	Organizations 为 AWSOrganizationsFullAccess 托管式策略增加了 Sid 元素。	2024 年 2 月 6 日

更改	描述	日期
AWSOrganizationsReadOnlyAccess— 更新为包括描述政策声明的Sid元素。	Organizations 为 AWSOrganizationsReadOnlyAccess 托管式策略增加了 Sid 元素。	2024 年 2 月 6 日
AWSOrganizationsFullAccess— 更新为允许 Amazon Web Services 区域 通过 Organizations 控制台启用或禁用所需的账户API权限。	Organizations 添加了针对策略的 account:ListRegions 、account:EnableRegion 和 account:DisableRegion 操作，以启用写入访问权限，来启用或禁用账户的区域。	2022 年 12 月 22 日
AWSOrganizationsReadOnlyAccess— 更新为允许 Amazon Web Services 区域 通过 Organizations 控制台发布商品所需的账户API权限。	Organizations 添加了针对策略的 account:ListRegions 操作，以启用查看账户区域的访问权限。	2022 年 12 月 22 日
AWSOrganizationsFullAccess— 更新为允许通过 Organizations 控制台添加或编辑账户联系人所需的账户API权限。	Organizations 添加了针对策略的 account:GetContactInformation 和 account:PutContactInformation 操作，以启用用于修改账户联系人的写入访问权限。	2022 年 10 月 21 日
AWSOrganizationsReadOnlyAccess— 更新为允许通过 Organizations 控制台查看账户联系人所需的账户API权限。	Organizations 添加了针对策略的 account:GetContactInformation 操作，以启用用于查看账户联系人的访问权限。	2022 年 10 月 21 日
AWSOrganizationsFullAccess— 已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	描述	日期
AWSOrganizationsFullAccess— 更新为允许通过 Organizations 控制台添加、编辑或删除账户备用联系人所需的账户API权限。	Organizations 添加了针对策略的 `account:GetAlternateContact` 、`account:DeleteAlternateContact` 、`account:PutAlternateContact` 操作，以启用用于修改账户备用联系人的写访问权限。	2022 年 2 月 22 日
AWSOrganizationsReadOnlyAccess— 更新为允许通过 Organizations 控制台查看账户备用联系人所需的账户API权限。	Organizations 添加了针对策略的 `account:GetAlternateContact` 操作，以启用用于查看账户备用联系人的访问权限。	2022 年 2 月 22 日

Amazon Organizations 托管服务控制策略

服务控制策略 (SCPs) 与IAM权限策略类似，但却是的功能， Amazon Organizations 而不是IAM。您可以使用指定SCPs受影响实体的最大权限。您可以附加SCPs到组织中的根目录、组织单位 (OUs) 或帐户。您可以创建自己的策略，也可以使用 IAM 定义的策略。您可以在 Organizations 控制台的 Policies (策略) 页面上查看组织中的策略列表。

> **Important**
>
> 每个 root、OU 和账户必须始终至少SCP关联一个。

策略名称	描述	ARN
FullAWSAccess	提供对成员账户的 Amazon Organizations 管理账户访问权限。	arn: aws: 组织:: aws:-F policy/service_control_policy/p ullAWSAccess

使用 Amazon Organizations 的标签进行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
- 检查附加到发出请求的 IAM 用户或角色的标签
- 检查请求中作为参数包含的标签

有关在策略中使用标签进行访问控制的更多信息，请参阅使用资源标签控制对 IAM 用户和角色的访问。有关 IAM 权限策略的完整语法，请参阅 IAM JSON 策略参考

检查附加到请求中指定资源的标签

当您使用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，以下示例策略仅在请求中存在的所有三个标签是此策略中的三个标签的子集时，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。

对 Amazon Organizations 身份和访问进行故障排除

以下信息有助您诊断和修复在使用 Organizations 和 IAM 时可能遇到的常见问题。

主题

- 我未获得在 Organizations 中执行操作的授权
- 我无权执行 iam：PassRole
- 我想允许我以外的人访问我的 Org Amazon Web Services 账户 anizations 资源

我未获得在 Organizations 中执行操作的授权

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `organizations:`*`GetWidget`* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 organizations:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 organizations:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到指示您未被授执行 iam:PassRole 操作的错误，则必须更新策略以允许您将角色传递给 Organizations。

有些 Amazon Web Services 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 Organizations 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人访问我的 Org Amazon Web Services 账户 anizations 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Organizations 是否支持这些功能，请参阅如何 Amazon Organizations 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 Amazon Web Services 账户 ，请参阅 IAM 用户指南中的向您拥有 Amazon Web Services 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 Amazon Web Services 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 Amazon Web Services 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。

- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

登录和监控 Amazon Organizations

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。这可以帮助您确保可以调查任何意外更改并回退不需要的更改。 Amazon Organizations 目前支持两个功能 Amazon Web Services 服务 ，使您能够监控您的组织及其内部发生的活动。

主题

使用 for 记录 API Amazon CloudTrail 调用 Amazon Organizations

Amazon Organizations 与 Amazon CloudTrail一项服务集成，该服务提供用户、角色或 Amazon 服务在中执行的操作的记录 Amazon Organizations。 CloudTrail 将所有 API 调用捕获 Amazon Organizations 为事件，包括来自 Amazon Organizations 控制台的调用和对的代码调用 Amazon Organizations APIs。如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括的事件 Amazon Organizations。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的事件历史记录中查看最新的事件。使用收集到的信息 CloudTrail，您可以确定向哪个请求发出 Amazon Organizations、发出的 IP 地址、谁发出、何时发出以及其他详细信息。

要了解更多信息 CloudTrail，请参阅Amazon CloudTrail 用户指南。

> **Important**
>
> 您 Amazon Organizations 只能查看美国东部（弗吉尼亚北部）区域的所有 CloudTrail 信息。如果您在 CloudTrail 主机中看不到自己的 Amazon Organizations 活动，请使用右上角的菜单将您的主机设置为美国东部（弗吉尼亚北部）。如果您使用 Amazon CLI 或 SDK 工具 CloudTrail 进行查询，请将查询定向到美国东部（弗吉尼亚北部）终端节点。

Amazon Organizations 信息在 CloudTrail

CloudTrail 在您创建账户 Amazon Web Services 账户 时已在您的账户上启用。当活动发生在中时 Amazon Organizations，该活动会与其他 Amazon 服务 CloudTrail 事件一起记录在事件历史记录中。

您可以在中查看、搜索和下载最近发生的事件 Amazon Web Services 账户。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

对于 Amazon Web Services 账户中的事件的持续记录（包括 Amazon Organizations的事件），请创建跟踪记录。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。在您的中启用 CloudTrail 日志记录后 Amazon Web Services 账户，对 Amazon Organizations 操作进行的 API 调用将在 CloudTrail 日志文件中进行跟踪，这些调用与其他 Amazon 服务记录一起写入日志文件。您可以配置其他 Amazon Web Services 服务 ，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail

所有 Amazon Organizations 操作均由 API 参考记录 CloudTrail 并记录在 Amazon Organizations API 参考中。例如，调用`CreateAccount`（包括`CreateAccountResult`事件）、`ListHandshakesForAccount`、`CreatePolicy`、和`InviteAccountToOrganization`会在 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
- 请求是否由其他 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

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。 CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会以任何特定顺序显示。

日志条目示例： CloseAccount

以下示例显示了`CloseAccount`调用 API 且关闭账户的工作流程在后台开始处理时生成的示例调用的 CloudTrail 日志条目。

```
{
    "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"
}
```

以下示例显示了成功完成关闭账户的后台工作流程之后CloseAccountResult呼叫的 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"
}
```

日志条目示例： CreateAccount

以下示例显示了CreateAccount调用 API 且创建账户的工作流程在后台开始处理时生成的示例调用的 CloudTrail 日志条目。

```
{
    "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"
```

```
}
```

以下示例显示了创建账户的后台工作流程成功完成后的CreateAccount呼叫 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"
    }
  }
}
```

以下示例显示了在后CreateAccount台工作流程无法创建帐户后生成的 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
    }
  }
}
```

日志条目示例： CreateOrganizationalUnit

以下示例显示了示例`CreateOrganizationalUnit`调用的 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"
}
```

日志条目示例： InviteAccountToOrganization

以下示例显示了示例`InviteAccountToOrganization`调用的 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"
}
```

日志条目示例： AttachPolicy

以下示例显示了示例AttachPolicy调用的 CloudTrail 日志条目。该响应指示，在请求尝试附加到的根中，由于请求的策略类型未启用，调用失败。

```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
        "policyId": "p-examplepolicyid111",
```

```
        "targetId": "ou-examplerootid111-exampleouid111"
    },
    "responseElements": null,
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

亚马逊 EventBridge 和 Amazon Organizations

Amazon Organizations 可以与 Amazon EventBridge（前身为 Amazon CloudWatch Events）合作，在组织中发生管理员指定的操作时引发事件。例如，大多数管理员希望每次在组织中创建新帐户时，或成员帐户的管理员尝试离开组织时收到提醒，因为这些都是敏感操作。您可以配置 EventBridge 规则来查找这些操作，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。

有关展示 EventBridge 如何启用监控组织中关键活动的教程，请参阅教程：使用 Amazon 监控组织的重要变更 EventBridge。

> **Important**
>
> 目前， Amazon Organizations 仅在美国东部（弗吉尼亚北部）地区托管（尽管它在全球范围内可用）。要执行本教程中的步骤，必须将配置 Amazon Web Services Management Console 为使用该区域。

要了解更多信息 EventBridge，包括如何配置和启用它，请参阅 Amazon EventBridge 用户指南。

Amazon Organizations的合规性验证

要了解是否属于特定合规计划的范围，请参阅Amazon Web Services 服务 “” Amazon Web Services 服务 中的 “按合规计划划分的范围”，然后选择您感兴趣的合规计划。 Amazon Web Services 服务 有关一般信息，请参阅合规计划。

您可以使用下载第三方审计报告 Amazon Artifact。有关更多信息，请参阅中的 “下载报告” Amazon Artifact。

您在使用 Amazon Web Services 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 Amazon 提供了以下资源来帮助实现合规性：

- Security & Compliance：这些解决方案实施指南讨论了架构考虑因素，并提供了部署安全性和合规性功能的步骤。
- 合规资源 — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- 使用Amazon Config 开发人员指南中的规则评估资源 — 该 Amazon Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- Amazon Security Hub— 这 Amazon Web Services 服务 可以全面了解您的安全状态 Amazon。Security Hub 通过安全控制措施评估您的 Amazon 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控制措施的列表，请参阅 Security Hub 控制措施参考。
- Amazon GuardDuty — 它通过监控您的 Amazon Web Services 账户环境中是否存在可疑和恶意活动，来 Amazon Web Services 服务 检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。

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。

Amazon Organizations 中的基础设施安全性

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

您可以使用Amazon发布的 API 调用通过网络访问 Organizations。客户端必须支持以下内容：

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

此外，必须使用访问密钥 ID 和与 IAM 主体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。

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 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

故障排除 Amazon Organizations

如果您在使用时遇到问题 Amazon Organizations，请查阅本节的主题。

排查一般问题

使用此处的信息可以帮助您诊断和修复在使用时可能遇到的访问被拒绝或其他常见问题。 Amazon Organizations

主题

当我向发送请求时，我收到 “访问被拒绝” 消息 Amazon Organizations

- 验证您是否具有调用您请求的操作和资源的许可。管理员必须通过将 IAM policy 附加到您的用户、组或角色来授予权限。如果授予这些权限的政策声明包含任何条件，例如 time-of-day或 IP 地址限制，则您在发送请求时也必须满足这些要求。有关查看或修改适用于用户、组或角色的策略的信息，请参阅《IAM 用户指南》中的使用策略。
- 如果您要手动签署 API 请求（不使用 Amazon SDKs），请确认您已正确签署请求。

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

- 请确认您用于发出请求的 用户或角色具有正确的权限。临时安全凭证权限派生自 用户或角色，因此权限范围仅限于相应 用户或角色的权限。有关临时安全凭证权限的确定方式的更多信息，请参阅《IAM 用户指南》中的控制临时安全凭证的权限。

- 验证您的请求是否采用了正确的签名和适当的格式。有关详细信息，请参阅 IAM 用户指南中您所选软件开发工具包的工具包文档或使用临时安全证书请求 Amazon 资源访问权限。
- 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。当你使用 Amazon Organizations 控制台、API 或 Amazon CLI 命令在组织中创建账户时，这些信息不会自动收集。对于要独立开设的账户，您必须接受 Amazon 客户协议，选择支持计划，提供并验证所需的联系信息，并提供当前的付款方式。 Amazon 使用付款方式对账户未关联到组织期间发生的任何可计费（非 Amazon 免费套餐）Amazon 活动收费。有关更多信息，请参阅 使用成员账户退出组织 Amazon Organizations。

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。

- 在关闭或删除之前 Amazon Web Services 账户，请将其从您的组织中删除，这样它就不会继续计入您的配额。
- 有关如何请求增加配额的更多信息，请参阅最大值和最小值。

我在添加或删除账户时收到了一条“此操作需要一段等待期”消息

某些操作需要一段等待期。例如，您无法立即删除新创建的账户。过几天再尝试此操作。如果您在添加和删除账户时遇到有关账户配额的问题，请参阅最大值和最小值来了解有关如何请求提高配额的信息。

尝试向组织中添加账户时，我收到“organization is still initializing”消息

如果您收到此类错误，而且距您创建组织已过了一个多小时，请联系 Amazon Web Services 支持。

当我尝试将账户邀请到我的组织时，收到“Invitations are disabled (邀请被禁用)”消息。

当您启用组织中的所有功能时，会发生这种情况。此操作可能需要一些时间才能完成，并且需要所有成员账户进行响应。在操作完成之前，您无法邀请新账户加入组织。

我所做的更改不总是立即可见

作为全球数据中心的计算机要访问的服务， Amazon Organizations 使用称为最终一致性的分布式计算模型。您所做的任何更改都 Amazon Organizations 需要一段时间才能从所有可能的端点中看到。有些延迟是由将数据从服务器发送到服务器或从复制区域发送到复制区域所花费的时间造成的。 Amazon Organizations 还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。

有关其他人如何 Amazon Web Services 服务 受此影响的更多信息，请查阅以下资源：

- 《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
- 在 Amazon 大数据博客中@@ 使用 Amazon S3 和 Amazon Elast MapReduce ic 处理 ETL 工作流程时确保一致性
- EC2 亚马逊 EC2 API 参考中的@@ 最终一致性。

通过提出 HTTP 查询请求来调用 API

本节包含有关使用查询 API 的常规信息 Amazon Organizations。有关 API 操作和错误的详细信息，请参阅 Amazon Organizations API 参考。

> **Note**
>
> 与其直接调用 Amazon Organizations Query API，不如使用其中一个 Amazon SDKs。Amazon SDKs 由适用于各种编程语言和平台（Java、Ruby、.NET、iOS、Android 等）的库和示例代码组成。 SDKs 提供了一种便捷的方法来创建对 Amazon Organizations 和的编程访问 Amazon。例如，负责处理诸如对请求 SDKs 进行加密签名、管理错误和自动重试请求之类的任务。有关信息 Amazon SDKs，包括如何下载和安装它们，请参阅适用于 Amazon Web Services 的工具。

的查询 API Amazon Organizations 允许您调用服务操作。查询 API 请求是 HTTPS 请求，必须包含用于指示要执行的操作的`Action`参数。 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

- 了解如何查看、监控和管理 SageMaker 端点。
- 必须使用 HTTPS
- 对 Amazon Organizations API 请求进行签名

了解如何查看、监控和管理 SageMaker 端点。

Amazon Organizations 有一个托管在美国东部（弗吉尼亚北部）区域的全球 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，请参阅中的区域终端节点Amazon Web Services 一般参考。

必须使用 HTTPS

由于查询 API 返回安全凭证等敏感信息，必须使用 HTTPS 对所有 API 请求加密。

对 Amazon Organizations API 请求进行签名

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您的 Amazon Web Services 账户根用户 凭据进行日常工作 Amazon Organizations。您可以使用用户或角色的凭证。

要签署您的 API 请求，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 I AM 用户指南中的签署 Amazon API 请求。

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 安全证书-提供有关可用于访问的证书类型的一般信息 Amazon。
- IAM 中的安全最佳实践 — 提供有关使用 IAM 服务来帮助保护您的 Amazon 资源（包括中的资源）的建议 Amazon Organizations。
- IAM 中的临时安全凭证：说明如何创建和使用临时安全凭证。

使用 Organizations 的代码 Amazon SDKs

以下代码示例展示了如何将 Organizations 与 Amazon 软件开发套件 (SDK) 一起使用。

操作是大型程序的代码摘录，必须在上下文中运行。您可以通过操作了解如何调用单个服务函数，还可以通过函数相关场景的上下文查看操作。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

代码示例

- Organizations 的基本示例 Amazon SDKs
  - 使用 Organizations Amazon SDKs
    - 与 Amazon SDK或AttachPolicy一起使用 CLI
    - 与 Amazon SDK或CreateAccount一起使用 CLI
    - 与 Amazon SDK或CreateOrganization一起使用 CLI
    - 与 Amazon SDK或CreateOrganizationalUnit一起使用 CLI
    - 与 Amazon SDK或CreatePolicy一起使用 CLI
    - 与 Amazon SDK或DeleteOrganization一起使用 CLI
    - 与 Amazon SDK或DeleteOrganizationalUnit一起使用 CLI
    - 与 Amazon SDK或DeletePolicy一起使用 CLI
    - 与 Amazon SDK或DescribePolicy一起使用 CLI
    - 与 Amazon SDK或DetachPolicy一起使用 CLI
    - 与 Amazon SDK或ListAccounts一起使用 CLI
    - 与 Amazon SDK或ListOrganizationalUnitsForParent一起使用 CLI
    - 与 Amazon SDK或ListPolicies一起使用 CLI

Organizations 的基本示例 Amazon SDKs

以下代码示例说明如何使用 with 的基础 Amazon Organizations 知识 Amazon SDKs。

示例

- 使用 Organizations Amazon SDKs
  - 与 Amazon SDK或AttachPolicy一起使用 CLI

- 与 Amazon SDK或CreateAccount一起使用 CLI
- 与 Amazon SDK或CreateOrganization一起使用 CLI
- 与 Amazon SDK或CreateOrganizationalUnit一起使用 CLI
- 与 Amazon SDK或CreatePolicy一起使用 CLI
- 与 Amazon SDK或DeleteOrganization一起使用 CLI
- 与 Amazon SDK或DeleteOrganizationalUnit一起使用 CLI
- 与 Amazon SDK或DeletePolicy一起使用 CLI
- 与 Amazon SDK或DescribePolicy一起使用 CLI
- 与 Amazon SDK或DetachPolicy一起使用 CLI
- 与 Amazon SDK或ListAccounts一起使用 CLI
- 与 Amazon SDK或ListOrganizationalUnitsForParent一起使用 CLI
- 与 Amazon SDK或ListPolicies一起使用 CLI

使用 Organizations Amazon SDKs

以下代码示例演示了如何使用执行各个 Organizations 操作 Amazon SDKs。每个示例都包含一个指向的链接 GitHub，您可以在其中找到有关设置和运行代码的说明。

以下示例仅包括最常用的操作。有关完整列表，请参阅《Amazon Organizations API参考资料》。

示例

- 与 Amazon SDK或AttachPolicy一起使用 CLI
- 与 Amazon SDK或CreateAccount一起使用 CLI
- 与 Amazon SDK或CreateOrganization一起使用 CLI
- 与 Amazon SDK或CreateOrganizationalUnit一起使用 CLI
- 与 Amazon SDK或CreatePolicy一起使用 CLI
- 与 Amazon SDK或DeleteOrganization一起使用 CLI
- 与 Amazon SDK或DeleteOrganizationalUnit一起使用 CLI
- 与 Amazon SDK或DeletePolicy一起使用 CLI
- 与 Amazon SDK或DescribePolicy一起使用 CLI
- 与 Amazon SDK或DetachPolicy一起使用 CLI
- 与 Amazon SDK或ListAccounts一起使用 CLI

- 与 Amazon SDK或ListOrganizationalUnitsForParent一起使用 CLI
- 与 Amazon SDK或ListPolicies一起使用 CLI

与 Amazon SDK或**AttachPolicy**一起使用 CLI

以下代码示例演示如何使用 `AttachPolicy`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then calls the
    /// AttachPolicyAsync method to attach the policy to the root
    /// organization.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var policyId = "p-00000000";
        var targetId = "r-0000";

        var request = new AttachPolicyRequest
        {
```

```
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.AttachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
 Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 AttachPolicy” 中的。

CLI

Amazon CLI

将策略附加到根、OU 或账户

示例 1

以下示例说明如何将服务控制策略 (SCP) 附加到 OU：

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

示例 2

以下示例演示如何将服务控制策略直接附加到账户：

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
```

```
    --target-id 333333333333
```

- 有关API详细信息，请参阅Amazon CLI 命令参考AttachPolicy中的。

Python

SDK适用于 Python (Boto3)

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- 有关API详细信息，请参阅AttachPolicy中的 Amazon SDKPython (Boto3) API 参考。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或`CreateAccount`一起使用 CLI

以下代码示例演示如何使用 `CreateAccount`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
    /// the new account with the name specified in accountName.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var accountName = "ExampleAccount";
        var email = "someone@example.com";

        var request = new CreateAccountRequest
        {
            AccountName = accountName,
            Email = email,
        };

        var response = await client.CreateAccountAsync(request);
        var status = response.CreateAccountStatus;
```

```
            Console.WriteLine($"The staus of {status.AccountName} is
{status.State}.");
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 CreateAccount” 中的。

CLI

Amazon CLI

创建自动属于组织的成员账户

以下示例演示如何创建组织的成员账户。为成员账户配置的名称为 Production Account，电子邮件地址为 susan@example.com。 OrganizationAccountAccessRole 由于未指定 roleName 参数，Organizations 会使用默认名称自动创建IAM角色。此外，ALLOW由于未指定 IamUserAccessToBilling 参数，允许具有足够权限的IAM用户或角色访问账户账单数据的设置被设置为默认值。Organiations 会自动向 Susan 发送一封 “欢迎来到 Amazon” 电子邮件：

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

输出包括一个请求对象，以显示状态目前为 IN_PROGRESS：

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

稍后，您可以通过向 describe-create-account-status命令提供 Id 响应值作为 create-account-request-id参数值来查询请求的当前状态。

有关更多信息，请参阅《Organi Amazon zations 用户指南》中的在Amazon 组织中创建帐户。

- 有关API详细信息，请参阅Amazon CLI 命令参考CreateAccount中的。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或**CreateOrganization**一起使用 CLI

以下代码示例演示如何使用 `CreateOrganization`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Creates an organization in AWS Organizations.
    /// </summary>
    public class CreateOrganization
    {
        /// <summary>
        /// Creates an Organizations client object and then uses it to create
        /// a new organization with the default user as the administrator, and
        /// then displays information about the new organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
            {
                FeatureSet = "ALL",
            });
```

```
            Organization newOrg = response.Organization;

            Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
 {newOrg.MasterAccountId}");
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 CreateOrganization” 中的。

CLI

Amazon CLI

示例 1：创建新组织

Bill 想使用账户 111111111111 中的凭证创建一个组织。以下示例显示该账户成为新组织中的主账户。由于他没有指定功能集，因此，新组织默认为在根上启用所有功能并启用服务控制策略。

```
aws organizations create-organization
```

输出包括一个组织对象，其中包含有关新组织的详细信息：

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
```

```
        }
}
```

示例 2：创建仅启用整合账单功能的新组织

以下示例创建仅支持整合账单功能的组织：

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

输出包括一个组织对象，其中包含有关新组织的详细信息：

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

有关更多信息，请参阅《Amazon Organizations 用户指南》中的“创建组织”。

- 有关API详细信息，请参阅Amazon CLI 命令参考CreateOrganization中的。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或**CreateOrganizationalUnit**一起使用 CLI

以下代码示例演示如何使用 `CreateOrganizationalUnit`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitName = "ProductDevelopmentUnit";

        var request = new CreateOrganizationalUnitRequest
        {
            Name = orgUnitName,
            ParentId = "r-0000",
        };

        var response = await client.CreateOrganizationalUnitAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
```

```
                Console.WriteLine($"Successfully created organizational unit:
 {orgUnitName}.");
                Console.WriteLine($"Organizational unit {orgUnitName} Details");
                Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
 {response.OrganizationalUnit.Id}");
            }
            else
            {
                Console.WriteLine("Could not create new organizational unit.");
            }
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 CreateOrganizationalUnit” 中的。

CLI

Amazon CLI

在根 OU 或父 OU 中创建 OU

以下示例演示如何创建名为 AccountingOU 的 OU：

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

输出包括一个 organizationalUnit 对象，其中包含有关新 OU 的详细信息：

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- 有关API详细信息，请参阅Amazon CLI 命令参考CreateOrganizationalUnit中的。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或**CreatePolicy**一起使用 CLI

以下代码示例演示如何使用 `CreatePolicy`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations Policy.
/// </summary>
public class CreatePolicy
{
    /// <summary>
    /// Initializes the AWS Organizations client object, uses it to
    /// create a new Organizations Policy, and then displays information
    /// about the newly created Policy.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var policyContent = "{" +
            "   \"Version\": \"2012-10-17\"," +
            " \"Statement\" : [{" +
                " \"Action\" : [\"s3:*\"]," +
                " \"Effect\" : \"Allow\"," +
                " \"Resource\" : \"*\"" +
            "}]" +
```

```
            "}";

            try
            {
                var response = await client.CreatePolicyAsync(new
CreatePolicyRequest
                {
                    Content = policyContent,
                    Description = "Enables admins of attached accounts to
delegate all Amazon S3 permissions",
                    Name = "AllowAllS3Actions",
                    Type = "SERVICE_CONTROL_POLICY",
                });

                Policy policy = response.Policy;
                Console.WriteLine($"{policy.PolicySummary.Name} has the following
content: {policy.Content}");
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 CreatePolicy” 中的。

CLI

Amazon CLI

示例 1：使用策略的文本源文件创建JSON策略

以下示例说明如何创建名为的服务控制策略 (SCP) `AllowAllS3Actions`。策略内容取自本地计算机上名为 `policy.json` 的文件。

```
aws organizations create-policy --content file://policy.json --
name AllowAllS3Actions, --type SERVICE_CONTROL_POLICY --description "Allows
 delegation of all S3 actions"
```

输出包括一个策略对象，其中包含有关新策略的详细信息：

```
{
        "Policy": {
                "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource\":[\"*\"]}]}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::o-exampleorgid:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Allows delegation of all S3 actions",
                        "Name": "AllowAllS3Actions",
                        "Type":"SERVICE_CONTROL_POLICY"
                }
        }
}
```

示例 2：创建以JSON策略为参数的策略

以下示例向您展示了如何创建相同的策略SCP，这次是将策略内容作为JSON字符串嵌入到参数中。字符串必须在双引号前使用反斜杠进行转义，以确保在参数中将其视为文本，参数本身用双引号引起来：

```
aws organizations create-policy --content "{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource
\":[\"*\"]}]}" --name AllowAllS3Actions --type SERVICE_CONTROL_POLICY --
description "Allows delegation of all S3 actions"
```

有关在组织中创建和使用策略的更多信息，请参阅《Amazon Organizations 用户指南》中的“管理组织策略”。

- 有关API详细信息，请参阅Amazon CLI 命令参考CreatePolicy中的。

Python

SDK适用于 Python (Boto3)

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
def create_policy(name, description, content, policy_type, orgs_client):
    """
    Creates a policy.

    :param name: The name of the policy.
    :param description: The description of the policy.
    :param content: The policy content as a dict. This is converted to JSON
 before
                    it is sent to AWS. The specific format depends on the policy
 type.
    :param policy_type: The type of the policy.
    :param orgs_client: The Boto3 Organizations client.
    :return: The newly created policy.
    """
    try:
        response = orgs_client.create_policy(
            Name=name,
            Description=description,
            Content=json.dumps(content),
            Type=policy_type,
        )
        policy = response["Policy"]
        logger.info("Created policy %s.", name)
    except ClientError:
        logger.exception("Couldn't create policy %s.", name)
        raise
    else:
        return policy
```

- 有关API详细信息，请参阅CreatePolicy中的 Amazon SDKPython (Boto3) API 参考。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或**DeleteOrganization**一起使用 CLI

以下代码示例演示如何使用 DeleteOrganization。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Shows how to delete an existing organization using the AWS
    /// Organizations Service.
    /// </summary>
    public class DeleteOrganization
    {
        /// <summary>
        /// Initializes the Organizations client and then calls
        /// DeleteOrganizationAsync to delete the organization.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
```

```
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 DeleteOrganization” 中的。

CLI

Amazon CLI

删除组织

以下示例演示如何删除组织。要执行此操作，您必须是组织中主账户的管理员。该示例假设您之前已从组织中删除了所有成员账户和政策：OUs

```
aws organizations delete-organization
```

- 有关API详细信息，请参阅Amazon CLI 命令参考DeleteOrganization中的。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或**DeleteOrganizationalUnit**一起使用 CLI

以下代码示例演示如何使用 `DeleteOrganizationalUnit`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
```

```
    using Amazon.Organizations.Model;

    /// <summary>
    /// Shows how to delete an existing AWS Organizations organizational unit.
    /// </summary>
    public class DeleteOrganizationalUnit
    {
        /// <summary>
        /// Initializes the Organizations client object and calls
        /// DeleteOrganizationalUnitAsync to delete the organizational unit
        /// with the selected ID.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var orgUnitId = "ou-0000-00000000";

            var request = new DeleteOrganizationalUnitRequest
            {
                OrganizationalUnitId = orgUnitId,
            };

            var response = await client.DeleteOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 DeleteOrganizationalUnit” 中的。

CLI

Amazon CLI

删除 OU

以下示例说明如何删除 OU。该示例假设您之前已OUs从 OU 中删除了所有账户和其他账户：

```
aws organizations delete-organizational-unit --organizational-unit-id ou-examplerootid111-exampleouid111
```

- 有关API详细信息，请参阅Amazon CLI 命令参考DeleteOrganizationalUnit中的。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或**DeletePolicy**一起使用 CLI

以下代码示例演示如何使用 DeletePolicy。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
```

```
        /// Initializes the Organizations client object and then uses it to
        /// delete the policy with the specified policyId.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";

            var request = new DeletePolicyRequest
            {
                PolicyId = policyId,
            };

            var response = await client.DeletePolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted Policy: {policyId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete Policy: {policyId}.");
            }
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 DeletePolicy” 中的。

CLI

Amazon CLI

删除策略

以下示例演示如何删除组织的策略。该示例假设您之前已将策略与所有实体分离：

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- 有关API详细信息，请参阅Amazon CLI 命令参考DeletePolicy中的。

Python

SDK适用于 Python (Boto3)

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- 有关API详细信息，请参阅DeletePolicy中的 Amazon SDKPython (Boto3) API 参考。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或`DescribePolicy`一起使用 CLI

以下代码示例演示如何使用 `DescribePolicy`。

CLI

Amazon CLI

获取有关策略的信息

以下示例演示如何请求有关策略的信息：

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

输出包括一个策略对象，其中包含有关策略的详细信息：

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
}
```

- 有关API详细信息，请参阅Amazon CLI 命令参考DescribePolicy中的。

Python

SDK适用于 Python (Boto3)

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
```

```
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- 有关API详细信息，请参阅DescribePolicy中的 Amazon SDKPython (Boto3) API 参考。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或**DetachPolicy**一起使用 CLI

以下代码示例演示如何使用 DetachPolicy。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
```

```
    /// Shows how to detach a policy from an AWS Organizations organization,
    /// organizational unit, or account.
    /// </summary>
    public class DetachPolicy
    {
        /// <summary>
        /// Initializes the Organizations client object and uses it to call
        /// DetachPolicyAsync to detach the policy.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new DetachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.DetachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 DetachPolicy” 中的。

CLI

Amazon CLI

从根、OU 或账户分离策略

以下示例演示了如何从 OU 分离策略：

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- 有关API详细信息，请参阅Amazon CLI 命令参考DetachPolicy中的。

Python

SDK适用于 Python (Boto3)

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- 有关API详细信息，请参阅DetachPolicy中的 Amazon SDKPython (Boto3) API 参考。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或**ListAccounts**一起使用 CLI

以下代码示例演示如何使用 `ListAccounts`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Uses the AWS Organizations service to list the accounts associated
/// with the default account.
/// </summary>
public class ListAccounts
{
    /// <summary>
    /// Creates the Organizations client and then calls its
    /// ListAccountsAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();
```

```
            var request = new ListAccountsRequest
            {
                MaxResults = 5,
            };

            var response = new ListAccountsResponse();
            try
            {
                do
                {
                    response = await client.ListAccountsAsync(request);
                    response.Accounts.ForEach(a => DisplayAccounts(a));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about an Organizations account.
        /// </summary>
        /// <param name="account">An Organizations account for which to display
        /// information on the console.</param>
        private static void DisplayAccounts(Account account)
        {
            string accountInfo = $"{account.Id}
{account.Name}\t{account.Status}";

            Console.WriteLine(accountInfo);
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 ListAccounts” 中的。

CLI

Amazon CLI

检索组织中所有账户的列表

以下示例演示了如何请求组织中的账户列表：

```
aws organizations list-accounts
```

输出包含账户摘要对象的列表。

```
{
        "Accounts": [
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481830215.45,
                        "Id": "111111111111",
                        "Name": "Master Account",
                        "Email": "bill@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/222222222222",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835741.044,
                        "Id": "222222222222",
                        "Name": "Production Account",
                        "Email": "alice@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/333333333333",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835795.536,
                        "Id": "333333333333",
                        "Name": "Development Account",
                        "Email": "juan@example.com",
                        "Status": "ACTIVE"
```

```
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/444444444444",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835812.143,
                        "Id": "444444444444",
                        "Name": "Test Account",
                        "Email": "anika@example.com",
                        "Status": "ACTIVE"
                }
        ]
}
```

- 有关API详细信息，请参阅Amazon CLI 命令参考ListAccounts中的。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或**ListOrganizationalUnitsForParent**一起使用 CLI

以下代码示例演示如何使用 `ListOrganizationalUnitsForParent`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Lists the AWS Organizations organizational units that belong to an
    /// organization.
```

```
    /// </summary>
    public class ListOrganizationalUnitsForParent
    {
        /// <summary>
        /// Initializes the Organizations client object and then uses it to
        /// call the ListOrganizationalUnitsForParentAsync method to retrieve
        /// the list of organizational units.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var parentId = "r-0000";

            var request = new ListOrganizationalUnitsForParentRequest
            {
                ParentId = parentId,
                MaxResults = 5,
            };

            var response = new ListOrganizationalUnitsForParentResponse();
            try
            {
                do
                {
                    response = await
client.ListOrganizationalUnitsForParentAsync(request);
                    response.OrganizationalUnits.ForEach(u =>
DisplayOrganizationalUnit(u));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
```

```
        /// Displays information about an Organizations organizational unit.
        /// </summary>
        /// <param name="unit">The OrganizationalUnit for which to display
        /// information.</param>
        public static void DisplayOrganizationalUnit(OrganizationalUnit unit)
        {
            string accountInfo = $"{unit.Id} {unit.Name}\t{unit.Arn}";

            Console.WriteLine(accountInfo);
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 ListOrganizationalUnitsForParent” 中的。

CLI

Amazon CLI

检索父 OU 或根目录OUs中的列表

以下示例向您展示了如何获取指定根目录OUs中的列表：

```
aws organizations list-organizational-units-for-parent --parent-id r-
examplerootid111
```

输出显示指定的根包含两个，OUs并显示每个根的详细信息：

```
{
        "OrganizationalUnits": [
                {
                        "Name": "AccountingDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid111"
                },
                {
                        "Name": "ProductionDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid222"
                }
```

```
        ]
}
```

- 有关API详细信息，请参阅Amazon CLI 命令参考ListOrganizationalUnitsForParent中的。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

与 Amazon SDK或**ListPolicies**一起使用 CLI

以下代码示例演示如何使用 `ListPolicies`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();
```

```
            // The value for the Filter parameter is required and must must be
            // one of the following:
            //     AISERVICES_OPT_OUT_POLICY
            //     BACKUP_POLICY
            //     SERVICE_CONTROL_POLICY
            //     TAG_POLICY
            var request = new ListPoliciesRequest
            {
                Filter = "SERVICE_CONTROL_POLICY",
                MaxResults = 5,
            };

            var response = new ListPoliciesResponse();
            try
            {
                do
                {
                    response = await client.ListPoliciesAsync(request);
                    response.Policies.ForEach(p => DisplayPolicies(p));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";
```

```
            Console.WriteLine(policyInfo);
        }
    }
```

- 有关API详细信息，请参阅 “适用于 .NET 的 Amazon SDK API参考 ListPolicies” 中的。

CLI

Amazon CLI

检索特定类型组织中所有策略的列表

以下示例向您展示了如何获取 filter 参数所指定的列表：SCPs

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

输出包括含摘要信息的策略列表：

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
```

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

- 有关API详细信息，请参阅Amazon CLI 命令参考ListPolicies中的。

Python

SDK适用于 Python (Boto3)

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- 有关API详细信息，请参阅ListPolicies中的 Amazon SDKPython (Boto3) API 参考。

有关 Amazon SDK开发者指南和代码示例的完整列表，请参阅Amazon Organizations 与 Amazon SDK一起使用。本主题还包括有关入门的信息以及有关先前SDK版本的详细信息。

的文档历史记录 Amazon Organizations

下表介绍了 Amazon Organizations的主要文档更新。

- API 版本：2016-11-28
- 最新文档更新：2025 年 1 月 24 日

变更	说明	日期
组织与 Amazon 用户通知服务	您可以 用户通知服务 与集成 Amazon Organizations ，以便在组织中的各个账户中集中配置和查看通知。	2025年1月24日
Organizations 与 Amazon Managed Services (AMS) 自助服务报告 (SSR) 集成	您可以将 AMS SSR 与集成 Amazon Organizations ，以启用聚合自助服务报告 (SSR)。这是一项 AMS 功能，它允许 Advanced 和 Accelerate 客户查看在组织层面、跨账户汇总的现有自助服务报告。	2025 年 1 月 21 日
添加了声明性政策	您可以使用声明性策略在整个组织中大规模地集中声明和强制执行给 Amazon Web Services 服务 定配置所需的配置。连接后，当服务添加新功能或时，配置将始终保持不变 APIs。	2024 年 12 月 1 日
新的 Amazon 托管策略	添加了启用 declarative-policies-ec 2.amazonaws.com 服务相关角色功能的`DeclarativePoliciesEC2Report` 政策。	2024 年 11 月 22 日

更新了备份策略	Amazon Backup 策略更新了`selections` 策略密钥以包含`conditions` 策略密钥，并在架构中添加了新的`resources` 策略密钥。有了新的架构，您可以更灵活地选择备份策略的资源。	2024 年 11 月 14 日
集中管理成员账户的根访问权限	现在，您可以通过集中的根访问在 Amazon Organizations 中管理跨成员账户的特权根用户凭证。集中保护 Amazon Web Services 账户 托管使用的根用户凭证， Amazon Organizations 以移除和防止根用户凭证恢复和大规模访问。	2024 年 11 月 14 日
添加了资源控制策略 (RCPs)	您可以使用资源控制策略 (RCPs) 来控制组织中资源的最大可用权限。	2024 年 11 月 13 日
增加了聊天机器人策略	您可以使用聊天机器人策略来控制聊天应用程序（例如 Slack 和 Microsoft Teams）对组织中账户的访问权限。	2024 年 9 月 26 日
场景驱动的内容更新	Amazon Organizations 文档已更新，在整个指南中更加以场景为导向，并对内容进行了重组，以提高可读性和发现性。如果您对这些更改有反馈，请使用页面底部的提供反馈按钮。	2024 年 9 月 4 日
新增有关选择退出所有 AI 服务的主题	添加了有关如何选择退出所有支持的 Amazon AI 服务的文档。	2024 年 8 月 16 日

Organizations 现在支持一个组织有 1 万个账户	现在，您可以在一个组织中管理多达 1 万个成员账户，是之前 5000 个账户限额的两倍。如果您有有效的要求和业务需求，则可以申请 1 万个账户配额并获得批准，而无需通过 Organizations 或其他集成的 Amazon Web Services 服务进行服务限额检查。	2024 年 8 月 14 日
新增账户迁移主题	增加了有关如何将账户从一个组织迁移到另一个组织的文档。	2024 年 8 月 1 日
更新了备份策略	Amazon Backup 策略现在支持亚马逊 Elastic Block Store (Amazon EBS) 快照存档。有关更新后的示例，请参阅更新备份策略和备份策略语法和示例。	2024 年 7 月 9 日
更新了 AWSOrganizationsReadOnlyAccess 托管策略	在`account:GetPrimaryEmail` AWSOrganizationsReadOnlyAccess 策略中添加了允许查看组织中任何成员账户的根用户电子邮件地址的`account:GetRegionOptStatus` 操作，并添加了允许访问组织中任何成员账户的已启用区域的操作。	2024 年 6 月 6 日
新增有关更新根用户电子邮件地址的主题	Organizations 现在提供了集中更新组织中任何成员账户的根用户电子邮件地址的功能。	2024 年 6 月 6 日

更新了策略语句	在 Amazon Organizations 托管策略声明中添加了新Sid元素。	2024 年 2 月 6 日
新增有关注销管理账户的主题	增加了有关注销管理账户的注意事项的链接以及有关如何注销管理账户的详细步骤。	2024 年 2 月 1 日
更新了最佳实践	在最佳实践部分增加了新信息，以帮助确保与 IAM 最佳实践保持一致。	2023 年 6 月 12 日
更新了 AWSOrganizationsFullAccess 和 AWSOrganizationsReadOnlyAccess托管策略	两个托管策略均已更新，以启用对账户联系人的写入或读取访问。	2022 年 10 月 21 日
更新了 AWSOrganizationsFullAccess 托管策略	更新了托管式策略，以允许通过添加创建新组织需要的服务相关角色时所需的权限来创建组织。	2022 年 8 月 24 日
Organizations 通过 Amazon Organizations 控制台关闭账户功能	管理账户中的主体可以从 Amazon Organizations 控制台关闭成员账户，并使用 IAM 策略保护成员账户免遭意外关闭。	2022 年 3 月 29 日
将公告更新为可以使用 Amazon Organizations 控制台更新备用联系人	Organizations 现在允许使用 Amazon Organizations 控制台更新组织内账户的备用联系人。宣布账户管理参考中的新功能和要点以供说明。	2022 年 2 月 8 日

Organizations 托管策略更新 - 对现有策略的更新	更新了 AWSOrganizationsFullAccess 和 AWSOrganizationsReadOnlyAccess托管政策，允许通过 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 7 日
组织与 Amazon DevOps Guru 集成	您可以将 Amazon DevOps Guru Amazon Organizations 与集成，全面监控所有组织账户的应用程序运行状况并获得见解。	2022 年 1 月 3 日
Organizations 与 Amazon Detective 的集成	您可以将 Amazon D Amazon Organizations etective 与集成，确保您的侦探行为图能够让您了解所有组织账户的活动。	2021 年 12 月 16 日
与 Organizations 的集成 Amazon Config 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
与 Organiz Amazon Firewall Manager ations 的集成现在包括对委派管理员的支持	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	您可以将 Amazon Backup 持续备份功能与组织的备份策略结合使用。	2021 年 3 月 10 日

与 Organiz Amazon CloudFormation StackSets ations 的集成现在包括对委派管理员的支持	现在，您可以将组织中的一个成员帐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 更新了流程以启用组织中的所有功能。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
引入 Amazon Organizations 控制台 2.0 版	Amazon 推出了新版本的主 Amazon 机。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	现在 Amazon Web Services Marketplace ，您可以更轻松地在组织中的所有帐户之间共享软件许可证。	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	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 Amazon Web Services 账户 中的其他地方。	2020 年 11 月 18 日

Amazon Web Services 区域 在中国，现在 Amazon Resource Access Manager 支持作为 Organizations 值得信赖的服务	现在，在中国，当你使用 Organizations时，你可以将与 Organizations集成的 Amazon RAM 功能作为可信 Amazon RAM 的服务使用。	2020 年 11 月 18 日
Organizations 现在支持与 Amazon Security Hub	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	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 的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 tag-on-create和基于标签的访问控制	您可以在创建 Organizations 资源时为它们添加标签。您可以使用标签策略标准化 Organizations 资源上的标签使用情况。您可以使用 IAM 策略来限制仅访问具有指定标签键和值的资源。	2020 年 9 月 15 日
已添加 Amazon Health 为可信服务	您可以汇总组织中各个账户 Amazon Health 的事件。	2020 年 8 月 4 日
人工智能 (AI) 服务选择退出策略	您可以使用 AI 服务选择退出政策来控制 Amazon AI 服务是否可以存储和使用这些服务处理的客户内容（AI 内容），以开发和持续改进 Amazon 人工智能服务与技术。	2020 年 7 月 8 日
添加了备份策略并与集成 Amazon Backup	可以使用备份策略为组织中的所有账户创建和强制执行备份策略。	2020 年 6 月 24 日
支持 IAM 访问分析器的委托管理	使您能够将组织中的访问分析器的管理访问权限委派给指定的成员账户。	2020 年 3 月 30 日

与集成 Amazon CloudFormation StackSets	您可以创建服务托管的堆栈集，以将堆栈实例部署到由Amazon Organizations管理的账户。	2020 年 2 月 11 日
与 Compute Optimizer 集成	Compute Optimizer 已添加为可用于组织账户的服务。	2020 年 2 月 4 日
标签策略	您可以使用标签策略帮助在组织账户中跨资源标准化标签。	2019 年 11 月 26 日
与 Systems Manager 集成	您可以在 Systems Manager Explorer 中同步组织中所有 Amazon Web Services 账户 组织的操作数据。	2019 年 11 月 26 日
aws：PrincipalOrgPaths	新的全局条件密钥会检查发出请求的 IAM 用户、IAM 角色或 Amazon Web Services 账户 根用户的 Amazon Organizations 路径。	2019 年 11 月 20 日
与 Amazon Config 规则集成	您可以使用 Amazon Config API 操作来管理组织 Amazon Web Services 账户 内所有部门的 Amazon Config 规则。	2019 年 7 月 8 日
新增的可信访问服务	将 Service Quotas 作为可用于组织账户的服务添加。	2019 年 6 月 24 日
与 Cont Amazon rol Tower 集成	Amazon Control Tower 作为一项服务添加，可以与组织中的帐户配合使用。	2019 年 6 月 24 日

与集成 Amazon Identity and Access Management	IAM 为您的组织实体（组织根和账户）提供上次访问服务的数据。 OUs您可以使用这些数据将访问权限限制为仅您需要 Amazon Web Services 服务的。	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
资源、条件和服务控制策略中的NotAction 要素 (SCPs)	现在，您可以在中指定资源、条件和NotAction 元素，SCPs 以拒绝组织或组织单位 (OU) 中的账户进行访问。	2019 年 3 月 25 日
新增的可信访问服务	Amazon License Manager 并将 Service Catalog 添加为可与组织中的账户配合使用的服务。	2018 年 12 月 21 日
新增的可信访问服务	Amazon CloudTrail 并 Amazon RAM 添加为可与组织中的账户配合使用的服务。	2018 年 12 月 4 日
新增的可信访问服务	Amazon Directory Service 添加为一项可以与组织中的帐户配合使用的服务。	2018 年 9 月 25 日
电子邮件地址验证	您必须先验证您拥有与管理账户关联的电子邮件地址，然后才能邀请现有账户加入您的组织。	2018 年 9 月 20 日
CreateAccount notifications	CreateAccount 通知会发布到管理账户的 CloudTrail 日志中。	2018 年 6 月 28 日

新增的可信访问服务	Amazon Artifact 添加为一项可以与组织中的帐户配合使用的服务。	2018 年 6 月 20 日
新增的可信访问服务	Amazon Config 并 Amazon Firewall Manager 添加为可与组织中的账户配合使用的服务。	2018 年 4 月 18 日
可信服务访问	现在，您可以启用或禁用对组织中账户进行选择 Amazon Web Services 服务 工作的访问权限。IAM Identity Center 是最初受支持的可信服务。	2018 年 3 月 29 日
账户删除现在是自助服务	现在，您 Amazon Organizations 无需联系即可删除从内部创建的账户 Amazon Web Services 支持。	2017 年 12 月 19 日
增加了对新服务的支持 Amazon IAM Identity Center	Amazon Organizations 现在支持与 Amazon IAM Identity Center （IAM 身份中心）集成。	2017 年 12 月 7 日
Amazon 向所有组织账户添加了服务相关角色	将名`AWSServiceRoleForOrganizations` 为的服务相关角色添加到组织中的所有账户，以实现与其他 Amazon Web Services 服务账户 Amazon Organizations 之间的集成。	2017 年 10 月 11 日
您现在可以删除已创建的账户	客户现在可以在 Amazon Web Services 支持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	新服务发布时附带的 Amazon Organizations 文档的初始版本。	2017 年 2 月 17 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。