
AWS Organizations

用户指南



AWS Organizations: 用户指南

Copyright © 2019 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

什么是 AWS Organizations ?	1
AWS Organizations 功能	1
AWS Organizations 定价	2
访问 AWS Organizations	2
对 AWS Organizations 的支持和反馈	3
其他 AWS 资源	3
可与 AWS Organizations 一起使用的 AWS 服务	3
AWS Organizations 入门	7
了解...	7
AWS Organizations 术语和概念	7
教程	10
教程：创建和配置组织	10
先决条件	10
步骤 1：创建组织	11
步骤 2：创建组织单元	12
步骤 3：创建服务控制策略	13
步骤 4：测试组织的策略	16
教程：使用 CloudWatch Events 进行监控	16
先决条件	17
步骤 1：配置跟踪和事件选择器	18
步骤 2：配置 Lambda 函数	18
步骤 3：创建向订阅者发送电子邮件的 Amazon SNS 主题	19
步骤 4：创建 CloudWatch Events 规则	19
步骤 5：测试您的 CloudWatch Events 规则	20
清理：删除您不再需要的资源	21
创建和管理组织	22
创建组织	22
电子邮件地址验证	23
启用所有功能	24
在启用所有功能之前	24
开始启用所有功能的流程	24
批准启用所有功能或重新创建服务相关角色的请求	25
完成流程以启用所有功能	26
查看有关您的组织的详细信息	27
从主账户查看组织的详细信息	27
查看根的详细信息	27
查看 OU 的详细信息	28
查看账户的详细信息	28
查看策略的详细信息	29
移除主账户并删除组织	30
管理账户	31
您邀请 AWS 账户加入组织后对该账户的影响	31
您在组织中创建一个 AWS 账户对该账户的影响	31
邀请账户加入组织	32
向 AWS 账户发送邀请	32
管理组织的待处理邀请	33
接受或拒绝来自组织的邀请	34
创建账户	35
创建属于组织的 AWS 账户	35
访问成员账户	37
以根用户身份访问成员账户	37
在受邀成员账户中创建 OrganizationAccountAccessRole	38
访问具有主账户访问权角色的成员账户	39
删除成员账户	40

从组织中删除账户前需知	40
从组织中删除成员账户	41
作为成员账户退出组织	42
关闭账户	43
管理 OU	45
浏览根和 OU 层次结构	45
创建 OU	46
重命名 OU	46
将账户移动到 OU 或者在根和 OU 之间移动	47
删除您不再需要的 OU	47
管理策略	49
列出和显示有关 AWS Organizations 策略的信息	49
列出所有策略	49
列出附加到根、OU 或账户的所有策略	50
列出策略附加到的所有根、OU 和账户	50
获取有关策略的详细信息	51
在根上启用和禁用策略类型	51
将策略附加到根、OU 或账户	52
从根、OU 或账户分离策略	53
删除策略	54
服务控制策略	54
测试 SCP 的影响	55
SCP 大小限制	55
对权限的影响	55
使用访问数据改进 SCP	56
不受 SCP 限制的任务和实体	56
SCP 的工作方式	56
有关使用 SCP 的策略	57
创建和更新 SCP	59
示例 SCPs	62
SCP 语法	68
标记资源	74
AWS Organizations 中支持的资源	74
添加标签	74
查看账户上的标签	75
编辑标签值	75
删除标签	76
启用其他 AWS 服务的可信访问	77
允许可信访问所需的权限	77
禁止可信访问所需的权限	77
如何允许或禁止可信访问	78
AWS Organizations 和服务相关角色	79
在您的组织中支持可信访问的服务	79
AWS Artifact 和 AWS Organizations	80
AWS CloudTrail 和 AWS Organizations	80
AWS Config 和 AWS Organizations	80
AWS Directory Service 和 AWS Organizations	81
AWS Firewall Manager 和 AWS Organizations	81
AWS License Manager 和 AWS Organizations	82
AWS RAM 和 AWS Organizations	82
AWS Service Catalog 和 AWS Organizations	82
Service Quotas 和 AWS Organizations	83
AWS Single Sign-On 和 AWS Organizations	83
安全性	84
AWS Organizations 中的 AWS Identity and Access Management	84
身份验证	85
访问控制	85

管理您的 AWS 组织的访问权限	85
日志记录和监控	89
使用 AWS CloudTrail 记录 AWS Organizations API 调用	89
Amazon CloudWatch Events	94
合规性验证	94
弹性	95
基础设施安全	95
AWS Organizations 参考	96
AWS Organizations 的限制	96
名称的限制	96
最大值和最小值	96
管理的策略	97
AWS Organizations 托管服务控制策略	97
AWS Organizations 疑难解答	99
排查一般问题	99
当我向 AWS Organizations 发出请求时，收到了“access denied”(访问被拒绝) 消息	99
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	99
当我尝试以成员账户身份离开组织或以主账户身份删除成员账户时，收到“access denied”(拒绝访问) 消息	100
尝试向组织中添加账户时，我收到“limit exceeded”消息	100
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	100
尝试向组织中添加账户时，我收到“organization is still initializing”消息	100
我在创建了成员账户时使用了不正确的电子邮件地址	100
我所做的更改不总是立即可见	100
排查策略问题	101
服务控制策略	101
发出 HTTP 查询请求	104
终端节点	104
必须使用 HTTPS	104
签署 AWS Organizations API 请求	104
文档历史记录	106
AWS 词汇表	108

什么是 AWS Organizations ?

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

本用户指南定义 [AWS Organizations 的关键概念](#)、提供 [教程](#) 并说明了如何 [创建和管理组织](#)。

主题

- [AWS Organizations 功能 \(p. 1\)](#)
- [AWS Organizations 定价 \(p. 2\)](#)
- [访问 AWS Organizations \(p. 2\)](#)
- [对 AWS Organizations 的支持和反馈 \(p. 3\)](#)
- [可与 AWS Organizations 一起使用的 AWS 服务 \(p. 3\)](#)

AWS Organizations 功能

AWS Organizations 提供以下功能：

集中管理您的所有 AWS 账户

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

所有成员账户的整合账单

整合账单是 AWS Organizations 的一项功能。您可以使用组织的主账户整合和支付所有成员账户。

对账户进行分层分组以满足预算、安全性或合规性需求

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

控制每个账户可访问的 AWS 服务和 API 操作

作为组织主账户的管理员，您可以使用服务控制策略 (SCP) 指定组织中成员账户的最大权限数。在 SCP 中，您可以限制每个成员账户中的用户和角色可以访问的 AWS 服务、资源和各个 API 操作。您还可以定义有关何时限制对 AWS 服务、资源和 API 操作的访问的条件。这些限制甚至会覆盖组织内的成员账户的管理员。当 AWS Organizations 阻止某个成员账户访问服务、资源或 API 操作时，该账户中的用户或角色将无法访问这些对象，即使该成员账户的管理员在 IAM 策略中明确授予此类权限也是如此。

有关更多信息，请参阅 [管理 AWS Organizations 策略 \(p. 49\)](#)。

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

[IAM](#) 提供对单个账户中的用户和角色的精细控制。AWS Organizations 通过使您能够控制一个账户或一组账户中的哪些用户和角色可执行哪些操作来扩展对账户级别的控制。生成的权限是账户级别的 AWS Organizations 允许的内容的逻辑交集，以及 IAM 在该账户内的用户或角色级别明确授予的权限。换言之

之，用户只能访问 AWS Organizations 策略和 IAM 策略都允许的内容。如果任一策略阻止某个操作，用户将无法访问该操作。

与其他 AWS 服务集成

您可以将 AWS Organizations 中提供的多账户管理服务与选定 AWS 服务结合使用，以在作为组织成员的所有账户上执行任务。有关服务以及在组织范围级别使用每项服务的好处的列表，请参阅[可与 AWS Organizations 一起使用的 AWS 服务 \(p. 3\)](#)。

当您启用某个 AWS 服务代表您执行组织成员账户中的任务时，AWS Organizations 会在每个成员账户中为该服务创建一个 [IAM 服务相关角色](#)。此服务相关角色具有预定义的 IAM 权限，此类权限允许另一 AWS 服务在您的组织及其账户中执行特定任务。为了做到这一点，组织内的所有账户都自动具有一个 [服务相关角色](#)，该角色使 AWS Organizations 服务能够创建 AWS 服务（您为之允许可信访问）所需的服务相关角色。这些额外的服务相关角色附带有使指定服务能够仅执行您的配置选择所需的那些任务的策略。有关更多信息，请参阅[启用其他 AWS 服务的可信访问 \(p. 77\)](#)。

具备最终一致性的数据复制

与许多其他 AWS 服务一样，AWS Organizations 具有[最终一致性](#)。AWS Organizations 通过复制其区域内 AWS 数据中心的多个服务器上的数据来实现高可用性。如果成功请求更改某些数据，则更改会提交并安全存储。但是，之后必须在多个服务器中复制此更改。有关更多信息，请参阅[我所做的更改不总是立即可见 \(p. 100\)](#)。

AWS Organizations 定价

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

访问 AWS Organizations

您可以通过以下任何方式使用 AWS Organizations：

AWS 管理控制台

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

AWS 命令行工具

通过使用 AWS 命令行工具，您可以在系统的命令行上发出命令以执行 AWS Organizations 和 AWS 任务；这比使用控制台更快且更方便。如果要构建执行 AWS 任务的脚本，命令行工具也会十分有用。

AWS 提供两组命令行工具：[AWS 命令行界面 \(AWS CLI\)](#) 和 [AWS Windows PowerShell 工具](#)。有关安装和使用 AWS CLI 的更多信息，请参阅[AWS Command Line Interface 用户指南](#)。有关安装和使用 Windows PowerShell 工具的更多信息，请参阅[适用于 Windows PowerShell 的 AWS 工具 用户指南](#)。

AWS 开发工具包

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

AWS Organizations HTTPS 查询 API

AWS Organizations HTTPS 查询 API 使您能够以编程方式访问 AWS Organizations 和 AWS。HTTPS 查询 API 可让您直接向服务发布 HTTPS 请求。使用 HTTPS API 时，必须添加代码，才能使用您的

凭证对请求进行数字化签名。有关更多信息，请参阅[通过提出 HTTP 查询请求来调用 API](#) 和 [AWS Organizations API 参考](#)。

对 AWS Organizations 的支持和反馈

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

其他 AWS 资源

- [AWS 培训和课程](#) – 指向基于角色的专业课程和自主进度动手实验室的链接，这些课程和实验室旨在帮助您增强 AWS 技能并获得实践经验。
- [AWS 开发人员工具](#) – 指向开发人员工具和资源的链接，其中提供了文档、代码示例、发行说明和有助于您利用 AWS 构建创新应用程序的其他信息。
- [AWS Support 中心](#) – 用于创建和管理 AWS Support 案例的中心。还包括指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况和 AWS Trusted Advisor。
- [AWS Support](#) – 提供有关 AWS Support 的信息的主要网页，是一种一对一的快速响应支持渠道，可帮助您在云中构建和运行应用程序。
- [联系我们](#) – 用于查询有关 AWS 账单、账户、事件、滥用和其他问题的中央联系点。
- [AWS 网站条款](#) – 有关我们的版权和商标、您的账户、许可、网站访问和其他主题的详细信息。

可与 AWS Organizations 一起使用的 AWS 服务

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

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

AWS 服务	与 AWS Organizations 一起使用的优势	
AWS Identity and Access Management – 帮助您安全地控制对 AWS 资源的访问权限。	您可在 IAM 中，使用 服务上次访问数据 帮助您更好地了解组织中的 AWS 活动。您可以使用此数据来创建和更新 服务控制策略 (SCP) (p. 54)，将访问限制在仅您的组织账户所使用的 AWS 服务。 有关示例，请参阅 IAM 用户指南中的 使用数据来细化组织部门的权限 。	
AWS Artifact – 使您能够下载 AWS 安全合规性报告，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。 要与 AWS Organizations 一起使用，请参阅 AWS Artifact 和 AWS Organizations (p. 80)。	

AWS 服务	与 AWS Organizations 一起使用的优势	
AWS CloudTrail – 可帮助对您的账户进行监管、合规性检查、操作审核和风险审核。	<p>主账户中的用户可以创建组织跟踪，记录该组织中所有账户的所有事件。</p> <p>有关与 AWS Organizations 一起使用的信息，请参阅AWS CloudTrail 和 AWS Organizations (p. 80)。</p>	
Amazon CloudWatch Events – 实时监控您的 AWS 资源以及您在 AWS 中运行的应用程序。	<p>您可以在组织中的所有账户之间启用所有 CloudWatch Events 的共享。</p> <p>有关更多信息，请参阅 Amazon CloudWatch Events 用户指南中的在 AWS 账户之间发送和接收事件。</p>	
AWS Config – 可让您访问、审核和评估您的 AWS 资源的配置。	<p>您可以在组织范围内查看合规性状态。您还可以使用 AWS Config API 在组织中跨所有 AWS 账户来管理 AWS Config 规则。</p> <p>有关与 AWS Organizations 一起使用的信息，请参阅AWS Config 和 AWS Organizations (p. 80)。</p>	
AWS Control Tower – 可帮助您设置和管理安全、合规的多账户 AWS 环境。	<p>您可以使用 Control Tower 设置登录区（适用于您所有 AWS 资源的多账户环境）。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 AWS 账户实施合规性监管。</p> <p>有关更多信息，请参阅 AWS Control Tower 用户指南中的AWS Control Tower 的工作原理和通过 AWS Organizations 管理账户。</p>	
AWS Directory Service – 可让您轻松地在 AWS 云中设置和运行目录，也可以将 AWS 资源与现有本地 Microsoft Active Directory 连接。	<p>将 AWS Directory Service 与 AWS Organizations 集成可实现跨一个区域中的多个账户和任何 VPC 的无缝目录共享。</p> <p>有关与 AWS Organizations 一起使用的信息，请参阅AWS Directory Service 和 AWS Organizations (p. 81)。</p>	

AWS 服务	与 AWS Organizations 一起使用的优势	
AWS Firewall Manager – 跨账户和应用程序集中配置和管理 Web 应用程序防火墙规则。	<p>您可以在组织中跨跨户集中配置和管理 AWS WAF 规则。</p> <p>有关与 AWS Organizations 一起使用的信息，请参阅AWS Firewall Manager 和 AWS Organizations (p. 81)。</p>	
AWS License Manager – 简化将软件许可证迁移到云中的过程。	<p>您可以在整个组织中启用计算资源的跨账户发现。</p> <p>有关与 AWS Organizations 一起使用的信息，请参阅AWS License Manager 和 AWS Organizations (p. 82)。</p>	
AWS RAM – 可让您与其他账户共享您指定的 AWS 资源。	<p>您可以在组织内共享资源，而无需交换其他邀请。</p> <p>您可以共享资源的包括 Route 53 解析程序规则、按需容量预留等。有关共享预留容量的信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例） 或 Amazon EC2 用户指南（适用于 Windows 实例）。有关可共享资源的列表，请参阅 AWS RAM 用户指南 中的 可共享资源。</p> <p>有关与 AWS Organizations 一起使用的信息，请参阅AWS RAM 和 AWS Organizations (p. 82)。</p>	
AWS Service Catalog – 可让您创建和管理获准在 AWS 上使用的 IT 服务的目录。	<p>您可以更轻松地跨账户共享产品组合和复制产品，而无需共享产品组合 ID。</p> <p>有关与 AWS Organizations 一起使用的信息，请参阅AWS Service Catalog 和 AWS Organizations (p. 82)。</p>	
Service Quotas – 使您能够从中央位置查看和管理您的服务配额（也称为限制）。	<p>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。</p> <p>有关与 AWS Organizations 一起使用的信息，请参阅Service Quotas 和 AWS Organizations (p. 83)。</p>	

AWS 服务	与 AWS Organizations 一起使用的优势	
AWS Single Sign-On – 为您的所有账户和云应用程序提供单一登录服务。	<p>无论账户是主账户还是成员账户，用户都可以使用其公司凭证登录 AWS SSO 用户门户并访问其分配的账户中的资源。</p> <p>有关与 AWS Organizations 一起使用的信息，请参阅AWS Single Sign-On 和 AWS Organizations (p. 83)。</p>	

有关启用对 AWS Organizations 的可信访问的更多信息，请参阅[启用其他 AWS 服务的可信访问](#) (p. 77)。

AWS Organizations 入门

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

了解...

[AWS Organizations 术语和概念 \(p. 7\)](#)

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

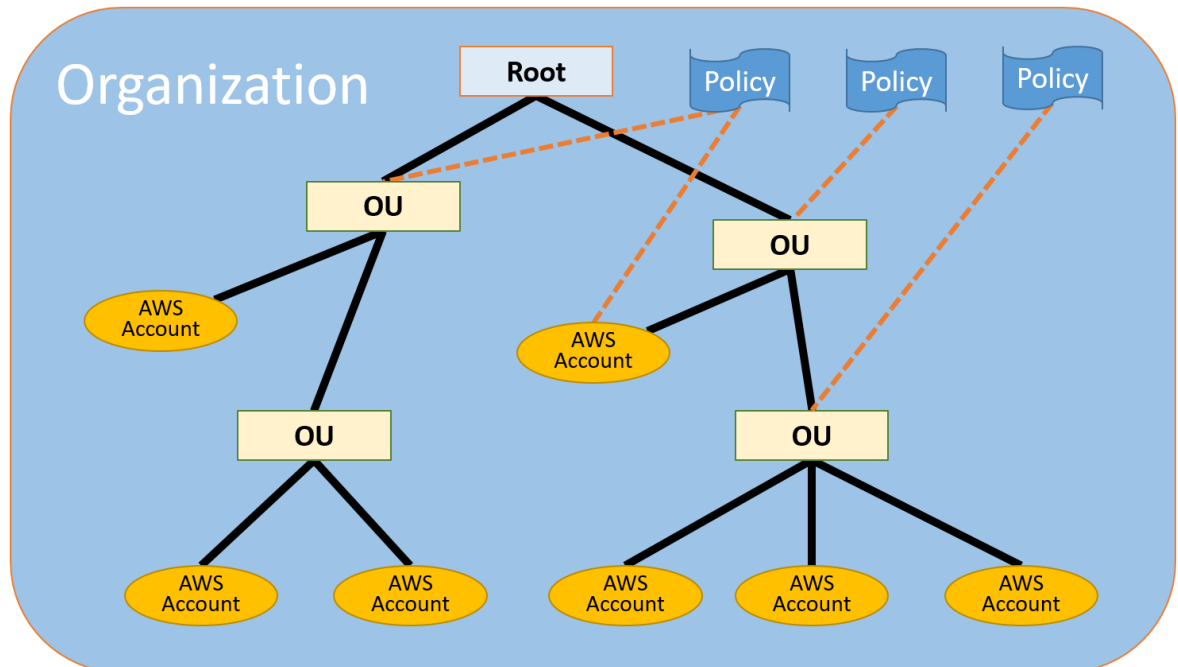
[组织的整合账单](#)

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

AWS Organizations 术语和概念

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

下图显示了一个包含七个账户的基本组织，这些账户在根下分为四个组织部门 (OU)。此外，该组织还有一些策略附加到其中部分 OU 或者直接附加到账户。有关这些项目中每一项的描述，请参阅本主题中的定义。



组织

您创建用于整合您的 AWS [账户 \(p. 8\)](#) 的实体。您可以使用 [AWS Organizations 控制台](#) 集中查看和管理组织内您的所有账户。一个组织有一个主账户以及零个或多个成员账户。您可以以分层树状结构组

织账户，将[根 \(p. 8\)](#)放在树顶部，[组织部门 \(p. 8\)](#)嵌套在根下。每个账户都可以直接放在根中，也可以放在层次结构的其中一个 OU 中。一个组织的功能由您启用的[功能集 \(p. 8\)](#)决定。

Root

您的组织的所有账户的父容器。如果您将一个策略附加到根，则它应用于组织中的所有[组织部门 \(OU\) \(p. 8\)](#)和[账户 \(p. 8\)](#)。

Note

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

组织部门 (OU)

[根 \(p. 8\)](#)中[账户 \(p. 8\)](#)的容器。OU 还可以包含其他 OU，这使您能够创建类似于倒置树的层次结构，根位于顶部，OU 分支向下延伸，结束于作为树叶的账户。当您策略附加到层次结构中的一个节点时，策略会向下流动，影响该节点下的所有分支 (OU) 和树叶 (账户)。一个 OU 有且仅有一个父级，而目前每个账户都正好是一个 OU 的成员。

账户

包含您的 AWS 资源的标准 AWS 账户。您可以将策略附加到账户，以仅对这个账户进行控制。

组织中有两种类型的账户：一个指定为主账户的单个账户，以及成员账户。

- 主账户是创建组织的账户。从组织的主账户中，您可以执行以下操作：
 - 在组织中创建账户
 - 邀请其他现有账户到组织中
 - 从组织中删除账户
 - 管理邀请
 - 将策略应用到组织内的实体（根、OU 或者账户）

主账户具有付款人账户的责任，并负责支付成员账户产生的所有费用。

- 属于组织的其他账户称为成员账户。一个账户一次只能是一个组织的成员。

邀请

邀请其他[账户 \(p. 8\)](#)加入您的[组织 \(p. 7\)](#)的过程。邀请可以仅由组织的主账户发出，并且可以扩展到与受邀账户相关联的账户 ID 或电子邮件地址。受邀账户接受邀请后，它将成为组织中的成员账户。如果组织需要所有当前成员账户批准将仅支持[整合账单 \(p. 8\)](#)功能更改为支持组织中的[所有功能 \(p. 8\)](#)，也可以将邀请发送到所有成员。通过交换[握手 \(p. 8\)](#)信息，对各个账户发出邀请。当您在 AWS Organizations 控制台中工作时，虽然您可能不会看到握手信息，但如果您使用 AWS CLI 或 AWS Organizations API，则必须直接处理握手。

握手

在双方之间交换信息的多步骤过程。它在 AWS Organizations 中的一项主要用途就是作为[邀请 \(p. 8\)](#)的底层实施。握手消息在握手发起方和接收方之间传递并由双方进行响应，使得握手消息可确保双方总是知道当前状态是什么。将组织从仅支持[整合账单 \(p. 8\)](#)功能更改为支持 AWS Organizations 提供的[所有功能 \(p. 8\)](#)时，也可以使用握手。仅当您使用 AWS Organizations API 或命令行工具（如 AWS CLI）时，您通常需要直接与握手交互。

可用的功能集

- 所有功能 – AWS Organizations 可用的默认功能集。它包括整合账单的所有功能，此外还包括高级功能，可让您更好地控制组织中的账户。例如，当启用了所有功能时，组织的主账户将能够完全控制成员账户可以执行的操作。主账户可以应用[SCP \(p. 54\)](#)来限制账户中的用户（包括根用户）和角色可以访问的服务和操作，并且可以防止成员账户离开组织。您可以创建一个已启用所有功能的组织，或者您可以启用最初仅支持整合账单功能的组织中的所有功能。要启用所有功能，所有受邀成员账户都必须批准更改，方法为接受当主账户启动此过程时发送的邀请。

整合账单 – 此功能集提供共享账单功能，但不包括 AWS Organizations 的更高级功能，如使用策略限制不同账户中的用户和角色可以执行的操作。要使用高级 AWS Organizations 功能，您必须启用组织中的[所有功能 \(p. 8\)](#)。

服务控制策略 (SCP)

一个策略，用于指定 [SCP \(p. 54\)](#) 所影响账户中的用户和角色可以使用的服务和操作。SCP 类似于 IAM 权限策略，不同的是前者不授予任何权限。相反，SCP 指定组织、组织单位 (OU) 或账户的最大权限数。在将 SCP 附加到组织根或 OU 时，SCP 限制成员账户中实体的权限。即使已使用 IAM 权限策略向用户授予完整管理员权限，影响该账户的 SCP 未明确允许或已明确拒绝的任何访问也将被阻止。例如，如果您分配一个仅允许数据库服务访问您的“数据库”账户的 SCP，则该账户中的任何用户、组或角色都被拒绝访问任何其他服务的操作。仅当您启用您组织中的[所有功能 \(p. 8\)](#)时，SCP 才可用。您可以将 SCP 附加到以下内容：

- 根，它影响组织中的所有账户
- OU，它影响自身的所有账户及其子树中任何 OU 的所有账户
- 单个账户

Important

组织的主账户不受附加到它的任何 SCP 的影响，也不受附加到主账户可能位于其中的任何根或 OU 的任何 SCP 的影响。

允许列表与拒绝列表

允许列表和拒绝列表是您应用 [SCP \(p. 54\)](#) 筛选可供账户使用的权限时的互补型技术。

- 允许列表（也称为“白名单”）– 您明确指定允许的访问权。隐式阻止所有其他访问权。默认情况下，AWS Organizations 将名为 FullAWSAccess 的 AWS 托管策略附加到所有根、OU 和账户。这样可以确保在您构建您的组织时，除非您希望，否则不会阻止任何内容。换句话说，默认情况下将允许所有权限。当您准备限制权限时，您需要将 FullAWSAccess 策略替换为仅允许限制性更强的所需权限集的策略。然后，受影响账户中的用户和角色只能使用该级别的访问权，即使其 IAM 策略允许所有操作也是如此。如果您在根上替换默认策略，则组织中的所有账户都受限制规则的影响。您不能在层次结构中的较低级别重新添加它们，因为 SCP 永远不会授予权限；它只筛选权限。
- 拒绝列表（也称为“黑名单”）– 您明确指定不允许的访问权。允许所有其他访问权。在这种情况下，除非明确阻止，否则允许所有权限。这是 AWS Organizations 的默认行为。默认情况下，AWS Organizations 将名为 FullAWSAccess 的 AWS 托管策略附加到所有根、OU 和账户。这样允许任何账户访问任何服务或操作，没有 AWS Organizations 施加的限制。与上文所述的允许列表方法不同，在使用拒绝列表时，您通常保留默认 FullAWSAccess 策略（允许“所有”），然后附加其他策略来显式拒绝访问不需要的服务和操作。与使用 IAM 权限策略一样，显式拒绝服务操作将覆盖该操作的任何允许规则。

AWS Organizations 教程

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

[教程：创建和配置组织 \(p. 10\)](#)

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

[教程：使用 CloudWatch Events 监控组织的重要更改 \(p. 16\)](#)

配置 Amazon CloudWatch Events，当组织中发生您指定的操作时，触发电子邮件、短信或日志条目形式的警报，监控组织中的重要更改。例如，许多组织希望了解何时创建了新账户，或账户何时尝试离开组织。

教程：创建和配置组织

在本教程中，您将创建组织并为其配置两个 AWS 成员账户。您可以在组织中创建其中一个成员账户，然后邀请另一个账户加入您的组织。接下来，您可以使用[允许列表 \(p. 9\)](#)方法指定账户管理员只能委派明确列出的服务和操作。这使得管理员可以先验证 AWS 引入的任何新服务，然后才允许由公司中的任何其他人员使用。这样，如果 AWS 引入新服务，它将保持被禁止的状态，直至管理员将该服务添加到相应策略的允许列表中。本教程还为您演示如何使用[拒绝列表 \(p. 9\)](#)来确保成员账户中的任何用户都无法更改 AWS CloudTrail 创建的审核日志的配置。

下图演示了本教程的主要步骤。



[步骤 1：创建组织 \(p. 11\)](#)

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

[步骤 2：创建组织单元 \(p. 12\)](#)

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

[步骤 3：创建服务控制策略 \(p. 13\)](#)

您可以应用限制，使用[服务控制策略 \(SCP\) \(p. 54\)](#)来限制可以将哪些操作委派给成员账户中的用户和角色。在此步骤中，您将创建两个 SCP 并将其附加到您组织中的 OU。

[步骤 4：测试组织的策略 \(p. 16\)](#)

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

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

先决条件

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

教程使用的账户如下：

- 111111111111 – 您用于创建组织的账户。此账户将成为主账户。此账户的所有者的电子邮件地址为 `masteraccount@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，使用该账户作为主账户创建组织，然后邀请现有账户 222222222222 作为成员账户加入。

1. 以账户 111111111111 的管理员身份登录 AWS，并通过 <https://console.aws.amazon.com/organizations/> 打开 AWS Organizations 控制台。
2. 在介绍页面上，选择 Create organization。
3. 在 Create organization 确认对话框中，选择 Create organization。

Note

默认情况下，组织在创建时已启用所有功能。您也可以创建自己的组织并仅启用[整合账单功能 \(p. 8\)](#)。

组织已创建。您此时在账户 (Accounts) 选项卡上。账户电子邮件旁边的星号指示这是主账户。

验证电子邮件自动发送至您的主账户关联的地址。在您接收到验证电子邮件之前可能会有一段延迟。

4. 在 24 小时内验证您的电子邮件地址。有关更多信息，请参阅 [电子邮件地址验证 \(p. 23\)](#)。

您现在拥有一个组织，并且您的账户是其唯一成员。这是组织的主账户。

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。

邀请现有账户加入

1. Open the 组织 console at <https://console.aws.amazon.com/organizations/>.
2. 选择 Accounts 选项卡。账户名称旁边的星号指示这是主账户。

现在，您可以邀请其他账户作为成员账户加入。

3. 在 Accounts (账户) 选项卡上，选择 Add account (添加账户)，然后选择 Invite account (邀请账户)。
4. 在 Account ID or email (账户 ID 或电子邮件) 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`。
5. 在 Notes (备注) 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。
6. 选择 Invite (邀请)。AWS Organizations 向账户所有者发送邀请。

Important

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

7. 对于本教程，您现在需要接受自己的邀请。执行以下操作之一可在控制台中打开 Invitations 页面：
 - 打开 AWS 从主账户发出的电子邮件，并选择链接以接受邀请。在系统提示登录时，以受邀成员账户的管理员身份执行操作。
 - 打开 AWS Organizations 控制台 (<https://console.aws.amazon.com/organizations/>) 并以成员账户的管理员身份登录。选择 Invitations。链接旁的数字指示此账户有多少个邀请。
8. 在 Invitations (邀请) 页面上，选择 Accept (接受)，然后选择 Confirm (确认)。
9. 注销成员账户，然后以主账户管理员的身份登录。

创建成员账户

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

创建成员账户

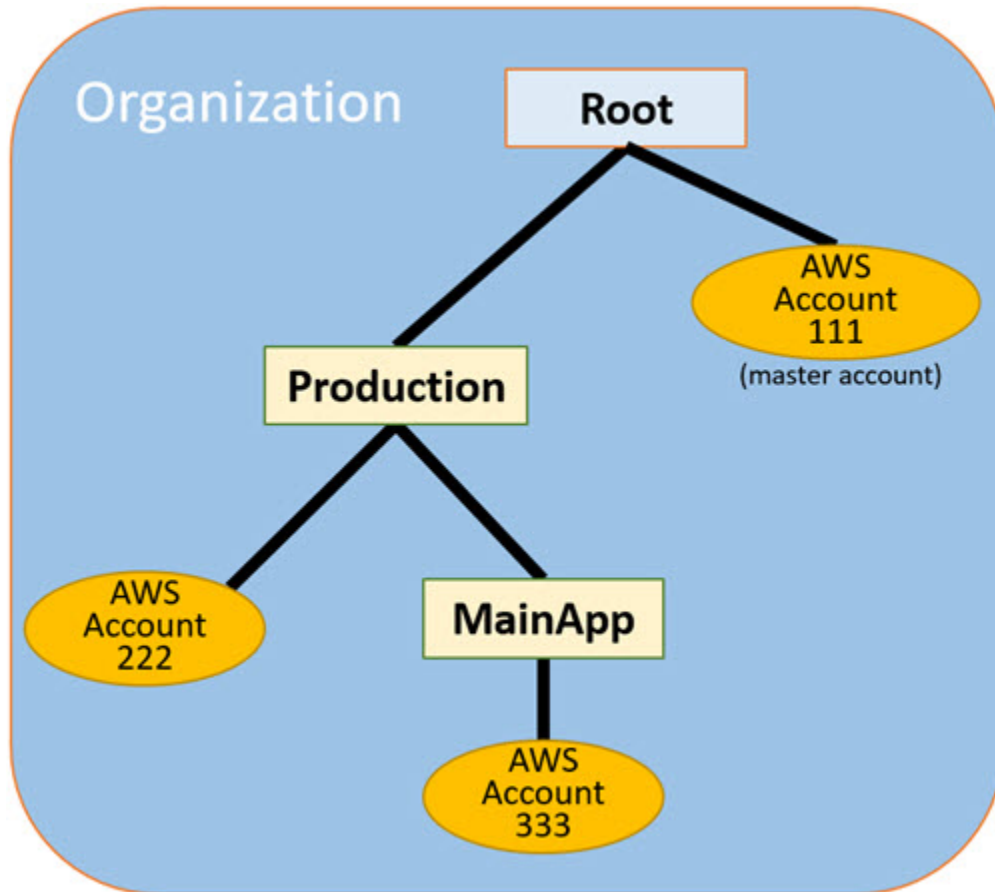
1. 在 AWS Organizations 控制台的 Accounts (账户) 选项卡上，选择 Add account (添加账户)。
2. 对于 Full name (全名)，输入账户的名称，例如 **MainApp Account**。
3. 对于 Email (电子邮件)，输入代表账户接收通信的人员的电子邮件地址。此值必须全局唯一。任何两个账户不能具有相同的电子邮件地址。例如，您可能会使用类似于 **mainapp@example.com** 的内容。
4. 对于 IAM role name，您可以将此处留空以自动使用 OrganizationAccountAccessRole 的默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

Important

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

步骤 2：创建组织单元

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



创建和填充 OU

1. 在 AWS Organizations 控制台上，选择 Organize Accounts (组织账户) 选项卡，然后选择 + New organizational unit (新建组织部门)。
2. 对于 OU 的名称，输入 **Production**，然后选择 Create organizational unit (创建组织部门)。
3. 选择您的新 Production (生产) OU 以导航到它，然后选择 + New organizational unit (新建组织部门)。
4. 对于第二个 OU 的名称，输入 **MainApp**，然后选择 Create organizational unit (创建组织部门)。

现在，您可以将成员账户移动到这些 OU 中。

5. 在左侧的树状图中，选择 Root。
6. 选择第一个成员账户 222222222222，然后选择 Move (移动)。
7. 在 Move accounts (移动账户) 对话框中，选择 Production (生产)，然后选择 Move (移动)。
8. 选择第二个成员账户 333333333333，然后选择 Move (移动)。
9. 在 Move accounts (移动账户) 对话框中，选择 Production (生产) 以公开 MainApp。选择 MainApp，然后选择 Move (移动)。

步骤 3：创建服务控制策略

在本部分的步骤中，您将创建三个服务控制策略 (SCP) (p. 54) 并将其附加到根和 OU，用于限制组织账户中的用户所能执行的操作。第一个 SCP 防止任何成员账户中的任何人创建或修改您配置的任何 AWS CloudTrail 日志。主账户不受任何 SCP 的影响，因此在应用 CloudTrail SCP 之后，您必须从主账户创建任何日志。

创建阻止 CloudTrail 配置操作的第一个 SCP

1. 选择 Policies (策略) 选项卡，然后选择 Create policy (创建策略)。
2. 对于 Policy name (策略名称)，输入 **Block CloudTrail Configuration Actions**。
3. 在左侧的 Policy (策略) 部分中，选择服务的 CloudTrail。然后选择以下操作：AddTags、CreateTrail、DeleteTrail、RemoveTags、StartLogging、StopLogging 和 UpdateTrail。
4. 在左侧窗格中，选择添加资源并指定 CloudTrail 和所有资源。选择添加资源。

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

5. 选择 Create policy (创建策略)。

第二条策略定义一个[允许列表 \(p. 9\)](#)，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。

创建第二条策略，将允许生产 OU 的已批准服务

1. 从策略列表中，选择 Create policy (创建策略)。
2. 对于 Policy Name (策略名称)，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 Create policy (创建策略)。

最后一条策略提供了阻止在 MainApp OU 中使用的服务的[拒绝列表](#) (p. 9)。对于本教程，您需要阻止 MainApp OU 中的任何账户访问 Amazon DynamoDB。

创建第三条策略，将拒绝访问不能在 MainApp OU 中使用的服务

1. 在 Policies (策略) 选项卡上，选择 Create Policy (创建策略)。
2. 对于 Policy Name (策略名称)，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，选择添加资源并指定 DynamoDB 和所有资源。选择添加资源。

右侧的策略语句将更新为与以下内容类似的内容。

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

5. 选择 Create policy (创建策略) 保存 SCP。

在根中启用服务控制策略类型

您必须先为根启用策略类型，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，任何根中都未启用策略类型。本部分的步骤将向您演示如何为组织中的根启用服务控制策略 (SCP) 类型。

Note

目前，您的组织中只能有一个根。此根是在您创建组织时为您创建的，并命名为 Root。

为您的根启用 SCP

1. 在 Organize accounts (组织账户) 选项卡上，选择您的根。
2. 在右侧 Details (详细信息) 窗格中的 ENABLE/DISABLE POLICY TYPES (启用/禁用策略类型) 下 (Service control policies (服务控制策略) 旁边)，选择 Enable (启用)。

将 SCP 附加到您的 OU

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

将策略附加到根和 OU

1. 仍在 Organize accounts (组织账户) 选项卡上右侧的 Details (详细信息) 窗格中，在 POLICIES (策略) 下选择 SERVICE CONTROL POLICIES (服务控制策略)。
2. 选择名为 Block CloudTrail Configuration Actions 的 SCP 旁边的 Attach (附加)，阻止任何人变更 CloudTrail 的配置方式。在本教程中，您会将其附加到根，这样它会影响所有成员账户。

此时将显示 Details (详细信息) 窗格，其中突出显示了两个附加到根的 SCP：您刚刚创建的一个以及默认的 FullAWSAccess SCP。

3. 选择 Production (生产) OU (不是复选框) 可导航到其内容。
4. 选择 POLICIES (策略) 下的 SERVICE CONTROL POLICIES (服务控制策略)，然后选择 Allow List for All Approved Services 旁的 Attach (附加)，允许生产 OU 中成员账户中的用户或角色访问批准的服务。
5. 现在，信息窗格显示有两个 SCP 附加到了 OU：您刚刚附加的一个以及默认的 FullAWSAccess SCP。但是，由于 FullAWSAccess SCP 同时也是允许所有服务和操作的允许列表，您必须分离此 SCP 以确保只允许您批准的服务。
6. 要从 Production OU 中删除默认策略，请选择 FullAWSAccess 旁的 Detach。删除此默认策略之后，根下的所有成员账户都将立即失去对不在允许列表 SCP (您已在前一步中附加) 中的所有操作和服务的访问权。任何使用未包含在所有批准服务的允许列表 SCP 中的操作的请求都将被拒绝。即使账户中的管理员通过将 IAM 权限策略附加到其中一个成员账户中的用户来授予对其他服务的访问权限，情况依然如此。
7. 现在，您可以附加名为 Deny List for MainApp Prohibited services 的 SCP，以防止 MainApp OU 的账户中的任何人使用任何受限制服务。

要实现此目的，请选择 MainApp OU (不是复选框)，导航到其内容。

8. 在 Details (详细信息) 窗格中的 POLICIES (策略) 下，展开 Service control policies (服务控制策略) 部分。在可用策略列表中的 Deny List for MainApp Prohibited Services (MainApp 禁止的服务的拒绝列表) 旁，选择 Attach (附加)。

步骤 4：测试组织的策略

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

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

教程：使用 CloudWatch Events 监控组织的重要更改

本教程介绍如何配置 CloudWatch Events，以监控对组织进行的更改。首先，学会配置一条规则，当用户调用特定 AWS Organizations 操作时即触发该规则。然后，您可将 CloudWatch Events 配置为触发规则后运行 AWS Lambda 函数，并将 Amazon SNS 配置为发送一封电子邮件，其中包含有关该事件的详细信息。

下图演示了本教程的主要步骤。



步骤 1：配置跟踪和事件选择器 (p. 18)

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

步骤 2：配置 Lambda 函数 (p. 18)

创建 AWS Lambda 函数，将事件的详细信息记录到 S3 存储桶中。

步骤 3：创建向订阅者发送电子邮件的 Amazon SNS 主题 (p. 19)

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

步骤 4：创建 CloudWatch Events 规则 (p. 19)

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

步骤 5：测试您的 CloudWatch Events 规则 (p. 20)

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。有关将 AWS CloudTrail 和 CloudWatch Events 与 AWS Organizations 配合使用的更多信息，请参阅 [AWS Organizations 中的日志记录和监控](#) (p. 89)。

先决条件

本教程假定：

- 您可以从组织的主账户中以 IAM 用户的身份登录 AWS 管理控制台。IAM 用户必须有权在 CloudTrail 中创建和配置日志，在 Lambda 中创建和配置函数，在 Amazon SNS 中创建和配置主题以及在 CloudWatch 中创建和配置规则。有关授予权限的更多信息，请参阅 IAM 用户指南中的 [访问管理](#)，或参阅要配置访问权限的服务的指南。
- 您可以访问现有的 Amazon Simple Storage Service (Amazon S3) 存储桶（或有权创建存储桶），用于接收在第一步配置的 CloudTrail 日志。

Important

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

步骤 1：配置跟踪和事件选择器

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

创建跟踪

1. 以组织主账户的管理员身份登录 AWS，然后通过 <https://console.aws.amazon.com/cloudtrail/> 打开 CloudTrail 控制台。
2. 在控制台右上角的导航栏中，选择 美国东部（弗吉尼亚北部）区域。如果您选择其他区域，AWS Organizations 不会在 CloudWatch Events 配置设置中作为一个选项出现，CloudTrail 也不会捕获 AWS Organizations 的相关信息。
3. 在导航窗格中，选择 Trails。
4. 选择 Create trail (创建跟踪)。
5. 对于 Trail name (跟踪名称)，输入 **My-Test-Trail**。
6. 执行下列选项之一来指定 CloudTrail 将日志提交到的位置：
 - 如果您已有一个存储桶，选择 Create a new S3 bucket (创建新 S3 存储桶) 旁边的 No (否)，然后从 S3 bucket (S3 存储桶) 列表中选择存储桶名称。
 - 如果您需要创建存储桶，请选择 Create a new S3 bucket (创建新 S3 存储桶) 旁边的 Yes (是)，然后在 S3 bucket (S3 存储桶) 中输入新存储桶的名称。

Note

S3 存储桶的名称必须是全球唯一的。

7. 选择 Create。
8. 选择您刚刚创建的 My-Test-Trail 跟踪。
9. 选择 Management events 旁边的铅笔图标。
10. 对于 Read/Write events，依次选择 All、Save、Configure。

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

步骤 2：配置 Lambda 函数

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

创建记录 CloudWatch Events 事件的 Lambda 函数

1. 从 <https://console.aws.amazon.com/lambda/> 打开 AWS Lambda 控制台。
2. 如果您是首次使用 Lambda，请在欢迎页面上选择 Get Started Now (立即开始使用)；否则，选择 Create a function (创建函数)。
3. 在 Create function (创建函数) 页面上，选择 Blueprints (蓝图)。
4. 从 Blueprints (蓝图) 搜索框中，为筛选条件输入 **hello**，然后选择 hello-world 蓝图。

5. 选择 Configure (配置)。
6. 在 Basic information (基本信息) 页面上，执行以下操作：
 - a. 对于 Lambda 函数名称，在 Name (名称) 文本框中输入 **LogOrganizationEvents**。
 - b. 对于 Role (角色)，选择 Create a custom role (创建自定义角色)，然后在 AWS Lambda requires access to your resources (AWS Lambda 需要访问您的资源) 页面底部，选择 Allow (允许)。此角色授予您的 Lambda 函数访问所需数据的权限和写入输出日志的权限。
 - c. 选择 Create function (创建函数)。
7. 在下一页上，编辑 Lambda 函数的代码，如以下示例所示：

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

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

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

8. 选择 Save (保存)。

步骤 3：创建向订阅者发送电子邮件的 Amazon SNS 主题

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

创建可向订阅者发送电子邮件的 Amazon SNS 主题

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

步骤 4：创建 CloudWatch Events 规则

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

创建 CloudWatch Events 规则

1. 从 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Rules (规则)，然后选择 Create rule (创建规则)。
3. 对于 Event source (事件源)，执行以下操作：
 - a. 选择 Event pattern。
 - b. 选择 Build event pattern to match events by service。
 - c. 对于 Service Name，选择 Organizations。
 - d. 对于 Event Type (事件类型)，选择 AWS API Call via CloudTrail (通过 CloudTrail 进行的 AWS API 调用)。
 - e. 选择 Specific operation(s) (特定操作)，然后输入您希望监控的 API：CreateAccount 和 CreateOrganizationalUnit。您还可以选择所需的任何其他内容。有关可用 AWS Organizations API 的完整列表，请参阅 [AWS Organizations API 参考](#)。
4. 在 Targets (目标) 下，对于 Function (函数)，选择您在上一过程中创建的函数。
5. 在 Targets (目标) 下，选择 Add target (添加目标)。
6. 在新目标行中，选择下拉标题，然后选择 SNS topic (SNS 主题)。
7. 对于 Topic (主题)，选择您在上一过程中创建的名为 OrganizationCloudWatchTopic 的主题。
8. 选择 Configure details (配置详细信息)。
9. 在 Configure rule details (配置规则详细信息) 页面上，对于 Name (名称)，输入 **OrgsMonitorRule**，将 State (状态) 保持选中状态，然后选择 Create rule (创建规则)。

步骤 5：测试您的 CloudWatch Events 规则

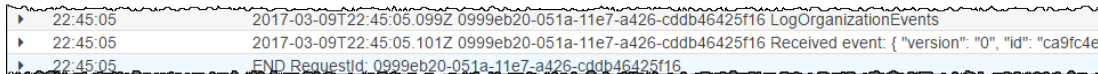
在此步骤中，您将创建一个组织部门 (OU)，然后观察 CloudWatch Events 规则生成日志条目，并向您发送有关事件详细信息的电子邮件。

创建 OU

1. 从 <https://console.aws.amazon.com/organizations/> 打开 AWS Organizations 控制台。
2. 选择 Organize accounts (组织账户) 选项卡，然后选择 New organizational unit (新建组织部门)。
3. 对于 OU 的名称，输入 **TestCWEOU**，然后选择 Create organizational unit (创建组织部门)。

查看 CloudWatch Events 日志条目

1. 从 <https://console.aws.amazon.com/cloudwatch/> 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Logs (日志)。
3. 在 Log Groups (日志组) 下，选择与您的 Lambda 函数关联的组：/aws/lambda/LogOrganizationEvents。
4. 每个组包含一个或多个流，应该有一个今天的组。选择这个组。
5. 查看日志。您应该可以看到与以下内容类似的行：



The screenshot shows a log stream with three entries. The first entry is a timestamp '22:45:05' followed by a long alphanumeric string and the text 'LogOrganizationEvents'. The second entry is a timestamp '22:45:05' followed by the same alphanumeric string and the text 'Received event: { "version": "0", "id": "ca9fc4e' (truncated). The third entry is a timestamp '22:45:05' followed by the text 'END RequestId: 0999eb20-051a-11e7-a426-cddb46425f16'.

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::123456789012:ou/o-exampleOrgId/ou-exampleRootId-exampleOUId"
    }
  },
  "requestID": "123456-EXAMPLE-GUID-123456",
  "eventID": "123456-EXAMPLE-GUID-123456",
  "eventType": "AwsApiCall"
}
```

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

清理：删除您不再需要的资源

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

清理您的 AWS 环境

1. 使用 CloudTrail 控制台 (<https://console.aws.amazon.com/cloudtrail/>) 删除您通过步骤 1 创建的、名为 **My-Test-Trail** 的跟踪。
2. 如果您在步骤 1 中创建了 Amazon S3 存储桶，请使用 Amazon S3 控制台 (<https://console.aws.amazon.com/s3/>) 将其删除。
3. 使用 Lambda 控制台 (<https://console.aws.amazon.com/lambda/>) 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 (<https://console.aws.amazon.com/sns/>) 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 (<https://console.aws.amazon.com/cloudwatch/>) 删除您通过步骤 4 创建的、名为 **OrgsMonitorRule** 的 CloudWatch 规则。

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

创建和管理组织

您可以使用 AWS Organizations 控制台执行以下任务：

- [创建组织 \(p. 22\)](#)。使用您当前的账户作为主账户创建组织。在您的组织内创建成员账户，并邀请其他账户加入组织。
- [启用组织中的所有功能 \(p. 24\)](#)。启用所有功能是使用 AWS Organizations 的首选方式。在创建组织时，您可以选择启用用于整合账单的所有或部分功能。启用所有功能是默认选择，它包括整合账单功能。

在启用所有功能的情况下，您可以使用 AWS Organizations 中提供的高级账户管理功能，例如[服务控制策略 \(SCP\) \(p. 54\)](#)。SCP 提供对组织中所有账户的最大可用权限的集中控制，使您能够确保您的账户遵循组织的访问控制指南。

- [查看有关组织的详细信息 \(p. 27\)](#)。查看有关您的组织、根、组织单元 (OU) 和账户的详细信息。
- [删除组织 \(p. 30\)](#)。当您不再需要某个组织时删除它。

Note

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

创建组织

使用 AWS Organizations 创建自己的组织来整合和管理 AWS 账户。

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

Note

目前，您的组织中只能有一个根。

创建组织之后，您可以通过以下方式从主账户中向您的组织添加账户：

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

最小权限

要使用您当前的 AWS 账户创建组织，您必须具有以下权限：

- `organizations:CreateOrganization`

创建组织（控制台）

1. 通过以下网址登录 AWS 管理控制台并打开 AWS Organizations 控制台：<https://console.aws.amazon.com/organizations/>。您必须以 IAM 用户身份登录，代入 IAM 角色；或以要作为组织主账户的账户中的根用户身份登录（[不推荐](#)）。
2. 在介绍页面上，选择 Create organization。

3. 在 Create organization 确认对话框中，选择 Create organization。

Note

默认情况下，组织在创建时已启用所有功能。您也可以创建自己的组织并仅启用[整合账单功能 \(p. 8\)](#)。

组织已创建。您此时在账户 (Accounts) 选项卡上。账户电子邮件旁边的星号指示这是主账户。

验证电子邮件自动发送至您的主账户关联的地址。在您接收到验证电子邮件之前可能会有一段延迟。

4. 在 24 小时内验证您的电子邮件地址。有关更多信息，请参阅[电子邮件地址验证 \(p. 23\)](#)。
5. 向组织添加账户，如下所示：
 - 要创建自动属于 AWS 组织的 AWS 账户，请参阅[在组织中创建 AWS 账户 \(p. 35\)](#)。
 - 若要邀请现有账户加入您的组织，请参阅[邀请 AWS 账户加入组织 \(p. 32\)](#)。

Note

您可以在不验证主账户电子邮件地址的情况下向组织添加新账户。要邀请现有账户，您必须先验证电子邮件地址。

创建组织 (AWS CLI、AWS API)

您可以使用以下命令之一创建组织：

- AWS CLI：[aws organizations create-organization](#)
- AWS API：[CreateOrganization](#)

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主账户关联的电子邮件地址。

创建组织时，AWS 会自动向指定的电子邮件地址发送验证邮件。在您接收到验证电子邮件之前可能会有一段延迟。

在 24 小时内，按照电子邮件中的说明验证您的电子邮件地址。

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

- 要查看与您的主账户关联的电子邮件地址是什么，请参阅[从主账户查看组织的详细信息 \(p. 27\)](#)。
- 要更改与主账户关联的电子邮件地址，请参阅 AWS Billing and Cost Management 用户指南 中的[管理 AWS 账户](#)。

若要重新发送验证请求

1. 通过以下网址登录 AWS 管理控制台并打开 AWS Organizations 控制台：<https://console.aws.amazon.com/organizations/>。您必须以 IAM 用户身份登录，代入 IAM 角色；或以要作为组织主账户的账户中的根用户身份登录（[不推荐](#)）。
2. 选择“设置 (Settings)”选项卡，然后选择发送验证请求。
3. 在 24 小时内验证您的电子邮件地址。

验证您的电子邮件地址后，您可以邀请其他 AWS 账户加入您的组织。有关更多信息，请参阅[邀请 AWS 账户加入组织 \(p. 32\)](#)。

如果您更改主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。

启用组织中的所有功能

AWS Organizations 有两个可用的功能集：

- [所有功能 \(p. 8\)](#) – 此功能集是使用 AWS Organizations 的首选方式，并且它包括整合账单功能。在创建组织时，默认情况下将启用所有功能。在启用所有功能的情况下，您可以使用 AWS Organizations 中提供的高级账户管理功能，例如[服务控制策略 \(SCP\) \(p. 54\)](#)。SCP 提供对组织中所有账户的最大可用权限的集中控制，使您能够确保您的账户遵循组织的访问控制指南。
- [整合账单功能 \(p. 8\)](#) – 所有组织都支持此功能子集，这提供了可用于集中管理组织中的账户的基本管理工具。

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

在启用所有功能之前

在从仅支持整合账单功能的组织更改为支持所有功能的组织之前，请注意以下几点：

- 当您开始启用所有功能的流程时，AWS Organizations 会向您邀请 加入组织的每个成员账户发送请求。每个受邀账户必须通过接受请求来批准启用所有功能。只有这样，您才可以完成在组织中启用所有功能的流程。如果某个账户拒绝了请求，则您必须从组织中删除该账户，或者重新发送请求并让该账户接受请求，然后才能完成启用所有功能的过程。您使用 AWS Organizations 创建 的账户不会获取请求，因为这些账户无需批准额外控制。
- 组织还将验证每个账户是否都有一个名为 `AWSServiceRoleForOrganizations` 的服务相关角色。此角色在要启用所有功能的所有账户中都是必需的。如果您在受邀账户中删除了此角色，则接受“启用所有功能”邀请会重新创建此角色。如果您已删除使用 AWS Organizations 创建的账户中的此角色，则该账户会收到专门重新创建此角色的邀请。组织必须接受所有这些邀请才能完成启用所有功能的过程。
- 在启用所有功能的过程中，您可以继续在组织内创建 账户，但无法邀请 现有账户加入组织。要邀请账户，您必须等待，直到启用所有功能的过程完成。您也可以取消启用所有功能的过程，邀请账户，然后重新开始启用所有功能的过程。
- 由于启用所有功能可让您使用 [SCP \(p. 54\)](#)，因此，请确保账户管理员了解将 SCP 附加到组织、组织单位或账户的效果。SCP 可以限制用户甚至是管理员能够在受影响的账户中执行的操作。例如，主账户可以应用 SCP，防止成员账户退出组织。
- 主账户不受任何 SCP 的影响。您无法通过应用 SCP 来限制主账户中的用户和角色能够执行的操作。SCP 仅影响成员账户。
- 从整合账单功能迁移到所有功能的过程是单向的。您无法将已启用了所有功能的组织切换回仅启用整合账单功能。
- 如果您的组织仅启用了整合账单功能，则成员账户管理员可以选择删除名为 `AWSServiceRoleForOrganizations` 的服务相关角色。但是，当您在组织中启用所有功能时，此角色是必需的，并且将在所有账户中作为接受“启用所有功能”邀请的一部分重新创建。有关 AWS Organizations 如何使用此角色的更多信息，请参阅[AWS Organizations 和服务相关角色 \(p. 79\)](#)。

开始启用所有功能的流程

在以拥有组织主账户权限的身份登录后，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`

邀请您的成员账户同意在组织中启用所有功能

1. 通过以下网址登录 AWS 管理控制台并打开 AWS Organizations 控制台：<https://console.aws.amazon.com/organizations/>。您必须以 IAM 用户身份登录，代入 IAM 角色；或以组织主账户中的根用户身份登录（**不推荐**）。
2. 在 Settings 选项卡上，选择 Begin process to enable all features。
3. 确认您了解在通过选择 Begin process to enable all features (开始启用所有功能的流程) 切换之后，便无法再回到仅整合账单功能。AWS Organizations 将请求发送到组织中的每个受邀（而非已创建）账户，要求批准请求以在组织中启用所有功能。如果您有使用 AWS Organizations 创建的任何账户且成员账户管理员删除了名为 `AWSServiceRoleForOrganizations` 的服务相关角色，则 AWS Organizations 会向该账户发送重新创建该角色的请求。
4. 要查看请求的状态，请选择 View all feature request approval status。

All feature request approval status 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有绿色勾号并显示 Acceptance 日期。尚未同意的账户将显示有黄色感叹号图标以及发送请求的日期，请求状态为 Open (打开)。

Note

- 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。所有与此尝试相关的请求将被取消，您必须从步骤 2 从头开始。
 - 在您发出请求以启用所有功能之后，到所有账户接受或者出现超时的过程中，将自动取消其他账户等待接受的加入组织邀请。在启用所有功能的流程完成之前，您无法发出新邀请。
 - 完成启用所有功能的流程之后，您可以再次邀请账户加入组织。该流程没有变化，不过所有邀请中包括信息，让收件人知道接受邀请之后将对其应用所有适用策略。
5. 如果某个账户未批准其请求，则您可在该页面上选择该账户，然后选择 Remove (删除)。这可以取消选定账户的请求并从组织中删除该账户，避免妨碍到启用所有功能。
 6. 所有账户批准请求之后，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。只需在控制台中单击几次，即可完成该流程。请参阅[完成流程以启用所有功能](#) (p. 26)。

邀请受邀成员账户同意在组织中启用所有功能 (AWS CLI、AWS API)

可以使用以下命令之一在组织中启用所有功能：

- AWS CLI：[aws organizations enable-all-features](#)
- AWS API：[EnableAllFeatures](#)

批准启用所有功能或重新创建服务相关角色的请求

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

最小权限

要批准为成员账户启用所有功能的请求，您必须拥有以下权限：

- `organizations:AcceptHandshake`

- `iam:CreateServiceLinkedRole` – 仅当在成员账户中必须重新创建 `AWSServiceRoleForOrganizations` 角色时需要

Important

如果您执行以下过程中的步骤，则组织中的主账户可以在成员账户上应用基于策略的控制，限制用户甚至是作为管理员的您可以在账户中执行哪些操作。此外，主账户可以应用策略，防止您的账户退出组织。

同意在组织中启用所有功能的请求 (控制台)

1. 通过以下网址登录 AWS 管理控制台并打开 AWS Organizations 控制台：<https://console.aws.amazon.com/organizations/>。您必须以 IAM 用户身份登录，代入 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主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。

同意在组织中启用所有功能的请求 (AWS CLI、AWS API)

要同意请求，您必须使用 `"Action": "APPROVE_ALL_FEATURES"` 接受握手过程。

- AWS CLI：[aws organizations accept-handshake](#)
- AWS API：[AcceptHandshake](#)

完成流程以启用所有功能

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

最小权限

要完成为组织启用所有功能的流程，您必须拥有以下权限：

- `organizations:AcceptHandshake`

完成启用所有功能的流程 (控制台)

1. 通过以下网址登录 AWS 管理控制台并打开 AWS Organizations 控制台：<https://console.aws.amazon.com/organizations/>。您必须以 IAM 用户身份登录，代入 IAM 角色；或以组织主账户中的根用户身份登录（**不推荐**）。
2. 在 **Settings** 选项卡的 **ENABLE ALL FEATURES** 下，选择 **View all feature request approval status**。
3. 所有账户接受启用所有功能的请求之后，在页面顶部的绿色框中，选择 **Finalize process to enable all features** (完成启用所有功能的流程)，然后在确认对话框中再次选择 **Finalize process to enable all features** (完成启用所有功能的流程)。
4. 组织现已启用所有功能。下一步是启用您要使用的策略类型。有关更多信息，请参阅[在根上启用和禁用策略类型](#) (p. 51)。在此之后，您可以附加策略，管理组织中的账户。有关更多信息，请参阅[将策略附加到根、OU 或账户](#) (p. 52)。

完成流程以启用所有功能 (AWS CLI、AWS API)

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

- AWS CLI：[aws organizations accept-handshake](#)

- AWS API : [AcceptHandshake](#)

查看有关您的组织的详细信息

您可以使用 AWS Organizations 控制台执行以下任务：

- [从主账户查看组织的详细信息 \(p. 27\)](#)
- [查看根的详细信息 \(p. 27\)](#)
- [查看 OU 的详细信息 \(p. 28\)](#)
- [查看账户的详细信息 \(p. 28\)](#)
- [查看策略的详细信息 \(p. 29\)](#)

从主账户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`

查看组织的详细信息（控制台）

在 [AWS Organizations 控制台](#) 中登录组织的主账户时，您可以查看组织的详细信息。

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。
2. 选择 Settings 选项卡。

控制台中将显示组织的详细信息，包括其 ID、ARN 以及主账户所有者的电子邮件地址。

查看组织的详细信息（AWS CLI、AWS API）

您可以使用以下命令之一查看组织的详细信息：

- AWS CLI : [aws organizations describe-organization](#)
- AWS API : [DescribeOrganization](#)

查看根的详细信息

最小权限

要查看根的详细信息，您必须拥有以下权限：

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

查看根的详细信息（控制台）

在 [AWS Organizations 控制台](#) 中登录组织的主账户时，您可以查看根的详细信息。

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。
2. 选择 Organize accounts 选项卡，然后选择 Home。
3. 选择 Root 实体。Root 是默认名称，不过您可以使用 API 或命令行工具重命名。

页面右侧的 Root (根) 窗格显示根的详细信息。

查看根的详细信息 (AWS CLI、AWS API)

您可以使用以下命令之一查看根的详细信息：

- AWS CLI : [aws organizations list-roots](#)
- AWS API : [ListRoots](#)

查看 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` (仅限控制台)
- `organizations:ListOrganizationsUnitsForParent` (仅限控制台)
- `organizations:ListRoots` (仅限控制台)

查看 OU 的详细信息 (控制台)

在 [AWS Organizations 控制台](#) 中登录组织的主账户时，您可以查看组织中 OU 的详细信息。

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。
2. 在 Organize accounts 选项卡上，导航到要查看的 OU。如果您要查看的 OU 是其他 OU 的子级，则在层次结构中选择各个 OU 以查找您所要找的 OU。
3. 选中该 OU 的复选框。

页面右侧的详细信息窗格显示有关 OU 的信息。

查看 OU 的详细信息 (AWS CLI、AWS API)

您可以使用以下命令之一查看 OU 的详细信息：

- AWS CLI : [aws organizations describe-organizational-unit](#)
- AWS API : [DescribeOrganizationalUnit](#)

查看账户的详细信息

最小权限

要查看 AWS 账户的详细信息，您必须拥有以下权限：

- `organizations:DescribeAccount`

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

查看 AWS 账户的详细信息 (控制台)

在 [AWS Organizations 控制台](#) 中登录组织的主账户时，您可以查看有关账户的详细信息。

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录 ([不推荐](#))。
2. 执行以下任一操作：
 - 在 Accounts 选项卡上，选择要查看的账户。
 - 在 Organize accounts 选项卡上，导航到并选择某个账户卡。

页面右侧的 Account summary (账户摘要) 窗格显示所选账户的详细信息。

Note

默认情况下，Accounts 选项卡不显示失败的账户创建请求。您可以选择顶部的开关将其更改为 Show (显示)，以便在列表中包含此类请求。

查看账户的详细信息 (AWS CLI、AWS API)

您可以使用以下命令之一查看账户的详细信息：

- AWS CLI : [aws organizations describe-account](#)
- AWS API : [DescribeAccount](#)

查看策略的详细信息

最小权限

要查看策略的详细信息，您必须拥有以下权限：

- `organizations:DescribePolicy`
- `organizations:ListPolicies`

查看策略的详细信息 (控制台)

在 [AWS Organizations 控制台](#) 中登录组织的主账户时，您可以查看有关账户的详细信息。

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录 ([不推荐](#))。
2. 在 Policies (策略) 选项卡上，选择要检查的策略。
3. 在页面右侧的窗格中，选择 View policy details (查看策略详细信息)。

查看策略的详细信息 (AWS CLI、AWS API)

您可以使用以下命令之一查看策略的详细信息：

- AWS CLI : [aws organizations describe-policy](#)
- AWS API : [DescribePolicy](#)

移除主账户并删除组织

当您不再需要组织时，可将其删除。此操作会从组织中移除主账户，并删除组织本身。先前主账户将成为独立 AWS 账户。然后，您有三个选项：可以继续使用它作为独立账户、使用它创建不同的组织，也可以接受其他组织的邀请，将该账户作为成员账户添加到该组织。

Important

- 如果您删除组织，则将无法恢复它。如果您在组织内创建了任何策略，则也将删除它们。
- 必须先删除组织中的所有成员账户，然后才能删除组织。如果您使用 AWS Organizations 创建了一些成员账户，则可能无法删除这些账户。您只能删除拥有作为独立 AWS 账户运行所需的全部信息的成员账户。有关如何提供这些信息和删除账户的更多信息，请参阅[作为成员账户退出组织 \(p. 42\)](#)。

在通过删除组织来从组织中移除主账户时，该账户会在以下方面受到影响：

- 该账户只负责支付自己的费用，不再负责支付其他任何账户产生的费用。
- 与其他服务的集成可能会被禁用。例如，AWS Single Sign-On 需要组织才能运行，因此，如果您从支持 AWS SSO 的组织中移除账户，则此账户中的用户将无法再使用该服务。

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

从组织中移除主账户并删除组织 (控制台)

最小权限

要删除组织，您必须以主账户中的 IAM 用户或角色身份登录，并且您必须拥有以下权限：

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

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。
2. 您必须先移除组织中的所有账户，然后才能删除组织。有关更多信息，请参阅[从组织中删除成员账户 \(p. 40\)](#)。
3. 在 Settings 选项卡上，选择 Delete organization。
4. 在 Delete organization (删除组织) 确认对话框中，选择 Delete organization (删除组织)。
5. （可选）如果您还希望关闭此账户，则可以按照[关闭 AWS 账户 \(p. 43\)](#)中的步骤操作。

删除组织 (AWS CLI、AWS API)

您可以使用以下命令之一删除组织：

- AWS CLI：[aws organizations delete-organization](#)
- AWS API：[DeleteOrganization](#)

管理您组织中的 AWS 账户

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

- [查看您组织中账户的详细信息 \(p. 28\)](#)。您可以查看该账户的唯一 ID 号、其 Amazon 资源名称 (ARN) 以及向其附加的策略。
- [邀请现有 AWS 账户加入您的组织 \(p. 32\)](#)。创建邀请、管理您已创建的邀请以及接受或拒绝邀请。
- [创建 AWS 账户作为您组织的一部分 \(p. 35\)](#)。创建和访问自动成为您组织一部分的 AWS 账户。
- [从您的组织中删除 AWS 账户 \(p. 40\)](#)。作为主账户中的管理员，从组织中删除您不再希望管理的成员账户。作为成员账户的管理员，从其组织中删除您的账户。如果主账户已将一个策略附加到您的成员账户，则您可能无法删除您的账户。
- [删除 \(或关闭\) AWS 账户 \(p. 43\)](#)。您可以关闭不再使用的 AWS 账户，以免产生任何使用费或应计费用。

您邀请 AWS 账户加入组织后对该账户的影响

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

- AWS Organizations 将创建名为 [AWSServiceRoleForOrganizations \(p. 79\)](#) 的服务相关角色。如果您的组织支持所有功能，该账户必须具有此角色。如果组织仅支持整合账单功能集，您可以删除该角色。如果您删除该角色，然后在组织中启用所有功能，则 AWS Organizations 将为该账户重新创建该角色。
- 如果您在 [OU 树的根级别附加了服务控制策略 \(SCP\) \(p. 54\)](#)，则这些 SCP 将立即应用于受邀账户中的所有用户和角色。默认情况下，AWS Organizations 将新账户添加到根 OU。
- 如果为您的组织[启用了对其他 AWS 服务的服务信任 \(p. 79\)](#)，则该可信服务可以在组织中的任何成员账户 (包括受邀账户) 中创建服务相关角色或执行操作。

对于受邀成员账户，AWS Organizations 不会自动创建 IAM 角色

[OrganizationAccountAccessRole \(p. 39\)](#)。此角色授予主账户对成员账户的管理控制权。如果您希望启用该级别的管理控制权，可以手动将该角色添加到受邀账户。有关更多信息，请参阅[在受邀成员账户中创建 OrganizationAccountAccessRole \(p. 38\)](#)。

如果您邀请一个账户加入仅启用了整合账单功能的组织，但稍后希望为该组织启用所有功能，则受邀账户必须批准此更改。

您在组织中创建一个 AWS 账户对该账户的影响

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

- AWS Organizations 将创建名为 [AWSServiceRoleForOrganizations \(p. 79\)](#) 的服务相关角色。如果您的组织支持所有功能，该账户必须具有此角色。如果组织仅支持整合账单功能集，您可以删除该角色。如果您删除该角色，然后在组织中启用所有功能，则 AWS Organizations 将为该账户重新创建该角色。
- AWS Organizations 将创建 IAM 角色 [OrganizationAccountAccessRole \(p. 39\)](#)。此角色授予主账户对新成员账户的访问权限。可以删除此角色。
- 如果您在 [OU 树的根级别附加了 SCP \(p. 54\)](#)，这些 SCP 会立即应用于新建账户中的所有用户和角色。默认情况下，新账户会添加到根 OU。

- 如果您为组织启用了[对其他 AWS 服务的服务信任 \(p. 79\)](#)，则该可信服务可以在组织中的任何成员账户（包括您创建的账户）中创建服务相关角色或执行操作。

邀请 AWS 账户加入组织

在创建组织并验证您与主账户关联的电子邮件地址后，才能邀请现有 AWS 账户加入您的组织。

您邀请账户时，AWS Organizations 将向账户所有者发送邀请，该所有者确定接受还是拒绝邀请。您可以使用 AWS Organizations 控制台启动和管理您发送到其他账户的邀请。您只能从组织的主账户发送邀请到其他账户。

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

当某个受邀账户加入您的组织时，您不会自动拥有对该账户的完全管理员控制权限，这不同于已创建的账户。如果您希望主账户具有对受邀成员账户的完全管理控制权，您必须在成员账户中创建 `OrganizationAccountAccessRole` IAM 角色并将权限授予主账户以代入该角色。要进行此配置，请在受邀账户成为成员之后，按照[在受邀成员账户中创建 OrganizationAccountAccessRole \(p. 38\)](#)中的步骤操作。

Note

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

AWS Organizations 会在受邀成员账户中创建一个服务相关角色以支持 AWS Organizations 与其他 AWS 服务之间的集成。有关更多信息，请参阅[AWS Organizations 和服务相关角色 \(p. 79\)](#)。

每个组织每天最多可以发送 20 个邀请。已接受的邀请不计入此限制。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限制。如果受邀账户拒绝邀请、主账户取消邀请或邀请过期，则撤销此计数。

要创建自动属于组织的账户，请参阅[在组织中创建 AWS 账户 \(p. 35\)](#)。

Important

出于法律和账单限制，您只能邀请主账户所属的 AWS 销售商的 AWS 账户。您不得在同一组织内混用 AWS、Amazon Internet Services Pvt.Ltd (AISPL，印度的一家 AWS 销售商) 或亚马逊通信技术服务（北京）有限公司 (ACTS，中国的一家 AWS 销售商) 的账户。您只能将来自某个 AWS 销售商的账户添加到具有同一 AWS 销售商账户的组织。

向 AWS 账户发送邀请

若要邀请账户加入您的组织，必须首先验证您与主账户关联的电子邮件地址。验证电子邮件地址后，请完成以下步骤来邀请账户加入您的组织。

最小权限

要邀请 AWS 账户加入您的组织，您必须拥有以下权限：

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

邀请其他账户加入组织 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。
2. 如果您的电子邮件地址已完整验证，请跳过此步骤。

如果您的电子邮件地址还未验证，请在 24 小时内按照[验证电子邮件 \(p. 23\)](#)中的说明进行验证。在您接收到验证电子邮件之前可能会有一段延迟。在验证电子邮件地址前无法邀请账户。
3. 在 Accounts 选项卡上，选择 Add account。
4. 选择 Invite account。
5. 输入要邀请加入您的组织的 AWS 账户的电子邮件地址或账户 ID 号。如果您希望邀请多个账户，请使用逗号分隔。
6. （可选）对于 备注 (Notes)，输入您要包括在发送给其他账户所有者的电子邮件邀请中的任意消息。
7. 选择 Invite。

Important

如果您收到一条消息，它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，请联系 [AWS Support](#)。

8. 控制台会将您重定向到 Invitations 选项卡。在此查看所有待接受和已接受邀请。您刚刚创建的邀请将显示在列表的顶部，其状态设置为 OPEN。

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

对此账户的邀请立即计入组织的账户数量限制；AWS Organizations 不会等待账户接受邀请。如果受邀账户拒绝，则主账户会取消邀请。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限制。

邀请其他账户加入组织 (AWS CLI、AWS API)

您可以使用以下命令之一来邀请其他账户加入您的组织：

- AWS CLI：[aws organizations invite-account-to-organization](#)
- AWS API：[InviteAccountToOrganization](#)

管理组织的待处理邀请

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

最小权限

要管理组织的待处理邀请，您必须拥有以下权限：

- `organizations:DescribeOrganization` (仅限控制台)
- `organizations:ListHandshakesForOrganization`
- `organizations:CancelHandshake`

查看或取消从您的组织发送到其他账户的邀请 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。

2. 选择 **Invitations** 选项卡。此处列出从您的组织发送的所有邀请及其当前状态。

Note

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

3. 对于任何您要取消的待接受邀请，请在 **Actions** 列下选择 **Cancel**。

邀请的状态将从 **Open** 更改为 **Canceled**。

AWS 会发送电子邮件到账户所有者，说明您已取消邀请。除非您发送新邀请，否则账户无法再加入组织。

查看或取消从您的组织发送到其他账户的邀请 (AWS CLI、AWS API)

您可以使用以下命令来查看或取消邀请：

- AWS CLI：[aws organizations list-handshakes-for-organization](#)、[aws organizations cancel-handshake](#)
- AWS API：[ListHandshakesForOrganization](#)、[CancelHandshake](#)

接受或拒绝来自组织的邀请

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

最小权限

要接受或拒绝加入 AWS 组织的邀请，您必须拥有以下权限：

- `organizations:ListHandshakesForAccount` – 在 AWS Organizations 控制台中查看邀请列表时需要。
- `organizations:AcceptHandshake`。
- `organizations:DeclineHandshake`。
- `iam:CreateServiceLinkedRole` – 仅在接受邀请需要创建服务相关角色以支持与其他 AWS 服务的集成时需要。有关更多信息，请参阅[AWS Organizations 和服务相关角色](#) (p. 79)。

Note

组织的账户状态影响可见的成本和使用率数据：

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

接受或拒绝邀请 (控制台)

1. 加入组织的邀请发送到账户所有者电子邮件地址。如果您是账户所有者并且收到了邀请电子邮件，请按照电子邮件邀请中的说明操作或者在浏览器中转到 <https://console.aws.amazon.com/organizations/>，然后选择 **Respond to invitations** (响应邀请)。
2. 根据提示以 IAM 用户身份登录受邀账户，代入 IAM 角色；或以该账户的根用户身份登录 (**不推荐**)。

3. 在控制台中的 **Invitations** 页上，您可以看到加入组织的待接受邀请。根据需要选择 **Accept** (接受) 或 **Decline** (觉)。
- 如果在上一步中选择了 **Accept**，则请在 **Confirm joining the organization** 确认窗口中选择 **Confirm**。

控制台会将您重定向到 **Organization overview** 页面，其中提供了有关您账户现在所属的组织的详细信息。您可以查看组织的 ID 和所有者的电子邮件地址。

Note

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

AWS Organizations 会在新的成员账户中创建一个服务相关角色以支持 AWS Organizations 与其他 AWS 服务之间的集成。有关更多信息，请参阅[AWS Organizations 和服务相关角色 \(p. 79\)](#)。

AWS 将发送电子邮件到组织主账户的所有者，说明您接受了邀请。它还会发送电子邮件到成员账户所有者，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**，则您的账户仍在 **Invitations** 页面上，其中列出了任何其他待处理邀请。

AWS 将发送电子邮件到组织主账户的所有者，说明您拒绝了邀请。

Note

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

接受或拒绝邀请 (AWS CLI、AWS API)

您可以使用以下命令来接受或拒绝邀请：

- AWS CLI : [aws organizations accept-handshake](#)、[aws organizations decline-handshake](#)
- AWS API : [AcceptHandshake](#)、[DeclineHandshake](#)

在组织中创建 AWS 账户

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

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

- [创建属于组织的 AWS 账户 \(p. 35\)](#)
- [访问具有主账户访问权角色的成员账户 \(p. 39\)](#)

Important

当您在组织中创建成员账户时，AWS Organizations 将自动在成员账户中创建一个 IAM 角色，以允许主账户中的 IAM 用户对成员账户进行完全管理控制。此角色受应用于成员账户的任何[服务控制策略 \(SCP\) \(p. 54\)](#) 的限制。

AWS Organizations 还将自动创建一个名为 `AWSServiceRoleForOrganizations` 的服务相关角色，该角色支持与选定 AWS 服务的集成。您必须配置其他服务来允许集成。有关更多信息，请参阅[AWS Organizations 和服务相关角色 \(p. 79\)](#)。

创建属于组织的 AWS 账户

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

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

Important

使用以下过程创建账户时，AWS 不会自动收集账户作为独立账户运行所需的全部信息。如果您需要从组织中删除账户并使其成为独立账户，则您必须先提供账户的信息，然后才能删除账户。有关更多信息，请参阅[作为成员账户退出组织 \(p. 42\)](#)。

创建自动属于组织的 AWS 账户（控制台）

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。
2. 在 Accounts 选项卡上，选择 Add account。
3. 选择 Create account (创建账户)。
4. 输入要分配给账户的名称。此名称将帮助您区分该账户与组织中的所有其他账户，并且独立于 IAM 别名或拥有者的电子邮件名称。
5. 输入新账户拥有者的电子邮件地址。此地址对该账户必须唯一，因为它可用于以账户的根用户身份登录。
6. （可选）指定分配给在新账户中自动创建的 IAM 角色的名称。此角色向组织的主账户授予访问新创建的成员账户的权限。如果您不指定名称，AWS Organizations 将为角色提供默认名称 `OrganizationAccountAccessRole`。

Important

请记住此角色名称。稍后，您将需要使用此名称向主账户中的 IAM 用户的新账户授予访问权。

7. 选择 Create。

Important

- 如果您收到错误，指明您超出了组织的账户限制，请与 [AWS Support](#) 联系。
 - 如果您收到错误，指明由于您的组织仍在进行初始化，所以您无法添加账户，请等待一小时，然后重试。
 - 您还可以检查 AWS CloudTrail 日志以了解有关账户创建是否成功的信息。有关更多信息，请参阅 [AWS Organizations 中的日志记录和监控 \(p. 89\)](#)。
 - 如果错误仍然存在，请联系 [AWS Support](#)。
8. 系统会将您重定向到 Accounts (账户)/All accounts (所有账户) 选项卡，在列表的顶部显示您的新账户，其状态设置为 Pending creation (等待创建)。在创建账户时，此状态将更改为 Active (激活)。

Note

默认情况下，Accounts (账户) 选项卡不显示失败的账户创建请求。要显示此类请求，请选择列表顶部的开关并将其更改为 Show (显示)。

9. 现在，账户已存在，拥有向主账户中的用户授予管理员访问权的 IAM 角色，您可以按照[访问和管理组织中的成员账户 \(p. 37\)](#)中的步骤访问账户。

当您创建账户时，AWS Organizations 最初为根用户分配一个最少为 64 字符长的密码。所有字符都是随机生成的，不保证出现特定字符集。您无法检索此初始密码，因为它在创建账户之后丢弃。要首次以根用户身份访问该账户，您必须完成密码恢复过程。有关更多信息，请参阅[以根用户身份访问成员账户 \(p. 37\)](#)。

创建自动属于组织的 AWS 账户 (AWS CLI、AWS API)

您可以使用以下命令之一创建账户：

- AWS CLI：[aws organizations create-account](#)
- AWS API：[CreateAccount](#)

访问和管理组织中的成员账户

在组织中创建账户时，AWS Organizations 将自动为账户创建根用户和 IAM 角色（名为 `OrganizationAccountAccessRole`）。但是，AWS Organizations 不创建任何 IAM 用户、组或其他角色。要访问组织中的账户，您必须使用以下方法之一：

- 该账户具有您可用于登录的根用户。我们建议您只使用根用户创建 IAM 用户、组 and 角色，然后始终使用其中之一登录。请参阅 [以根用户身份访问成员账户 \(p. 37\)](#)。
- 如果您在组织中创建一个账户，您可以使用预配置角色（名为 `OrganizationAccountAccessRole`）访问该账户，该角色存在于通过这种方式创建的所有新账户中。请参阅 [访问具有主账户访问权角色的成员账户 \(p. 39\)](#)。
- 如果您邀请现有账户加入您的组织，并且该账户接受邀请，则您可以创建 IAM 角色来允许主账户访问受邀账户。这类似于在使用 AWS Organizations 创建的账户时自动添加到其中的角色。如需创建此角色，请参阅 [在受邀成员账户中创建 OrganizationAccountAccessRole \(p. 38\)](#)。创建角色之后，您可以使用 [访问具有主账户访问权角色的成员账户 \(p. 39\)](#) 中的步骤访问它。

最小权限

要从组织中的任何其他账户访问 AWS 账户，必须具有以下权限：

- `sts:AssumeRole` – `Resource` 元素必须设置为星号 (*) 或账户的账户 ID 号，该账户具有需要访问新成员账户的用户。

以根用户身份访问成员账户

当您创建新账户时，AWS Organizations 最初为根用户分配一个最少为 64 字符长的密码。所有字符都是随机生成的，不保证出现特定字符集。您无法检索此初始密码。要首次以根用户身份访问该账户，您必须完成密码恢复过程。

备注

- 我们建议的[最佳实践](#)是，除了创建其他具有更多受限权限的用户和角色之外，不要使用根用户访问账户。然后以这些用户或角色之一的身份登录。
- 此外，我们还建议您对根用户设置[多重验证 \(MFA\)](#)。重置密码，然后[向根用户分配 MFA 设备](#)。
- 如果您在组织中创建了一个电子邮件地址不正确的成员账户，则无法以根用户身份登录该账户。要更新电子邮件地址，请参阅[联系我们](#)页面，然后选择与账单相关的项目以联系 AWS Support。

为成员账户的根用户请求新密码 (控制台)

1. 转至 <https://console.aws.amazon.com/> 上的 AWS 控制台的 Sign in (登录) 页面。如果您已登录 AWS，则必须先注销才能看到登录页面。
2. 如果 Sign in (登录) 页面显示 Account ID or alias (账户 ID 或别名)、IAM user name (IAM 用户名) 和 Password (密码) 三个文本框，请选择 Sign in using root account credentials (使用根账户凭证登录)。
3. 输入与 AWS 账户关联的电子邮件地址，然后选择 Next (下一步)。

4. 选择 **Forgot your password?** (忘记密码?), 然后输入将密码重置为所提供的新密码所需的信息。要执行此操作, 您必须能够访问发送到与账户关联的电子邮件地址的传入邮件。

在受邀成员账户中创建 OrganizationAccountAccessRole

默认情况下, 如果您创建属于组织的成员账户, 则 AWS 将自动在账户中创建一个角色, 此角色为主账户中的委派 IAM 用户授予管理员权限。默认情况下, 该角色名为 `OrganizationAccountAccessRole`。有关更多信息, 请参阅[访问具有主账户访问权角色的成员账户](#) (p. 39)。

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。

在成员账户中创建 AWS Organizations 管理员角色 (控制台)

1. 登录 IAM 控制台, 网址为 <https://console.aws.amazon.com/iam/>。您必须以 IAM 用户的身份登录, 代入 IAM 角色, 或在有权创建 IAM 角色和策略的成员账户中, 以根用户的身份登录 (不推荐)。
2. 在 IAM 控制台中, 导航至 **Roles** (角色), 然后选择 **Create Role** (创建角色)。
3. 选择 **Another AWS account**。
4. 输入您希望向其授予管理员访问权的主账户的 12 位账户 ID 编号。
5. 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**。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?](#)
6. 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 AWS 中使用多重验证 \(MFA\)](#)。
7. 在 **Attach permissions policies** (附加权限策略) 页面上, 选择名为 `AdministratorAccess` 的 AWS 托管策略, 然后选择 **Next: Review** (下一步: 审核)。
8. 在 **Review** 页面上, 指定角色名称和可选描述。我们建议您使用 `OrganizationAccountAccessRole`, 这是分配给新账户中角色的默认名称。要提交您的更改, 请选择 **Create role** (创建角色)。
9. 您的新角色将显示在可用角色列表上。选择新角色的名称以查看详细信息, 特别注意提供的链接 URL。向成员账户中需要访问该角色的用户提供此 URL。此外, 记下 Role ARN (角色 ARN), 因为您在步骤 15 中需要它。
10. 登录 IAM 控制台, 网址为 <https://console.aws.amazon.com/iam/>。此时, 以主账户中有权创建策略和将策略分配给用户或组的用户身份登录。
11. 导航到 **Policies** (策略), 然后选择 **Create Policy** (创建策略)。

Note

本示例演示如何创建策略并将其附加到组。如果您已为其他账户创建此策略, 请跳至步骤 19。

12. 对于 **Service**, 选择 **STS**。
13. 对于 **Actions** (操作), 在 **Filter** (筛选条件) 框中开始键入 **AssumeRole**, 然后在该角色显示后选中其旁的复选框。
14. 选择 **Resources** (资源), 确保已选择 **Specific** (特定), 然后选择 **Add ARN** (添加 ARN)。
15. 输入 AWS 成员账户 ID 号, 然后输入您之前在步骤 1–9 中创建的角色名称。
16. 如果您正授予在多个成员账户中代入该角色的权限, 请为每个账户重复步骤 14 和 15。
17. 选择查看策略。
18. 输入新策略的名称, 然后选择 **Create policy** (创建策略) 以保存您的更改。
19. 选择导航窗格中的 **Groups** (组), 然后选择要用于委派成员账户的管理权限的组的名称 (不是复选框)。

20. 选择 Attach Policy (附加策略)，选择您在步骤 11–18 中创建的策略，然后选择 Attach Policy (附加策略)。

作为选定组成员的用户现在可以使用您在步骤 9 中捕获的 URL 来访问每个成员账户的角色。他们可以像访问您在组织中创建的账户一样访问这些成员账户。有关使用角色来管理成员账户的更多信息，请参阅[访问具有主账户访问权角色的成员账户](#) (p. 39)。

访问具有主账户访问权角色的成员账户

使用 AWS Organizations 控制台创建成员账户时，AWS Organizations 将自动在账户中创建 IAM 角色（名为 `OrganizationAccountAccessRole`）。此角色具有成员账户中的完整管理权限。此角色还配置为将该访问权授予组织的主账户。您可以按照[在受邀成员账户中创建 `OrganizationAccountAccessRole`](#) (p. 38) 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，您必须以有权代入角色的主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。

向主账户中 IAM 组的成员授予访问角色的权限（控制台）

1. 以主账户中具有管理员权限的用户身份登录位于 <https://console.aws.amazon.com/iam/> 处的 IAM 控制台。这是向 IAM 组委派权限所必需的，该组的用户将访问成员账户中的角色。
2. 在导航窗格中，选择 Groups (组)，然后选择其成员能够代入成员账户中角色的组的名称（不是复选框）。如果需要，您可以创建新组。
3. 选择 Permissions (权限) 选项卡，然后展开 Inline Policies (内联策略) 部分。
4. 如果不存在内联策略，则选择 [click here](#) 创建一个。否则，选择 Create Group Policy。
5. 在 Policy Generator 旁，选择 Select。
6. 在 Edit Permissions 页上，设置以下选项：
 - 对于 Effect，选择 Allow。
 - 对于 AWS Service，选择 AWS Security Token Service。
 - 对于 Actions，选择 AssumeRole。
 - 对于 Amazon Resource Name (ARN) (Amazon 资源名称 (ARN))，输入在成员账户中创建的角色角色的 ARN。在 IAM 控制台中角色的 Summary (摘要) 页面上，可以看到此 ARN。要构建此 ARN，请使用以下模板：

```
arn:aws:iam::accountIdNumber:role/rolename
```

替换在您创建账户时配置的成员账户 ID 编号和角色名称。如果未指定角色名称，则名称默认为 `OrganizationAccountAccessRole`。ARN 应如下所示：

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

7. 选择 Add Statement (添加语句)，然后选择 Next Step (下一步)。
8. 在 Review Policy 页面上，确保角色 ARN 正确。输入新策略的名称，然后选择 Apply Policy (添加策略)。

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

切换到成员账户的角色（控制台）

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

1. 从 AWS Organizations 控制台的右上角，选择包含当前登录名称的链接，然后选择 Switch Role (切换角色)。
2. 输入管理员提供的账户 ID 号和角色名称。

3. 对于 Display Name (显示名称)，输入文本；在您使用角色时，该文本将显示在导航栏的右上角用于替换您的用户名。您还可选择颜色。
4. 选择 Switch Role。现在，您执行的所有操作已完成，并且已将权限授予给您切换到的角色。在切换回之前，您不再具有与原始 IAM 用户关联的权限。
5. 完成需要角色权限的操作后，您可以切换回普通 IAM 用户。选择右上角的角色名称（无论您指定什么作为 Display Name (显示名称)），然后选择 Back to **UserName** (返回到 UserName)。

其他资源

- 有关授予切换角色权限的更多信息，请参阅 IAM 用户指南 中的 [向用户授予切换角色的权限](#)。
- 有关使用要代入的您已授予权限的角色的更多信息，请参阅 IAM 用户指南 中的 [切换到角色 \(AWS 管理控制台\)](#)。
- 有关使用角色进行跨账户访问的教程，请参阅 IAM 用户指南 中的 [教程：使用 IAM 角色委派跨 AWS 账户的访问权](#)。
- 有关关闭 AWS 账户的信息，请参阅 [关闭 AWS 账户 \(p. 43\)](#)。

从组织中删除成员账户

组织账户管理工作的一部分是删除不再需要的成员账户。此页面介绍了您在删除账户之前需要了解的信息，并提供了删除账户的过程。

有关删除主账户的信息，请参阅 [移除主账户并删除组织 \(p. 30\)](#)。

主题

- [从组织中删除账户前需知 \(p. 40\)](#)
- [从组织中删除成员账户 \(p. 41\)](#)
- [作为成员账户退出组织 \(p. 42\)](#)

从组织中删除账户前需知

删除账户之前，您需要了解以下内容：

- 仅当账户拥有作为独立账户运行所需的信息时，才能从组织中移除此账户。当您使用 AWS Organizations 控制台、API 或 AWS CLI 命令在组织中创建账户时，系统将不会自动收集独立账户所需的任何信息。对于您想用作独立账户的每个账户，您必须接受 AWS 客户协议，选择支持计划，提供和验证所需联系信息，并提供当前的付款方式。AWS 将使用该付款方式向账户未绑定到组织期间发生的任何可结算（非 AWS 免费套餐）AWS 活动收费。
- 即使在从组织内删除已创建的账户（使用 AWS Organizations 控制台或 CreateAccount API 创建的账户）之后，(i) 已创建账户仍受与我们达成的创建主账户协议条款的约束，并且 (ii) 创建主账户将对其创建的账户执行的任何操作承担共同和单独的责任。未经我们的事先同意，不得转让或转移客户与我们之间的协议以及这些协议下的权利和义务。要获得我们的同意，请通过 <https://aws.amazon.com/contact-us/> 与我们联系。
- 当某个成员账户离开组织后，该账户不再有权访问其属于该组织成员时的时间范围内的成本和使用率数据。但是，组织的主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。

从组织中移除账户的影响

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

- 现在，该账户负责支付自己的费用，并且必须向该账户附加有效的付款方式。
- 该账户中的委托人不再受组织内定义的任何 [服务控制策略 \(SCP\)](#) (p. 54) 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。
- 与其他服务的集成可能会被禁用。例如，AWS Single Sign-On 需要组织才能运行，因此，如果您从支持 AWS SSO 的组织中移除账户，则此账户中的用户将无法再使用该服务。

从组织中删除成员账户

登录组织的主账户后，您可以从组织中移除不再需要的成员账户。为此，请完成以下过程。这些过程仅适用于成员账户。要移除主账户，您必须 [删除组织](#)。

Note

如果从组织中删除成员账户，则该成员账户将不再由组织协议所涵盖。主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好新协议。有效的组织协议列表可在 [AWS Artifact 组织协议](#) 中进行查看。

最小权限

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

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

如果您选择在步骤 6 中以成员账户中的 IAM 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` (仅限控制台)。
- `organizations:LeaveOrganization` – 请注意，组织管理员可以将删除此权限的策略应用到您的账户，从而阻止您从组织中删除自己的账户。
- 如果您以 IAM 用户身份登录并且账户缺少付款信息，则 IAM 用户必须具有 `aws-portal:ModifyBilling` 和 `aws-portal:ModifyPaymentMethods` 权限。此外，成员账户必须已启用对账单的 IAM 用户访问权限。如果尚未启用此权限，请参阅 [AWS Billing and Cost Management 用户指南](#) 中的 [激活对账单和成本管理控制台的访问权](#)。

从组织中删除成员账户 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须登录组织的主账户。
2. 在 Accounts (账户) 选项卡上，选中要从组织中删除的成员账户旁的复选框。可以选择多个。
3. 选择 Remove account。
4. 在 Remove account 对话框中，选择 Remove。

这将显示一个对话框，其中显示每个账户的成功或失败状态。

5. 如果 AWS Organizations 无法删除一个或多个账户，通常是因为您没有提供账户作为独立账户运行所需的全部信息。执行以下步骤：
 - a. 登录其中一个失败的账户。
 - b. 建议您通过选择 Copy link (复制链接)，然后将它粘贴在新的无痕浏览器窗口的地址栏中来登录成员账户。如果您未使用无痕窗口，则您已注销主账户，并且无法导航回此对话框。
 - c. 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
 - 接受 AWS 客户协议
 - 提供有效的付款方式
 - 验证电话号码
 - 选择支持计划选项
- d. 在完成注册过程的最后一步后，AWS 会自动将您的浏览器重定向至成员账户的 AWS Organizations 控制台。选择 `Leave organization`，然后在确认对话框中确认您的选择。系统将您重定向到 AWS Organizations 控制台的 `Getting Started` (入门) 页面，在其中可以查看您的账户加入其他组织的任何待处理邀请。

从组织中删除成员账户 (AWS CLI、AWS API)

您可以使用以下命令之一删除成员账户：

- AWS CLI : [aws organizations remove-account-from-organization](#)
- AWS API : [RemoveAccountFromOrganization](#)

作为成员账户退出组织

登录成员账户后，您可以将该账户从其组织中删除。为此，请完成以下过程。主账户不能使用此方法离开组织。要移除主账户，您必须[删除组织](#)。

Note

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

最小权限

要退出 AWS 组织，您必须拥有以下权限：

- `organizations:DescribeOrganization` (仅限控制台)。
- `organizations:LeaveOrganization` – 请注意，组织管理员可以将删除此权限的策略应用到您的账户，从而阻止您从组织中删除自己的账户。
- 如果您以 IAM 用户身份登录并且账户缺少付款信息，则 IAM 用户必须具有 `aws-portal:ModifyBilling` 和 `aws-portal:ModifyPaymentMethods` 权限。此外，成员账户必须已启用对账单的 IAM 用户访问权限。如果尚未启用此权限，请参阅 [AWS Billing and Cost Management 用户指南](#) 中的[激活对账单和成本管理控制台的访问权](#)。

Note

组织的账户状态影响可见的成本和使用率数据：

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

以成员账户身份退出组织 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您可以具有必需权限的 IAM 用户的身份登录，或以要从组织中删除的成员账户的根用户的身份登录。默认情况下，您无权访问使用 AWS Organizations 创建的成员账户中的根用户密码。如果需要，请按照[以根用户身份访问成员账户 \(p. 37\)](#)中的步骤恢复根用户密码。
2. 在 Organization overview 页面上，选择 Leave organization。
3. 执行下列步骤之一：
 - 如果您的账户具有作为独立账户运行所需的全部信息，则将显示一个确认对话框。确认您选择删除账户。系统将您重定向到 AWS Organizations 控制台的 Getting Started (入门) 页面，在其中可以查看您的账户加入其他组织的任何待处理邀请。
 - 如果您的账户没有所有必需信息，请执行以下步骤：
 - a. 这将显示一个对话框，其中说明您必须完成一些额外步骤。单击链接。
 - b. 完成提供的所有注册步骤。步骤可能包括：
 - 提供联系人信息
 - 接受 AWS 客户协议
 - 提供有效的付款方式
 - 验证电话号码
 - 选择支持计划选项
 - c. 在出现一个指明注册过程已完成的对话框时，请选择 Leave organization。
 - d. 您将看到确认对话框。确认您选择删除账户。系统将您重定向到 AWS Organizations 控制台的 Getting Started (入门) 页面，在其中可以查看您的账户加入其他组织的任何待处理邀请。

作为成员账户退出组织 (AWS CLI、AWS API)

您可以使用以下命令之一离开组织：

- AWS CLI : [aws organizations leave-organization](#)
- AWS API : [LeaveOrganization](#)

关闭 AWS 账户

如果您不再需要某个 AWS 账户 (无论是否为组织中的成员账户) 并想要确保没有人会使该账户产生费用，您可以关闭此账户。

在关闭账户前，请备份您想要保留的所有应用程序和数据。此账户中存储的所有资源和数据都将丢失，并且无法恢复。有关更多信息，请参阅 KB 文章 [如何关闭 Amazon Web Services 账户？](#)

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

Important

- 已关闭 90 天的账户可能被永久删除，在此之后，将无法恢复该账户及其资源。
- 已关闭的账户将在组织中显示为“已暂停”状态。账户被永久删除后，它将不再显示在您的组织中。

您只能使用 Billing and Cost Management 控制台关闭账户，而不是使用 AWS Organizations 控制台或其工具。

要关闭主账户，请先[删除组织 \(p. 30\)](#)，然后使用以下过程中的步骤关闭它。

关闭 AWS 账户 (控制台)

建议：在关闭账户前，备份您想要保留的所有应用程序和数据。账户关闭后，AWS 无法恢复或还原账户资源和数据。

1. 使用与账户关联的电子邮件地址和密码，[以账户的根用户身份登录](#)您想要关闭的账户。如果您以 IAM 用户身份或角色登录，则无法关闭账户。

Note

默认情况下，您使用 AWS Organizations 创建的成员账户没有与账户根用户关联的密码。要登录，您必须请求根用户的密码。有关更多信息，请参阅[以根用户身份访问成员账户 \(p. 37\)](#)。

2. 从 <https://console.aws.amazon.com/billing/home#/> 打开 Billing and Cost Management 控制台。
3. 在右上角的导航栏中，选择账户名称（或别名），然后选择我的账户。
4. 在 Account Settings 页面上，滚动至页面底端的 Close Account 部分。阅读并确保您理解复选框旁的文本内容。
5. 选中复选框以确认您理解条款，然后选择 Close Account (关闭账户)。
6. 在确认对话框中，选择 Close Account。

关闭 AWS 账户后，您无法再使用其访问 AWS 服务或资源。在您关闭账户后的 90 天（“关闭后期间”），您将能够登录以查看过去的账单并访问 AWS Support。您可以在关闭后期间内联系 AWS Support 以重新打开账户。有关更多信息，请参阅知识中心内的[如何重新打开已关闭的 AWS 账户？](#)。

管理组织单元 (OU)

您可以使用组织单元 (OU)，将账户分组到一起，作为一个单元管理。这将极大简化您的账户管理。例如，您可以将基于策略的控制附加到 OU，该 OU 中的所有账户将自动继承策略。您可以在单个组织内创建多个 OU，也可以在其他 OU 中创建 OU。每个 OU 可以包含多个账户，您可以将账户从一个 OU 移动到另一个。但是，OU 名称必须在父 OU 或根内是唯一的。

Note

当前，您只能有一个根，它是在您首次设置组织时由 AWS Organizations 为您创建的。默认根的名称为“root”。


要确定组织中账户的结构，您可以执行以下任务：

- [查看 OU 的详细信息 \(p. 28\)](#)
- [创建 OU \(p. 46\)](#)
- [重命名 OU \(p. 46\)](#)
- [将账户移动到 OU 或者在根和 OU 之间移动 \(p. 47\)](#)

浏览根和 OU 层次结构

要在移动账户或附加策略时导航到不同的 OU 或根，可以使用树视图。

启用和使用组织的树视图

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。
2. 选择 Organize accounts 选项卡。
3. 如果页面左侧未显示树视图窗格，请选择 TREE VIEW (树视图) 开关图标 。
4. 初始状态下，树结构只显示根及子 OU 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 + 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 — 图标。
5. 选择要导航到的 OU 或根。树视图中以加粗文本显示的节点是当前在中心窗格中查看的节点。

备注

- 中央窗格中的重命名、删除和移动操作：在控制台中查看根或 OU 的内容时，可以与此根或 OU 的子实体进行交互。例如，选中子 OU 或账户的复选框后，可以选择此部分上方的 Rename、Delete 或 Move 链接对选中的实体执行相应的操作。这些操作只 应用到选中的子实体，不应用到上级根或 OU。要对上级 OU 执行同样的操作，必须导航到 OU 的父 OU 或根，然后选中要管理的子 OU 的复选框。
- Details 窗格：控制台右侧的详细信息窗格显示有关您正在查看的根或 OU 的信息。如果选中子实体的复选框，则详细信息窗格将切换为显示有关所选实体的信息。要再次查看上级根或 OU 的详细信息，则必须清除此复选框。或者，您也可以导航到父根或 OU，然后选中要查看其信息的 OU 的复选框。

不使用树视图进行导航

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。
2. 选择 Organize accounts 选项卡。
3. 选择要在中央窗格中查看的 OU 的名称 (而不是复选框) 可导航到下一个分支。

4. 选择中央窗格标题栏上的后退按钮 (<) 可导航到上一个分支。

创建 OU

登录到组织的主账户时，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。

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` (仅限控制台)
- `organizations:CreateOrganizationalUnit`

创建 OU (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。

控制台会显示根的内容。首次访问根时，控制台在该顶级视图中显示所有 AWS 账户。如果您以前创建了 OU 并将账户移动到其中，则控制台仅显示顶级 OU 以及任何您尚未移动到 OU 中的账户。

2. (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 来[导航到该子 OU \(p. 45\)](#)。
3. 当您处于层次结构中的正确位置时，选择 Create organizational unit (OU)。
4. 在 Create organizational unit 对话框中，键入要创建的 OU 的名称，然后选择 Create organizational unit。

您的新 OU 显示在父级内部。现在，您可以[将账户移动到此 OU \(p. 47\)](#) 或者[将策略附加到 \(p. 52\)](#)此 OU。

创建 OU (AWS CLI、AWS API)

您可以使用以下命令之一创建 OU：

- AWS CLI：[aws organizations create-organizational-unit](#)
- AWS API：[CreateOrganizationalUnit](#)

重命名 OU

登录到组织的主账户时，您可以重命名 OU。为此，请完成以下步骤。

最小权限

要在 AWS 组织的根中重命名 OU，您必须拥有以下权限：

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

重命名 OU (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。

2. 在 Organize accounts 选项卡上，[导航到要重命名的 OU 的父级 \(p. 45\)](#)。选中要重命名的子 OU 对应的复选框。
3. 选择 OU 列表上方的 Rename。
4. 在 Rename organizational unit 对话框中，键入新名称，然后选择 Rename organizational unit。

重命名 OU (AWS CLI、AWS API)

您可以使用以下命令之一重命名 OU：

- AWS CLI：[aws organizations update-organizational-unit](#)
- AWS API：[UpdateOrganizationalUnit](#)

将账户移动到 OU 或者在根和 OU 之间移动

登录到组织的主账户时，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，则该账户仅遵循附加到根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` (仅限控制台)
- `organizations:MoveAccount`

将账户移动到 OU (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录 ([不推荐](#))。
2. 选择 Organize accounts (组织账户) 选项卡，然后[导航到包含要移动的账户的 OU \(p. 45\)](#)。找到账户之后，选中其复选框。如果您要移动多个账户，请选中多个复选框。
3. 选择账户列表上方的 Move。
4. 在 Move accounts (移动账户) 对话框中，选择要将账户移动到的 OU 或根，然后选择 Select (选择)。

将账户移至 OU (AWS CLI、AWS API)

您可以使用以下命令之一移动账户：

- AWS CLI：[aws organizations move-account](#)
- AWS API：[MoveAccount](#)

删除您不再需要的 OU

登录到组织的主账户时，您可以删除不再需要的 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` (仅限控制台)

- `organizations:DeleteOrganizationalUnit`

删除 OU (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录 ([不推荐](#))。
2. 在 Organize accounts 选项卡上，[导航到要删除的 OU 的父容器 \(p. 45\)](#)。选中 OU 的复选框。如果要删除多个 OU，您可以选中多个 OU 的复选框。
3. 选择 OU 列表上方的 Delete。

AWS Organizations 将删除 OU 并将其从列表中删除。

删除 OU (AWS CLI、AWS API)

您可以使用以下命令之一删除 OU：

- AWS CLI：[aws organizations delete-organizational-unit](#)
- AWS API：[DeleteOrganizationalUnit](#)

管理 AWS Organizations 策略

使用 AWS Organizations 中的策略，您能够将其他类型的管理应用于组织中的 AWS 账户。您可以在组织中[启用所有功能 \(p. 24\)](#)的情况下使用策略。您可以将策略应用到您的组织中的以下实体：

- 根 – 应用到根的策略会应用于组织中的所有账户
- OU – 应用于 OU 的策略会应用于 OU 及其任何子 OU 中的所有账户
- 账户 – 应用于账户的策略仅应用于这一个账户

目前，服务控制策略 (SCP) 是唯一受支持的策略类型。

如果组织启用了所有功能，则可使用各种策略类型。但是，您可以在根级别使用 [EnablePolicyType](#) 和 [DisablePolicyType](#) 操作禁用单个策略类型。使用 [DescribeOrganization](#) API 操作可确定可供使用的组织策略类型。使用 [ListRoots](#) API 操作可查看在每个根级别启用和禁用的策略类型。

AWS Organizations 控制台也可以显示启用和禁用的策略类型。在 Organize accounts (组织账户) 选项卡上，选择左侧导航窗格中的 Root。右侧详细信息窗格显示所有可用的策略类型，并指示各自的启用和禁用状态。

Important

当您在根中禁用策略类型时，该类型的所有策略自动与此根中的所有实体分离。如果您重新启用该策略类型，此根将恢复为该策略类型的默认状态。例如，如果您重新启用根中的 SCP，则此根中的所有实体最初仅附加到默认的 SCP `FullAWSAccess` 策略。在禁用策略类型前附加到实体的任何策略附加对象都将丢失，无法自动恢复。

有关特定于 SCP 的过程，请参阅[创建和更新 SCP \(p. 59\)](#)。

以下过程适用于所有策略类型。您必须[启用根中的一个策略类型 \(p. 51\)](#)，然后才能将该类型的策略附加到该根中的任何实体。

主题

- [列出和显示有关 AWS Organizations 策略的信息 \(p. 49\)](#)
- [在根上启用和禁用策略类型 \(p. 51\)](#)
- [将策略附加到根、OU 或账户 \(p. 52\)](#)
- [从根、OU 或账户分离策略 \(p. 53\)](#)
- [删除策略 \(p. 54\)](#)
- [服务控制策略 \(p. 54\)](#)

列出和显示有关 AWS Organizations 策略的信息

本部分介绍了各种方法来获取有关您组织中的策略的详细信息。

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`

列出组织中的所有策略 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录 ([不推荐](#))。
2. 选择 Policies 选项卡。

显示的列表包含组织中当前定义的所有类型的策略。

列出组织中的所有策略 (AWS CLI、AWS API)

可以使用以下命令之一列出组织中的策略：

- AWS CLI : [aws organizations list-policies](#)
- AWS API : [ListPolicies](#)

列出附加到根、OU 或账户的所有策略

最小权限

要列出附加到您组织中的根、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 ARN (或 "*")。

列出直接附加到指定的根、OU 或账户的所有策略 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录 ([不推荐](#))。
2. 在 Organize accounts (组织账户) 选项卡上，[导航到 \(p. 45\)](#)要查看其策略附加对象的根、OU 或账户。
 - a. 对于根或 OU，请勿选中任何复选框。这样，右侧的详细信息窗格将显示有关您正在查看的根或 OU 的信息。或者，您也可以导航到 OU 的父级，然后选中要查看其信息的 OU 的复选框。
 - b. 对于账户，选中与账户对应的框。
3. 在右侧的详细信息窗格中，展开 Service control policies 部分。

所示列表中显示直接附加到该实体的所有策略。它还显示了因继承自根或父 OU 而影响此实体的策略。

列出直接附加到所指定根、OU 或账户的所有策略 (AWS CLI、AWS API)

可以使用以下命令之一列出附加到实体的策略：

- AWS CLI : [aws organizations list-policies-for-target](#)
- AWS API : [ListPoliciesForTarget](#)

列出策略附加到的所有根、OU 和账户

最小权限

要列出策略附加到的实体，您必须拥有以下权限：

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

列出附加了指定策略的所有根、OU 和账户 (控制台)

1. 选择 Policies (策略) 选项卡，然后选中您感兴趣的策略旁边的复选框。
2. 在右侧的详细信息窗格中，选择以下选项之一：
 - Accounts：查看策略直接附加到的账户的列表
 - Organizational units：查看策略直接附加到的 OU 的列表
 - Roots：查看策略直接附加到的根的列表

列出拥有附加的所指定策略的所有根、OU 和账户 (AWS CLI、AWS API)

可以使用以下命令之一列出具有策略的实体：

- AWS CLI：[aws organizations list-targets-for-policy](#)
- AWS API：[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 "*")。

获取有关策略的详细信息 (控制台)

1. 选择 Policies (策略) 选项卡，然后选中您感兴趣的策略旁边的复选框。

右侧的“Details”(详细信息) 窗格中显示有关策略的可用信息，包括 ARN、描述和附加项。

2. 要查看策略的内容，请选择 Policy editor。

中央窗格显示以下信息：

- 策略的详细信息：名称、描述、唯一 ID 和 ARN。
- 策略附加到的根、OU 和账户的列表。选择每个项目以查看每种类型的各个实体。
- 策略内容 (特定于策略类型)：
 - 对于 SCP，为用于定义附加账户中允许的权限的 JSON 文本

要更新策略文档的内容，请选择 Edit (编辑)。完成后选择 Save (保存)。有关更多详情，请参阅下一部分。

获取有关策略的详细信息 (AWS CLI、AWS API)

可以使用以下命令之一获取有关策略的详细信息：

- AWS CLI：[aws organizations describe-policy](#)
- AWS API：[DescribePolicy](#)

在根上启用和禁用策略类型

在您可以将任何类型的策略附加到根之前，您必须首先启用该根以支持指定的策略类型。

Note

- 目前，您的组织中只能有一个根。
- 当前，仅支持 SCP 策略类型。

Important

当您在根中禁用策略类型时，该类型的所有策略自动与此根中的所有实体分离。如果您重新启用该策略类型，此根将恢复为该策略类型的默认状态。例如，如果您重新启用根中的 SCP，则此根中的所有实体最初仅附加到默认的 FullAWSAccess 策略。在禁用策略类型前附加到实体的任何策略附加对象都将丢失，无法自动恢复。

Note

AWS Organizations 控制台可以显示每种策略类型的启用和禁用状态。在 Organize accounts (组织账户) 选项卡上，选择左侧导航窗格中的 Root。右侧屏幕上的详细信息窗格显示所有可用的策略类型，并指示其在根级别的启用和禁用状态。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。

最小权限

要在组织的根中启用一种策略类型，您必须拥有以下权限：

- `organizations:EnablePolicyType`
- `organizations:DescribeOrganization`

在根上启用或禁用策略类型 (控制台)

当您登录到您组织的主账户时，您可以在根上启用或禁用策略类型。

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录 ([不推荐](#))。
2. 在 Organize accounts (组织账户) 选项卡上，选择左侧导航窗格中的 Root (根)。
3. 在屏幕右侧的详细信息窗格中，选择 Service control policies 旁的 Enable 或 Disable。

Note

您必须先从根中的所有实体分离指定类型的所有策略，然后才能禁用该根中的策略类型。

在根上启用或禁用策略类型 (AWS CLI、AWS API)

可以使用以下命令之一禁用策略类型：

- AWS CLI : [aws organizations enable-policy-type](#) 和 [aws organizations disable-policy-type](#)
- AWS API : [EnablePolicyType](#) 和 [DisablePolicyType](#)

将策略附加到根、OU 或账户

当登录到您组织的主账户时，您可以将以前创建的策略附加到根或 OU，或者直接附加到账户。要附加策略，请完成以下步骤。

最小权限

要将策略附加到根、OU 或账户，您必须拥有以下权限：

- `organizations:AttachPolicy`，且同一条策略语句中有一个 `Resource` 元素包含“*”、指定策略的 ARN 或是您要附加该策略的根、OU 或账户的 ARN。

将策略附加到根、OU 或账户 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录 ([不推荐](#))。
2. 在 Organize accounts (组织账户) 选项卡上，[导航到 \(p. 45\)](#)要将策略附加到的根、OU 或账户并选中它们对应的复选框。
3. 在右侧的 Details (详细信息) 窗格中，展开 Service control policies (服务控制策略) 部分以查看当前附加的策略的列表。
4. 在可用策略列表中，找到所需策略，然后选择 Attach (附加)。附加策略列表会更新，其中新增了策略。该策略将立即生效。例如，SCP 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。

将策略附加到根、OU 或账户 (AWS CLI、AWS API)

可以使用以下命令之一附加策略：

- AWS CLI：[aws organizations attach-policy](#)
- AWS API：[AttachPolicy](#)

从根、OU 或账户分离策略

当登录到您组织的主账户时，您可以从策略所附加到的根、OU 或账户分离策略。从某个实体分离策略后，该策略将不再应用于现在分离的实体所影响的任何账户。要分离策略，请完成以下步骤。

Note

您无法从实体中分离最后一个 SCP。在任何时候都必须至少有一个 SCP 附加到所有实体。

最小权限

要从根、OU 或账户分离策略，您必须拥有以下权限：

- `organizations:DetachPolicy`

从根、OU 或账户分离策略 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录 ([不推荐](#))。
2. 在 Organize accounts (组织账户) 选项卡上，[导航到 \(p. 45\)](#)要分离策略的根、OU 或账户并选中它们对应的复选框。
3. 在右侧的 Details (详细信息) 窗格中，展开 Service control policies (服务控制策略) 部分以查看当前附加的策略的列表。Source (源) 字段指示策略的来源。它可以直接附加到账户或 OU，也可以附加到父 OU 或根。
4. 找到要分离的策略，然后选择 Detach (分离)。附加策略的列表会更新，其中删除了所选策略。分离策略所导致的策略更改会立即生效。例如，分离 SCP 会立即影响以前附加的账户或以前附加的根或 OU 下的账户中 IAM 用户和角色的权限。

从根、OU 或账户分离策略 (AWS CLI、AWS API)

可以使用以下命令之一分离策略：

- AWS CLI : [aws organizations detach-policy](#)
- AWS API : [DetachPolicy](#)

删除策略

当登录到您组织的主账户时，您可以删除您的组织中不再需要的策略。

备注

- 必须先将某个策略从所有附加实体中分离，然后才能删除该策略。
- 您无法删除任何 AWS 托管的 SCP，例如名为 FullAWSAccess 的 SCP。

要删除策略，请完成以下步骤。

最小权限

要删除策略，您必须拥有以下权限：

- `organizations:DeletePolicy`

删除策略 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。
2. 要删除的策略必须先从所有根、OU 和账户分离。执行[从根、OU 或账户分离策略 \(p. 53\)](#)中的步骤以从组织中的所有实体分离策略。
3. 在 Policies (策略) 选项卡上，选择要删除的策略。
4. 选择 Delete policy (删除策略)。

删除策略 (AWS CLI、AWS API)

可以使用以下命令之一删除策略：

- AWS CLI : [aws organizations delete-policy](#)
- AWS API : [DeletePolicy](#)

服务控制策略

服务控制策略 (SCP) 是一种可用来管理您的组织的策略。SCP 提供对组织中所有账户的最大可用权限的集中控制，使您能够确保您的账户遵循组织的访问控制指南。SCP 仅在[启用所有功能 \(p. 24\)](#)的组织中可用。如果您的组织只启用了整合账单功能，则不能使用 SCP。有关启用 SCP 的说明，请参阅[在根上启用和禁用策略类型 \(p. 51\)](#)。

SCP 是必要的，但不足以授予您组织中的账户访问权限。通过将 SCP 附加到组织根或组织单位 (OU)，会为组织根或 OU 中的账户可执行的操作定义防护机制。您仍然需要将 [IAM 策略](#)附加到组织账户中的用户和角色在以便实际向其授予权限。利用附加到这些账户的 SCP，仅当基于身份的策略和基于资源的策略以及 SCP 允许该操作时，才向实体授予这些权限。如果权限边界（高级 IAM 功能）和 SCP 同时存在，则边界、SCP 以及基于身份的策略必须全部允许操作。有关更多信息，请参阅 IAM 用户指南 中的[策略评估逻辑](#)。

主题

- [测试 SCP 的影响 \(p. 55\)](#)
- [SCP 大小限制 \(p. 55\)](#)
- [对权限的影响 \(p. 55\)](#)
- [使用访问数据改进 SCP \(p. 56\)](#)
- [不受 SCP 限制的任务和实体 \(p. 56\)](#)
- [SCP 的工作方式 \(p. 56\)](#)
- [有关使用 SCP 的策略 \(p. 57\)](#)
- [创建和更新 SCP \(p. 59\)](#)
- [示例服务控制策略 \(p. 62\)](#)
- [SCP 语法 \(p. 68\)](#)

测试 SCP 的影响

AWS 强烈建议您不要在没有彻底测试策略对账户的影响的情况下将 SCP 附加到组织的根。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](#)。另一种方法是使用 [AWS CloudTrail 记录 API 级别的服务使用情况](#)。

SCP 大小限制

SCP 中的所有字符将计入其[大小限制 \(p. 96\)](#)。本指南中的示例演示了使用额外空格编排格式的 SCP，以提高其可读性。但如果您的策略大小接近限制，则可以删除任何空格（例如，引号之外的空格字符和换行符）来节省空间。

Tip

使用可视化编辑器构建您的 SCP。它会自动删除额外的空格。

对权限的影响

SCP 类似于 IAM 权限策略，使用几乎相同的语法。但是，SCP 永远不会授予权限。相反，SCP 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略。请注意以下几点：

- SCP 限制成员账户中实体的权限，包括每个 AWS 账户根用户。任何账户都只有上方的每个父级允许的那些权限。如果权限在账户上面的任何级别被隐式阻止（通过不包括在 Allow 策略语句中）或明确阻止（通过包括在 Deny 策略语句中），则受影响账户中的用户或角色不能使用该权限，即使账户管理员将带有 `*/` 权限的 `AdministratorAccess` IAM 策略附加到用户也是如此。
- 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 权限策略的用户根本没有访问权，即使适用的 SCP 允许所有服务和所有操作也是如此。
- 如果用户或角色具有 IAM 权限策略，而该策略允许访问适用的 SCP 也允许的操作，则用户或角色可以执行该操作。
- 如果用户或角色具有 IAM 权限策略，而该策略允许访问不允许或被相应的 SCP 明确拒绝的操作，则用户或角色不能执行该操作。
- SCP 会影响附加账户中的所有用户和角色，包括根用户。唯一的例外是以下任务列表中描述的那些不受影响并且不能通过使用 SCP 进行限制的任务。
- SCP 不会影响任何服务相关角色。服务相关角色可让其他 AWS 服务与 AWS Organizations 集成且不受 SCP 的限制。
- SCP 只影响委托人，此类委托人由属于组织的账户进行管理。它们不会影响组织外的账户的用户或角色。例如，请考虑一个由组织中的账户“A”所有的 Amazon S3 存储桶。存储桶策略会向来自组织外账户的用户

授予访问权限。账户 A 附加了一个 SCP。该 SCP 不适用于这些外部用户。它仅适用于由该组织内的账户“A”所管理的用户。

- 您在根中禁用 SCP 策略类型时，所有 SCP 都将自动从该根中的所有实体分离。如果在根中重新启用 SCP，该根将仅恢复为自动附加到根中所有实体的默认 FullAWSAccess 策略。在禁用 SCP 之前 SCP 的任何附加对象都将丢失，并且不能自动恢复，不过您可以手动重新附加它们。

使用访问数据改进 SCP

使用主账户凭证登录时，您可在 IAM 控制台的 AWS Organizations 部分中，查看 AWS Organizations 实体或策略的[服务上次访问数据](#)。您还可在 IAM 中使用 AWS CLI 或 AWS API 检索上次访问的服务相关数据。此数据包含相关信息，说明 AWS Organizations 账户中的委托人上次尝试访问了哪些允许的服务以及访问这些服务的时间。您可以使用此信息确定不必要的权限，从而优化 SCP 以更好地遵循[最小特权原则](#)。

例如，您可能有一个[拒绝列表 SCP \(p. 58\)](#)，禁止访问三个 AWS 服务。SCP 的 Deny 语句中未列出的所有服务均允许访问。IAM 中的服务上次访问数据告知您哪些 AWS 服务是 SCP 允许但从未使用的。借助该信息，您可以更新 SCP 以拒绝对不需要服务的访问权限。

有关更多信息，请参阅 IAM 用户指南 中的以下页面：

- [为组织查看组织服务上次访问数据](#)
- [使用数据来细化组织部门的权限](#)

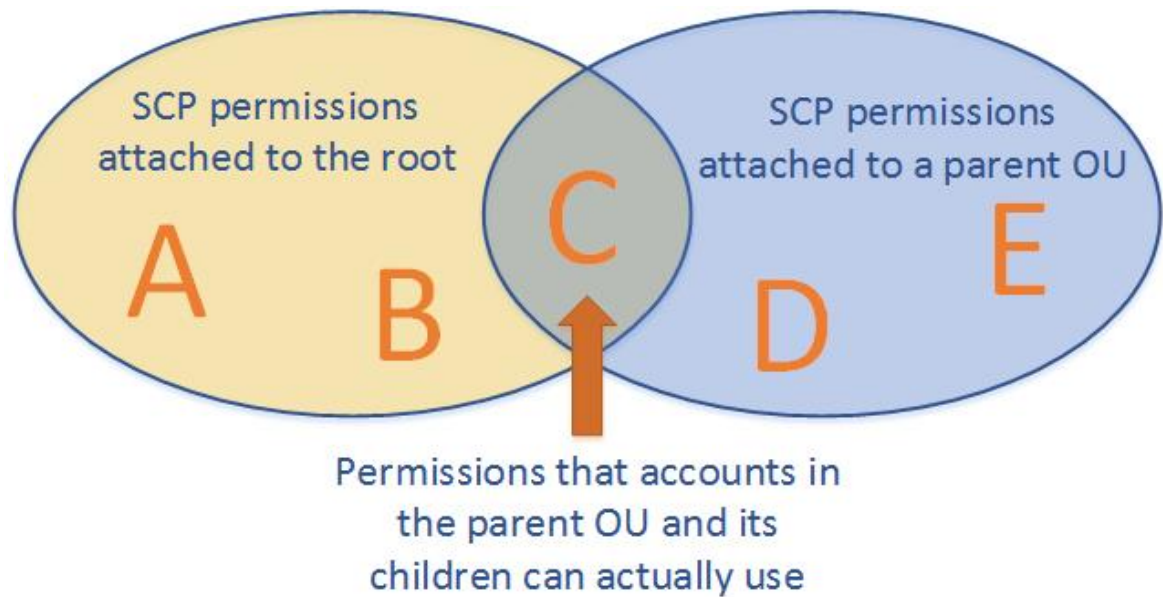
不受 SCP 限制的任务和实体

下列任务和实体不受 SCP 的限制：

- 由主账户执行的操作。
- 使用附加到服务相关角色的权限执行的任何操作。
- 管理根凭证。无论附加什么 SCP，账户中的根用户始终可以执行以下操作：
 - 更改根用户的密码
 - 创建、更新或删除根访问密钥
 - 在根用户上启用或禁用多重验证
 - 创建、更新或删除根用户的 x.509 密钥
- 以根用户身份注册企业支持计划
- 以根用户身份更改 AWS Support 级别
- 管理 Amazon CloudFront 密钥
- CloudFront 私有内容的可信签署人功能
- 修改 AWS 账户电子邮件限额/反向 DNS
- 对 AWS 相关的一些服务执行任务：
 - Alexa Top Sites
 - Alexa Web Information Service
 - Amazon Mechanical Turk
 - Amazon Product Marketing API

SCP 的工作方式

下图说明了 [SCP \(p. 54\)](#) 的工作方式。



在此图中，根的附加 SCP 允许权限 A、B 和 C。该根中的 OU 的 SCP 允许 C、D 和 E。由于根的 OU 不允许 D 或 E，因此，根或其任何子级中的任何项都无法使用这些权限，包括父 OU。即使父 OU 明确允许这些权限，这些权限最终也会被阻止，因为它们已由根阻止。此外，由于 OU 的 SCP 不允许 A 或 B，因此，已为父 OU 及其任何子级阻止这些权限。但是，根下的作为父 OU 的对等的其他 OU 可以允许 A 和 B。

仍必须使用已附加到用户和角色或组的 IAM 权限策略向用户和角色授予权限。SCP 筛选此类策略授予的权限，并且用户无法执行适用的 SCP 不允许的任何操作。如果一个或多个 IAM 权限策略向用户或角色授予 SCP 所允许的操作的权限，则可使用这些操作。

如果您将 SCP 附加到根或 OU，或将 SCP 直接附加到账户，则将使用控制 IAM 权限策略的相同规则来评估影响给定账户的所有策略：

- 无法向受影响账户中的用户或角色委派在 SCP 中具有显式 Deny 的任何操作。显式 Deny 语句将覆盖其他 SCP 可能授予的任何 Allow。
- 可向受影响账户中的用户和角色委派在 SCP (例如，默认“*”SCP 或调用特定服务或操作的任何其他 SCP) 中具有显式 Allow 的任何操作。
- SCP 未明确允许的任何操作将被隐式拒绝，且无法委派给受影响账户中的用户或角色。

默认情况下，名为 FullAWSAccess 的 SCP 将附加到每个根、OU 和账户。此默认 SCP 允许所有操作和服务。因此，在新组织中，在您开始创建或处理 SCP 之前，所有现有 IAM 权限仍会继续像以往一样运行。只要您将新的或修改后的 SCP 应用于包含账户的根或 OU，您的用户在该账户中拥有的权限将由 SCP 筛选。现在，如果层次结构的每个层到指定账户的 SCP 拒绝用于工作的权限，则这些权限可能被拒绝。

如果您在根中禁用 SCP 策略类型，则所有 SCP 都将自动从该根中的所有实体分离。如果您在该根中重新启用 SCP，则所有原始附加对象将丢失，并且所有实体将重置为仅附加到默认 FullAWSAccess SCP。

有关 SCP 的语法的详细信息，请参阅 [SCP 语法 \(p. 68\)](#)。

有关使用 SCP 的策略

您可以将组织中的 SCP 配置为用作以下任一项：

- [拒绝列表 \(p. 58\)](#) – 默认情况下允许操作，并且您指定禁止哪些服务和操作。
- [允许列表 \(p. 59\)](#) – 默认情况下禁止操作，并且您指定允许哪些服务和操作。

Tip

您可在 [IAM](#) 中，使用[服务上次访问数据](#)来更新 SCP，以将访问限制为仅您需要的 AWS 服务。有关更多信息，请参阅 IAM 用户指南 中的[为组织查看组织服务上次访问数据](#)。

将 SCP 用作拒绝列表

AWS Organizations 的默认配置支持将 SCP 用作拒绝列表。利用拒绝列表策略，账户管理员可以委派所有服务和操作，直到您创建并附加一个 SCP，它将拒绝一项特定服务或一组操作。拒绝语句需要较少的维护，因为在 AWS 添加新服务时不需要更新它们。拒绝语句通常使用较少的空间，因此更容易保持在 [SCP 大小限制 \(p. 96\)](#) 内。在 Effect 元素具有值 Deny 的语句中，您还可以限制对特定资源的访问，或者定义 SCP 何时生效的条件。

为了支持此操作，在创建每个根和 OU 时，AWS Organizations 会将一个名为 [FullAWSAccess](#) 的 AWS 托管 SCP 附加到该根和 OU。此策略允许所有服务和操作。您始终能够根据需要将它附加到您组织中的实体或从这些实体分离。由于该策略是 AWS 托管 SCP，因此它无法修改或删除。该策略看上去如下所示。

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

该策略使账户管理员可以委派任何服务或操作的权限，直到您创建并附加拒绝访问的 SCP 为止。您可以附加一个 SCP，该 SCP 显式禁止您不希望某些账户中的用户和角色执行的操作。

此类策略可能与以下示例类似，可阻止受影响账户中的用户对 Amazon DynamoDB 服务执行任何操作。组织管理员可以分离 FullAWSAccess 策略并改为附加此策略。此 SCP 仍允许所有其他服务及其操作。

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

受影响账户中的用户无法执行 DynamoDB 操作，因为第二个语句中的显式 Deny 元素将覆盖第一个语句中的显式 Allow。您也可以通过以下方式配置此设置：保留 FullAWSAccess 策略，然后附加另一个仅包含 Deny 语句的策略，如下所示。

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

```
{
  "Effect": "Deny",
  "Action": "dynamodb:*",
  "Resource": "*"
}
```

应用于根或 OU 的上一个 DynamoDB 策略中的 FullAWSAccess 策略和 Deny 语句的组合拥有与同时包含这两个语句的单个策略相同的作用。将会合并指定级别应用的所有策略。每个语句，无论源自哪个策略，都将根据前面讨论的规则进行评估（即，显式 Deny 覆盖显式 Allow，后者覆盖默认的隐式 Deny）。

将 SCP 用作允许列表

要将 SCP 用作允许列表，您必须将 AWS 托管 FullAWSAccess SCP 替换为一个仅明确允许您希望允许的服务和操作的 SCP。一旦删除默认 FullAWSAccess SCP，现在将隐式拒绝所有服务的所有操作。随后，仅对于您希望允许的操作，您的自定义 SCP 将使用显式 Deny 覆盖隐式 Allow。对于要为指定账户启用的某个权限，通过每个 OU 使用账户的直接路径从根提供的每个 SCP 甚至是附加到账户的 SCP 都必须允许该权限。

允许列表策略可能与以下示例类似，可允许账户用户为 Amazon EC2 和 Amazon CloudWatch 而非其他服务执行操作。父 OU 和根中的所有 SCP 还必须明确允许以下权限：

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

创建和更新 SCP

当使用权限登录到您组织的主账户时，您可以创建和更新[服务控制策略 \(SCP\)](#) (p. 54)。您可以通过构建拒绝或允许访问您指定的服务和操作的语句来创建 SCP。

使用 SCP 的默认配置是创建拒绝访问的语句。对于拒绝语句，您还可以为该语句指定资源和条件并使用 [NotAction](#) 元素。对于允许语句，您只能指定服务和操作。

有关拒绝访问和允许访问的语句的更多信息，请参阅 [有关使用 SCP 的策略](#) (p. 57)。

Tip

您可在 [IAM](#) 中，使用[服务上次访问数据](#)来更新 SCP，以将访问限制为仅您需要的 AWS 服务。有关更多信息，请参阅 IAM 用户指南 中的[为组织查看组织服务上次访问数据](#)。

创建 SCP

要创建 SCP，您必须拥有以下权限：

- `organizations:CreatePolicy`

要创建 SCP，请完成以下步骤。

创建服务控制策略（控制台）

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（**不推荐**）。
2. 在 Policies (策略) 选项卡上，选择 Create Policy (创建策略)。
3. 在 Create new policy (创建新策略) 页面上，输入策略的名称和描述。

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。利用 deny 语句，您可以进行额外的控制，因为您可以限制对特定资源的访问，定义 SCP 何时生效的条件并使用 [NotAction](#) 元素。有关更多信息，请参阅 [SCP 语法 \(p. 68\)](#)。

4. 要添加拒绝 访问的语句，请执行以下操作：

- a. 在 Policy (策略) 部分的左窗格中，选择要为其添加操作的服务。

当您选择左侧的选项时，右侧窗格将更新以显示 JSON 策略。您还可以在 Policy (策略) 部分的右侧窗格的编辑器中键入或粘贴策略，但此过程描述如何使用左侧的可视编辑器来构建 SCP。

- b. 从为该服务打开的可用操作的列表中，选择要拒绝的操作。

- c. 指定要包含在语句中的资源。

- 选择 Add resource (添加资源)。
- 在 Add resource (添加资源) 屏幕上，从列表中选择服务，然后选择 Resource type (资源类型)。输入 Resource ARN (资源 ARN)。
- 选择 Add resource (添加资源)。

Tip

需要资源元素。如果您要指定所选服务的所有资源，请在右窗格中编辑资源语句以读取 `"Resource": "*"。`

- d. 可选：要指定策略何时生效的条件，请选择 Add condition (添加条件)。对于所选服务，指定以下内容：

- 条件密钥 – 您可以指定适用于所有 AWS 服务的条件密钥（例如 `aws:SourceIp`）或服务特定的密钥（例如 `ec2:InstanceType`）。
- 限定词 –（可选）如果为条件输入多个值，则可指定 **限定词** 来针对值测试请求。
- 运算符 – 您可以使用 **运算符** 根据密钥与值的比较来限制访问。

对于 Null 条件之外的任何条件运算符，您可以选择 **IfExists** 选项。

- 值 –（可选）为条件指定一个或多个值。

选择 Add condition (添加条件)。

有关更多信息，请参阅 IAM 用户指南 中的 [IAM JSON 策略元素：Condition](#)。

- e. 可选：要使用 NotAction 元素来拒绝对所有列出的资源（指定操作除外）的访问，请将左窗格中的 Action 替换为 NotAction（位于 `"Effect": "Deny"`，元素的后面）。有关更多信息，请参阅 IAM 用户指南 中的 [IAM JSON 策略元素：NotAction](#)。

5. 要添加允许 访问的语句，请执行以下操作：

- a. 在 Policy (策略) 部分的右窗格中，将 `"Effect": "Deny"` 更改为 `"Effect": "Allow"`。
- b. 在 Policy (策略) 部分的左窗格中，选择要为其添加操作的服务。

当您选择左侧的选项时，右侧窗格将更新以显示 JSON 策略。您还可以在 Policy (策略) 部分的右侧窗格的编辑器中键入或粘贴策略，但此过程描述如何使用左侧的可视编辑器来构建 SCP。

- c. 从为该服务打开的可用操作的列表中，选择要允许的操作。
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. 添加完语句后，选择 [Create policy \(创建策略\)](#) 以保存已完成的 SCP。

您的新 SCP 会显示在组织的策略列表中。现在，您可以[将 SCP 附加到根、OU 或账户 \(p. 52\)](#)。

Note

SCP 在主账户和其他部分情况中不会生效。有关更多信息，请参阅 [不受 SCP 限制的任务和实体 \(p. 56\)](#)。

创建服务控制策略 (AWS CLI、AWS API)

您可以使用以下命令之一创建 SCP：

- AWS CLI：[aws organizations create-policy](#)
- AWS API：[CreatePolicy](#)

更新 SCP

当登录到您组织的主账户后，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。

要更新您的 AWS 组织中的策略，您必须拥有以下权限：

- `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 "*")。

更新策略 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录 ([不推荐](#))。
2. 选择 Policies 选项卡。
3. 选择要更新的策略。
4. 在右侧的详细信息窗格中，选择 Policy editor (策略编辑器)。
5. 选择 Edit (编辑) 启用策略更改。
6. 通过在右侧窗格中编辑策略来进行更改。对于拒绝语句，您还可以使用左窗格中的可视化编辑器来进行更改。完成后，选择 [Save changes \(保存更改\)](#)。

更新策略 (AWS CLI、AWS API)

可以使用以下命令之一来更新策略：

- AWS CLI：[aws organizations update-policy](#)
- AWS API：[UpdatePolicy](#)

了解更多信息

有关创建 SCP 的更多信息，请参阅以下页面：

- [示例服务控制策略 \(p. 62\)](#)
- [SCP 语法 \(p. 68\)](#)

示例服务控制策略

本主题中显示的示例[服务控制策略 \(SCP\)](#) (p. 54) 仅供参考。

在使用这些示例之前

尝试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它们。
- 请先测试您的策略，然后再在生产环境中使用它们。请记住，SCP 影响所附加到的每个账户中的每个用户和角色以及根用户。

Tip

您可在 [IAM](#) 中，使用[服务上次访问数据](#)来更新 SCP，以将访问限制为仅您需要的 AWS 服务。有关更多信息，请参阅 IAM 用户指南 中的[为组织查看组织服务上次访问数据](#)。

以下每个策略是[拒绝列表策略 \(p. 58\)](#)策略的示例。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 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。

主题

- [示例 1：阻止用户禁用 AWS CloudTrail \(p. 62\)](#)
- [示例 2：阻止用户禁用 Amazon CloudWatch 或变更其配置 \(p. 63\)](#)
- [示例 3：阻止用户删除 Amazon VPC 流日志 \(p. 63\)](#)
- [示例 4：阻止用户禁用 AWS Config 或更改其规则 \(p. 63\)](#)
- [示例 5：阻止还没有 Internet 访问权的任何 VPC 获取它 \(p. 64\)](#)
- [示例 6：根据请求的区域拒绝对 AWS 的访问 \(p. 64\)](#)
- [示例 7：防止 IAM 委托人进行某些更改 \(p. 65\)](#)
- [示例 8：防止 IAM 委托人进行某些更改（管理员除外）\(p. 65\)](#)
- [示例 9：要求对 Amazon S3 存储桶进行加密 \(p. 66\)](#)
- [示例 10：需要 Amazon EC2 实例以使用特定类型 \(p. 66\)](#)
- [示例 11：需要 MFA 以停止 Amazon EC2 实例 \(p. 67\)](#)
- [示例 12：限制根用户对 Amazon EC2 的访问 \(p. 67\)](#)

示例 1：阻止用户禁用 AWS CloudTrail

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 CloudTrail 日志。

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



```
}
```

示例 2：阻止用户禁用 Amazon CloudWatch 或变更其配置

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": "*"
    }
  ]
}
```

示例 3：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 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": "*"
    }
  ]
}
```

示例 4：阻止用户禁用 AWS Config 或更改其规则

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

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



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

示例 5：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": "*"
    }
  ]
}
```

示例 6：根据请求的区域拒绝对 AWS 的访问

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。要使用此 SCP，请将示例策略中的红色斜体文本替换为您自己的信息。

此策略将 [NotAction](#) 元素与 Deny 效果结合使用以拒绝对语句中未列出的所有操作的访问。列出的服务是 AWS 全局服务的示例，它们具有一个实际位于 us-east-1 区域的终端节点。如果将对 us-east-1 区域中的服务发出的请求包含在 NotAction 元素中，则不会拒绝该请求。对 us-east-1 区域中的服务发出的任何其他请求将被拒绝。

备注

- 此示例策略中未显示所有 AWS 全局服务。将用红色斜体文本表示的服务列表替换为由组织中的账户使用的全局服务。
- 此示例策略阻止对 AWS Security Token Service 全局终端节点 (sts.amazonaws.com) 的访问。要将 AWS STS 与此策略结合使用，请使用区域终端节点或将 "sts:*" 添加到 NotAction 元素。有关 AWS STS 终端节点的更多信息，请参阅 IAM 用户指南 中的 [在 AWS 区域中激活和停用 AWS STS](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAllOutsideEU",
      "Effect": "Deny",
      "NotAction": [
        "iam:*",
        "organizations:*",
        "route53:*"
      ]
    }
  ]
}
```

```
        "budgets:*",
        "waf:*",
        "cloudfront:*",
        "globalaccelerator:*",
        "importexport:*",
        "support:*"
    ],
    "Resource": "*",
    "Condition": {
        "StringNotEquals": {
            "aws:RequestedRegion": [
                "eu-central-1",
                "eu-west-1"
            ]
        }
    }
}
]
```

示例 7：防止 IAM 委托人进行某些更改

此 SCP 阻止账户中的 IAM 委托人对在组织的所有账户中创建的常见管理 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/role-to-deny"
      ]
    }
  ]
}
```

示例 8：防止 IAM 委托人进行某些更改（管理员除外）

此 SCP 基于前面的示例为管理员创建例外。它阻止账户中的 IAM 委托人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/role-to-deny"
    ],
    "Condition": {
        "StringNotLike": {
            "aws:PrincipalARN": "arn:aws:iam::*:role/role-to-allow"
        }
    }
}
]
}

```

示例 9：要求对 Amazon S3 存储桶进行加密

此 SCP 要求委托人在向 Amazon S3 存储桶写入时使用 AES256 加密。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyIncorrectEncryptionHeader",
      "Effect": "Deny",
      "Action": "s3:PutObject",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    },
    {
      "Sid": "DenyUnEncryptedObjectUploads",
      "Effect": "Deny",
      "Action": "s3:PutObject",
      "Resource": "*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": true
        }
      }
    }
  ]
}

```

示例 10：需要 Amazon EC2 实例以使用特定类型

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

```

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

```

```
    "Sid": "RequireMicroInstanceType",
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:InstanceType": "t2.micro"
      }
    }
  }
}
```

示例 11：需要 MFA 以停止 Amazon EC2 实例

使用如下所示的 SCP，要求先启用 Multi-Factor Authentication (MFA)，之后委托人或根用户才能停止 Amazon EC2 实例。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

示例 12：限制根用户对 Amazon EC2 的访问

以下策略限制账户中的[根用户](#)对 Amazon EC2 操作的所有访问。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"
          ]
        }
      }
    }
  ]
}
```

SCP 语法

服务控制策略 (SCP) 使用的语法与 IAM 权限策略和基于资源的策略 (例如 Amazon S3 存储桶策略) 使用的语法相似。有关 IAM 策略及其语法的更多信息, 请参阅 IAM 用户指南 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。它使用此页面上描述的元素。

Note

SCP 中的所有字符将计入其 [大小限制 \(p. 96\)](#)。本指南中的示例演示了使用额外空格编排格式的 SCP, 以提高其可读性。但如果您的策略大小接近限制, 则可以删除任何空格 (例如, 引号之外的空格字符和换行符) 来节省空间。

有关 SCP 的一般信息, 请参阅 [服务控制策略 \(p. 54\)](#)。

元素摘要

下表总结了可在 SCP 中使用的策略元素。一些策略元素仅在拒绝操作的 SCP 中可用。Supported Effects (支持的效果) 列中列出了可用于 SCP 中的每个策略元素的效果类型。

元素	目的	支持的效果
Version	指定要用于处理策略的语言语法规则。	Allow、Deny
Statement	充当策略元素的容器。您可以在 SCP 中拥有多个语句。	Allow、Deny
Statement ID (Sid)	(可选) 提供语句的友好名称。	Allow、Deny
效果	定义 SCP 语句是 允许 (p. 9) 还是 拒绝 (p. 9) 账户中的主要和根访问权限。	Allow、Deny
Action	指定 SCP 允许或拒绝的 AWS 服务/操作。	Allow、Deny
NotAction	指定不受 SCP 约束的 AWS 服务/操作。用来代替 Action 元素。	Deny

元素	目的	支持的效果
Resource	指定 SCP 应用于的 AWS 资源。	Deny
Condition	指定语句何时生效的条件。	Deny

以下部分提供了有关如何在 SCP 中使用策略元素的更多信息和示例。

Version 元素

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

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

Statement 元素

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

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

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

以下示例包括作为一个 Statement 元素中的数组列表的两个语句。第一条语句允许所有操作，第二条语句拒绝任何 EC2 操作。结果是账户中的管理员可以委派除了 EC2 的权限之外的任意权限：

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

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": "*"
  }
}
```

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。

"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。结果是它[允许 \(p. 9\)](#)任何附加账户的 Amazon S3 权限：

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

即使它使用与 IAM 权限策略相同的 Allow 值关键字，在 SCP 中它也不会实际授予用户执行任何操作的权限。相反，SCP 指定组织、组织单位 (OU) 或账户的最大权限数。在前面的示例中，即使账户中的用户已经附加了 AdministratorAccess 托管策略，SCP 也会将账户中的所有用户限制为只能执行 Amazon S3 操作。

"Effect": "Deny"

在 Effect 元素具有值 Deny 的语句中，您还可以限制对特定资源的访问，或者定义 SCP 何时生效的条件。

以下显示了有关如何在拒绝语句中使用条件密钥的示例。

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

SCP 中的此语句设置一个防护机制来阻止受影响的账户（其中，SCP 附加到账户本身或包含该账户的组织根或 OU）启动 Amazon EC2 实例（如果 Amazon EC2 实例未设置为 t2.micro）。即使将允许此操作的 IAM 策略附加到账户，SCP 所创建的防护机制也会阻止它。

Action 和 NotAction 元素

每个语句必须包含下列项目之一：

- 在允许和拒绝语句中，为 Action 元素。

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

Action 或 NotAction 元素的值为字符串的列表（JSON 数组），用于标识语句所允许或拒绝的 AWS 服务和操作。

所有字符串均包含服务简写（例如“s3”、“ec2”、“iam”或“organizations”），全小写，后跟冒号，然后是该服务的操作。这些操作和通知区分大小写，必须按照各个服务的文档中所示键入。通常，其键入方式为每个单词的开头是大写字母，其余为小写字母。例如：“s3:ListAllMyBuckets”。

您还可以使用星号作为通配符，匹配名称中包含相同部分的多个操作。值 “s3:*” 表示 Amazon S3 服务中的所有操作。值 “ec2:Describe*” 仅与以“Describe”开头的 EC2 操作匹配。

Note

在 SCP 中，Action 或 NotAction 元素中的通配符 (*) 字符只能由自身使用或用在字符串结尾处。它不能出现在字符串的开头或中间部分。因此，“servicename:action*” 是有效的，但 “servicename:*action” 和 “servicename:some*action” 在 SCP 中都是无效的。

有关 AWS Organizations SCP 和 IAM 权限策略中均支持的所有服务和操作的列表，请参阅 IAM 用户指南 中的 [AWS 服务的操作、资源和条件密钥](#)。

Action 元素的示例

以下示例演示带有一条语句的 SCP，该语句允许账户管理员在账户中委派 EC2 实例的描述、启动、停止和终止权限。这是一个 [允许列表 \(p. 9\)](#) 示例，这在未附加默认 Allow * 策略时非常有用，这种情况下将默认隐式拒绝权限。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 \(p. 9\)](#)您不希望用于所附加账户中的服务。它假定默认 "Allow *" SCP 仍附加到所有 OU 和根。此示例策略阻止所附加账户中的账户管理员委派 IAM、Amazon EC2 和 Amazon RDS 服务的任何权限。只要没有其他已附加策略拒绝，就可以委派来自其他服务的任何操作：

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

NotAction 元素的示例

以下示例说明如何使用 NotAction 元素来控制对服务的所有资源的区域的访问。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireBucketsInUSWest1",
      "Effect": "Deny",
      "NotAction": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
        }
      }
    }
  ]
}
```

利用此语句，受影响的账户仅限于创建指定区域的 Amazon S3 存储桶。

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 (ARN)。

在 Effect 元素具有值 Deny 的语句中，您可以指定单个 ARN，如下示例所示。

```
{
  "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 阻止账户中的 IAM 委托人对在组织的所有账户中创建的常见管理 IAM 角色进行更改。

Condition 元素

您可以在 SCP 中的拒绝语句中指定 Condition 元素。例如：

```
{
  "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。

不支持的元素

SCP 中不支持以下元素：

- Principal
- NotPrincipal
- NotResource

标记 AWS Organizations 资源

标签 是自定义的属性标签，您将其添加到 AWS 资源以便更轻松地确定、组织和搜索资源。每个标签具有两个部分：

- 标签键（例如，CostCenter、Environment 或 Project）。标签键区分大小写。
- 标签值（例如，111122223333 或 Production）。您可以将标签的值设为空的字符串，但是不能将其设为空值。省略标签值与使用空字符串相同。与标签键一样，标签值区分大小写。

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 [AWS 标记策略](#)。

AWS Organizations 中支持的资源

当前，在以主账户登录时，AWS Organizations 支持以下标记操作：

- 您可在 AWS Organizations 中标记和取消标记账户。
- 您可以查看 AWS Organizations 中账户上的标签。

AWS Organizations 当前不支持账户中的标记资源，或者 AWS Identity and Access Management (IAM) 的基于标签的访问控制功能。

添加标签

在以具有组织主账户权限的身份登录时，您可以将标签添加到组织中的账户。

最小权限

要将标签添加到组织中的账户，您必须拥有以下权限：

- `organizations:ListTagsForResource` (仅限控制台)
- `organizations:TagResource`

将标签添加到组织的账户中（控制台）

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。
2. 在账户选项卡上，选择账户。
3. 在右侧详细信息窗格标签部分，选择编辑标签。
4. 输入标签的键和（可选）值。

标签键和值要区分大小写。为希望标准化的标签使用大写字母。

5. 选择 Save changes。

您添加到账户的任何标签显示在右侧详细信息窗格的标签部分中。

将标签添加到组织的账户中（AWS CLI、AWS API）

您可以使用以下命令之一将标签添加到账户：

- AWS CLI : [aws organizations tag-resource](#)
- AWS API : [TagResource](#)

查看账户上的标签

在以具有组织主账户权限的身份登录时，您可以查看组织中账户上的标签。

最小权限

要查看组织中账户上的标签，您必须拥有以下权限：

- `organizations:ListTagsForResource`

查看组织中的账户上的标签（控制台）

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。
2. 在账户选项卡上，选择账户。
3. 在右侧详细信息窗格中，找到标签部分。

此处显示附加到所选账户的所有标签。

查看组织中的账户上的标签（AWS CLI、AWS API）

您可以使用以下命令之一查看账户上的标签：

- AWS CLI : [aws organizations list-tags-for-resource](#)
- AWS API : [ListTagsForResource](#)

编辑标签值

在以具有组织主账户权限的身份登录时，您可以编辑附加到账户上标签的标签值。

要编辑标签键，您需要删除该标签键，然后添加一个新的标签键。有关更多信息，请参阅 [删除标签 \(p. 76\)](#) 和 [添加标签 \(p. 74\)](#)。

最小权限

要对附加到账户的标签编辑标签值，您必须拥有以下权限：

- `organizations:ListTagsForResource`
- `organizations:TagResource`

编辑组织中账户标签的标签值（控制台）

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录（[不推荐](#)）。
2. 在账户选项卡上，选择账户。
3. 在右侧详细信息窗格标签部分，选择编辑标签。
4. 修改要更改的标签的值。

5. 选择 Save changes。

右侧详细信息窗格中的标签部分将进行更新，显示您对账户中标签的标签值所进行的任何更改。

编辑组织中账户的标签值 (AWS CLI、AWS API)

1. 使用以下命令之一删除现有标签值：
 - AWS CLI : [aws organizations untag-resource](#)
 - AWS API : [UntagResource](#)
2. 使用以下命令之一添加新标签值：
 - AWS CLI : [aws organizations tag-resource](#)
 - AWS API : [TagResource](#)

删除标签

在以具有组织主账户权限的身份登录时，您可以删除附加到您组织中账户的标签。

最小权限

要删除标签，您必须拥有以下权限：

- `organizations:ListTagsForResource`
- `organizations:UntagResource`

从组织的账户中删除标签 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。您必须以 IAM 用户的身份登录，代入 IAM 角色，或在组织的主账户中以根用户的身份登录 ([不推荐](#))。
2. 在账户选项卡上，选择账户。
3. 在右侧详细信息窗格标签部分，选择编辑标签。
4. 选择要删除的标签旁的删除。
5. 选择 Save changes。

详细信息窗格中的标签部分不再显示已经删除的标签。

从组织的账户中删除标签 (AWS CLI、AWS API)

您可以使用以下命令之一删除标签：

- AWS CLI : [aws organizations untag-resource](#)
- AWS API : [UntagResource](#)

启用其他 AWS 服务的可信访问

您可以使用可信访问 启用您指定的名为可信服务 的 AWS 服务，以执行您的组织及其代表您的账户中的任务。这涉及向可信服务授予权限，但不会以其他方式影响 IAM 用户或角色的权限。当您允许访问时，可信服务可以在您组织的每个账户中创建一个名为服务相关角色的 IAM 角色。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。可信服务按需异步创建角色，并非所有组织账户都需要。

Important

建议您通过使用可信服务的控制台、AWS CLI 或某个 [AWS 开发工具包](#) 中的 API 操作允许可信访问。这使可信服务能够执行任何所需初始化或创建任何所需资源。要了解可信服务执行的配置，请参阅该服务的文档。

允许可信访问所需的权限

可信访问需要以下两种服务的权限：AWS Organizations 和可信服务。要允许可信访问，请选择以下场景之一：

- 如果您有在 AWS Organizations 和可信服务中都具有权限的凭证，则通过使用可信服务中提供的工具（控制台或 AWS CLI）允许访问。这允许可信服务代表您在 AWS Organizations 中允许可信访问以及创建此服务在您的组织中运行所需的任何资源。

这些凭证的最低权限如下：

- `organizations:EnableAWSServiceAccess`。您还可以将 `organizations:ServicePrincipal` 条件键与此操作一起使用以将这些操作发出的请求限制为已批准的服务委托名称列表。有关更多信息，请参阅 [条件键](#) (p. 86)。
- `organizations:ListAWSServiceAccessForOrganization` – 当您使用 AWS Organizations 控制台时必需。
- 可信服务所需的最低权限取决于此服务。有关更多信息，请参阅可信服务的文档。
- 如果一人拥有在 AWS Organizations 中具有权限的凭证，但其他人拥有在可信服务中具有权限的凭证，请按以下顺序执行这些步骤：
 - 拥有在 AWS Organizations 中具有权限的凭证的人应使用 AWS Organizations 控制台、AWS CLI 或 AWS 开发工具包允许可信服务的可信访问。这为另一服务授予在执行以下步骤 (步骤 2) 后在组织中执行其所需配置的权限。

最低 AWS Organizations 权限如下：

- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization` – 仅当您使用 AWS Organizations 控制台时必需

有关在 AWS Organizations 中允许可信访问的步骤，请参阅 [如何允许或禁止可信访问](#) (p. 78)。

- 拥有在可信服务中具有权限的凭证的人可启用此服务以使用 AWS Organizations。这指示此服务执行任何所需初始化 (如，创建可信服务在组织中运行所需的任何资源)。有关信息，请参阅 [在您的组织中支持可信访问的服务](#) (p. 79) 处的服务特定说明。

禁止可信访问所需的权限

当您不再需要允许可信服务在您的组织或其账户上运行时，请选择以下场景之一。

Important

禁止可信服务访问不会阻止具有相应权限的用户和角色使用该服务。要完全阻止用户和角色访问 AWS 服务，您可以删除授予此访问权限的 IAM 权限，也可以使用 AWS Organizations 中的 [服务控制策略 \(SCP\)](#) (p. 54)。

- 如果您有在 AWS Organizations 和可信服务中都具有权限的凭证，则可通过使用为可信服务提供的工具（控制台或 AWS CLI）禁止访问。该服务之后将通过删除不再需要的资源并代表您在 AWS Organizations 中禁止此服务的可信访问来清理。

这些凭证的最低权限如下：

- `organizations:DisableAWSServiceAccess`。您还可以将 `organizations:ServicePrincipal` 条件键与此操作一起使用以将这些操作发出的请求限制为已批准的服务委托人名称列表。有关更多信息，请参阅 [条件键](#) (p. 86)。
- `organizations:ListAWSServiceAccessForOrganization` – 当您使用 AWS Organizations 控制台时必需。
- 可信服务所需的最低权限取决于此服务。有关更多信息，请参阅可信服务的文档。
- 如果在 AWS Organizations 中具有权限的凭证不是在可信服务中具有权限的凭证，请按以下顺序执行这些步骤：
 1. 在可信服务中具有权限的人首先使用此服务禁止访问。这将指示可信服务通过删除可信服务所需的资源进行清理。有关信息，请参阅 [在您的组织中支持可信访问的服务](#) (p. 79) 处的服务特定说明。
 2. 在 AWS Organizations 中具有权限的人之后可使用 AWS Organizations 控制台、AWS CLI 或 AWS 开发工具包禁止可信服务的访问。这将从组织及其账户中删除可信服务的权限。

最低 AWS Organizations 权限如下：

- `organizations:DisableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization` – 仅当您使用 AWS Organizations 控制台时必需

有关在 AWS Organizations 中禁止可信访问的步骤，请参阅 [如何允许或禁止可信访问](#) (p. 78)。

如何允许或禁止可信访问

如果您只有 AWS Organizations 的权限并且要代表另一 AWS 服务的管理员允许或禁止对您组织的可信访问，请使用以下过程。

允许或禁止可信服务访问 (控制台)

1. 通过 <https://console.aws.amazon.com/organizations/> 登录 组织 控制台。
2. 在右上角，选择 Settings (设置)。
3. 如果您要允许 访问，可继续下一步。如果您要禁止 访问，请一直等到管理员告知您已禁用此服务且已清理资源。
4. 在 AWS 服务的可信访问部分中，找到您需要的服务，然后酌情选择允许访问或禁止访问。
5. 如果您要允许 访问，请告知另一 AWS 服务的管理员，他们现在可以启用另一服务以使用 AWS Organizations。

允许或禁止可信服务访问 (AWS CLI、AWS API)

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

- AWS CLI : `aws organizations enable-aws-service-access`

- AWS CLI : `aws organizations disable-aws-service-access`
- AWS API : [EnableAWSServiceAccess](#)
- AWS API : [DisableAWSServiceAccess](#)

AWS Organizations 和服务相关角色

AWS Organizations 使用 [IAM 服务相关角色](#) 允许可信服务代表您执行组织的成员账户中的任务。当您配置可信服务并授权其与您的组织集成时，该服务可请求 AWS Organizations 在其成员账户中创建服务相关角色。可信服务按需异步执行此操作，同时并非所有组织账户都需要。此服务相关角色具有预定义的 IAM 权限，此权限允许可信服务执行账户内的特定任务。一般而言，AWS 将管理所有服务相关角色，这意味着，您通常无法更改角色或附加的策略。

为实现上述操作，当您在组织中创建账户或接受邀请以将现有账户加入组织时，AWS Organizations 将使用名为 `AWSServiceRoleForOrganizations` 的服务相关角色预置账户。仅 AWS Organizations 服务自身可以代入此角色。此角色具有仅允许 AWS Organizations 为其他 AWS 服务创建服务相关角色的权限。此服务相关角色存在于所有组织中。

如果您的组织仅启用了 [整合账单功能 \(p. 8\)](#) (但我们建议不要这样做)，则绝不使用名为 `AWSServiceRoleForOrganizations` 的服务相关角色并且可删除它。如果您之后要在组织中启用 [所有功能 \(p. 8\)](#)，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 `iam:CreateServiceLinkedRole` `AWSServiceRoleForOrganizations` 权限。如果 `AWSServiceRoleForOrganizations` 角色已存在，则管理员只需 `organizations:AcceptHandshake` 权限即可同意该请求。如果此管理员同意此请求，则 AWS Organizations 将创建服务相关角色 (如果此角色尚不存在)。
- 对于已在组织中创建 的每个成员账户 – 账户管理员将收到重新创建服务相关角色的请求。(成员账户的管理员不会收到启用所有功能的请求，因为主账户的管理员被视为所创建成员账户的所有者。) 如果成员账户管理员同意该请求，则 AWS Organizations 将创建服务相关角色。管理员必须同时具有 `organizations:AcceptHandshake` 和 `iam:CreateServiceLinkedRole` 权限才能成功接受握手。

在组织中启用所有功能后，您无法再删除任何账户中的 `AWSServiceRoleForOrganizations` 服务相关角色。

Important

AWS Organizations SCP 决不会影响服务相关角色。这些角色将免受任何 SCP 限制。

在您的组织中支持可信访问的服务

以下各节介绍了您可在组织中允许其的可信访问的 AWS 服务。每个部分包括以下内容：

- 可信服务以及此服务在您允许可信访问时如何运行的摘要
- 指向在组织中允许和禁止可信访问的说明的链接
- 您可在策略中指定的可信服务的委托人名称，以授予对组织中账户的可信访问权限
- 如果适用，允许可信访问时在所有账户中创建的 IAM 服务相关角色的名称

有关将其他 AWS 服务与 组织 结合使用的好处，请参阅 [可与 AWS Organizations 一起使用的 AWS 服务 \(p. 3\)](#)。

AWS Artifact 和 AWS Organizations

AWS Artifact 是一项使您能够下载 AWS 安全合规性报告（如 ISO 和 PCI 报告）的服务。使用 AWS Artifact，主账户中的用户可以代表组织中的所有成员账户自动接受协议，即使添加了新的报告和账户也是如此。成员账户用户可以查看和下载协议。有关 AWS Artifact 的详细信息，请参阅 [AWS Artifact 用户指南](#)。

以下列表提供您希望集成 AWS Artifact 和 组织 时要了解的有关信息：

- 允许对 AWS Organizations 的可信访问：您必须使用您的 AWS Organizations 主账户登录，才能在组织内配置一个账户作为 AWS Artifact 管理员账户。有关信息，请参阅 AWS Artifact 用户指南 中的 [步骤 1：创建管理员组并添加 IAM 用户](#)。
- 禁止对 AWS Organizations 的可信访问：AWS Artifact 需要对 AWS Organizations 的可信访问才能处理组织协议。如果您在将 AWS Artifact 用于组织协议时使用 AWS Organizations 禁止可信访问，则它将停止正常运行，因为它无法访问组织。您在 AWS Artifact 中接受的任何组织协议都将保留，但 AWS Artifact 无法访问它们。AWS Artifact 创建的 AWS Artifact 角色将会保留。如果您之后重新允许可信访问，则 AWS Artifact 将继续像以前一样运行，而无需您重新配置该服务。

从组织中删除的独立账户不再有权访问任何组织协议。

- AWS Artifact 的服务委托人名称：`aws-artifact-account-sync.amazonaws.com`。
- 为与 AWS Artifact 同步创建的角色名称：`AWSArtifactAccountSync`。

AWS CloudTrail 和 AWS Organizations

AWS CloudTrail 是一项 AWS 服务，可帮助对您的 AWS 账户进行监管、合规性检查、操作审核和风险审核。使用 AWS CloudTrail，主账户中的用户可以创建组织跟踪，记录该组织中所有 AWS 账户的所有事件。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，成员账户无权访问 Amazon S3 存储桶中组织跟踪的日志文件。这有助于您在组织的账户中统一应用和实施事件日志记录策略。有关更多信息，请参阅 AWS CloudTrail User Guide 中的 [为组织创建跟踪](#)。

以下列表提供了将 AWS CloudTrail 与 AWS Organizations 集成所需的信息：

- 允许对 AWS Organizations 的可信访问：您必须使用 AWS Organizations 主账户登录以创建组织跟踪。如果您从 AWS CloudTrail 控制台创建跟踪，则自动为您配置可信访问。如果您选择使用 AWS CLI 或 AWS API 创建组织跟踪，则必须手动配置可信访问。有关更多信息，请参阅 AWS CloudTrail User Guide 中的 [启用 CloudTrail 作为 AWS Organizations 中的可信访问](#)。
- 禁止对 AWS Organizations 的可信访问：AWS CloudTrail 需要对 AWS Organizations 的可信访问才能处理组织跟踪。如果您在将 AWS CloudTrail 用于组织跟踪时使用 AWS Organizations 禁止可信访问，则对于成员账户将停止跟踪，因为 CloudTrail 无法访问组织。组织跟踪继续，与创建 `AWSServiceRoleForCloudTrail` 角色以用于 CloudTrail 与 AWS Organizations 之间的集成一样。如果您重新允许可信访问，则 CloudTrail 将继续像以前一样运行，而无需您重新配置跟踪。
- AWS CloudTrail 的服务委托人名称：`cloudtrail.amazonaws.com`。
- 为与 AWS CloudTrail 同步创建的角色名称：`AWSServiceRoleForCloudTrail`。

AWS Config 和 AWS Organizations

AWS Config 中多账户、多区域数据聚合使您能够将多个账户和 AWS 区域中的 AWS Config 数据聚合到单个账户中。多账户、多区域数据聚合用于中心 IT 管理员监控企业中多个 AWS 账户的合规性。聚合器是 AWS Config 中的一种资源类型，用于从多个源账户和区域收集 AWS Config 数据。在要查看聚合 AWS Config 数据的区域中创建聚合器。创建聚合器时，您可以选择添加独立账户 ID 或您的组织。有关 AWS Config 的更多信息，请参阅 [AWS Config Developer Guide](#)。

您还可以使用 [AWS Config API](#) 在组织中跨所有 AWS 账户来管理 AWS Config 规则。有关更多信息，请参阅 AWS Config Developer Guide 中的 [跨组织内的所有账户启用 AWS Config 规则](#)。

以下列表提供您希望集成 AWS Config 和 AWS Organizations 时要了解的有关信息：

- 允许对 AWS Organizations 的可信访问：要通过 AWS Config 允许对 AWS Organizations 的可信访问，请创建多账户聚合器并添加组织。有关如何配置多账户聚合器的信息，请参阅 AWS Config Developer Guide 中的[使用控制台设置聚合器](#)。
- 服务委托人名称
 - 对于 AWS Config：config.amazonaws.com
 - 对于 AWS Config 规则：config-multiaccountsetup.amazonaws.com
- 允许可信访问时可在账户中创建的 IAM 服务相关角色的名称
 - 对于 AWS Config：AWSConfigRoleForOrganizations
 - 对于 AWS Config 规则：AWSServiceRoleForConfigMultiAccountSetup

AWS Directory Service 和 AWS Organizations

Microsoft Active Directory 版 AWS Directory Service 或 AWS Managed Microsoft AD 可使您以托管服务的形式运行 Microsoft Active Directory (AD)。通过 AWS Directory Service 可轻松在 AWS Cloud 中设置和运行目录，或将 AWS 资源与现有的本地 Microsoft Active Directory 相连。AWS Managed Microsoft AD 还可与 AWS Organizations 进行紧密集成，以实现在多个 AWS 账户和某一地区内的任意 VPC 内实现目录的无缝分享。有关更多信息，请参阅[AWS Directory Service Administration Guide](#)。

以下列表提供您希望集成 AWS Directory Service for Microsoft Active Directory (企业版) 和 AWS Organizations 时要了解的有关信息：

- 要通过 AWS Organizations 启用可信访问：AWS Directory Service 需要可对 AWS Organizations 进行可信访问后才能与您的组织内的账户分享 Microsoft AD directory。若要了解更多信息，请参阅 AWS Directory Service Administration Guide 中的[分享目录](#)。
- 禁止通过 AWS Organizations 进行可信访问：如果在使用 AWS Directory Service 时禁止使用 AWS Organizations 进行可信访问，所有先前共享的目录会继续正常运行。但是，在重新启用可信访问前，您将无法再在组织内共享新目录。
- AWS Directory Service 的服务委托人名称：ds.amazonaws.com。

AWS Firewall Manager 和 AWS Organizations

AWS Firewall Manager 是一种安全管理服务，用于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。通过使用 AWS Firewall Manager，您可跨 AWS 组织中的所有账户一次推出针对应用程序负载均衡器和 Amazon CloudFront 分配的 AWS WAF 规则。使用 AWS Firewall Manager 一次设置好防火墙规则，并让它们跨组织中的所有账户和资源自动应用，即使添加新资源和账户时也是如此。有关 AWS Firewall Manager 的更多信息，请参阅[AWS 防火墙开发人员指南](#)。

以下列表提供您希望集成 AWS Firewall Manager 和 AWS Organizations 时要了解的有关信息：

- 允许对 AWS Organizations 的可信访问：您必须使用您的 AWS Organizations 主账户登录，才能在组织内配置一个账户作为 AWS Firewall Manager 管理员账户。有关信息，请参阅 AWS Firewall Manager 开发人员指南中的[步骤 2：设置 AWS Firewall Manager 管理员账户](#)。
- 禁止对 AWS Organizations 的可信访问：您可以按照 AWS Firewall Manager 开发人员指南中的[指定另一个账户作为 AWS Firewall Manager 管理员账户](#)中的说明更改或撤销 AWS Firewall Manager 管理员账户。如果您撤销此管理员账户，则必须登录 AWS Organizations 主账户并为 AWS Firewall Manager 设置一个新的管理员账户。
- AWS Firewall Manager 的服务委托人名称：fms.amazonaws.com。
- 允许可信访问时可在账户中创建的 IAM 服务相关角色的名称：AWSServiceRoleForFMS。

AWS License Manager 和 AWS Organizations

AWS License Manager 简化将软件供应商的许可证迁移到云中的过程。当您在 AWS 上构建云基础设施时，您可以通过使用自带许可 (BYOL) 机会来节省成本，也就是说，可以通过重新利用现有许可证库存以便与云资源一起使用来节省成本。通过基于规则的许可证消耗控制，管理员可以对新的和现有的云部署设置硬限制或软限制，在发生不合规的服务器之前停止使用它。通过将 AWS License Manager 与 AWS Organizations 相关联，您可以在整个组织中启用计算资源的跨账户发现。有关 AWS License Manager 的更多信息，请参阅 [AWS License Manager 指南](#)。

以下列表提供您希望集成 AWS License Manager 和 AWS Organizations 时要了解的有用信息：

- 使用 AWS Organizations 启用可信访问：您必须使用 AWS Organizations 主账户登录以将其与您的 AWS License Manager 账户关联，然后配置您的 License Manager 设置。有关信息，请参阅[配置 AWS License Manager 指南设置](#)。
- AWS License Manager 的服务委托人名称：`license-manager.amazonaws.com` 和 `license-manager.member-account.amazonaws.com`。
- 启用可信访问时可在账户中创建的 IAM 服务相关角色的名称：`AWSLicenseManagerMasterAccountRole`、`AWSLicenseManagerMemberAccountRole` 和 `AWSServiceRoleForAWSLicenseManagerRole`。

有关更多信息，请参阅[使用 License Manager-主账户角色](#)和[使用 License Manager-成员账户角色](#)。

AWS RAM 和 AWS Organizations

AWS Resource Access Manager (AWS RAM) 可让您与其他 AWS 账户共享您指定的 AWS 资源。这是一种集中式服务，跨多个账户为共享不同类型的 AWS 资源提供一致的体验。有关 AWS RAM 的更多信息，请参阅[AWS RAM 用户指南](#)。

以下列表提供了将 AWS RAM 与 AWS Organizations 集成所需的信息：

- 使用 AWS Organizations 启用可信访问：从 AWS RAM CLI 中，使用 `enable-sharing-with-aws-organizations` 命令。有关更多信息，请参阅 AWS RAM 用户指南中的[共享您的资源](#)。
- AWS RAM 的服务委托人名称：`ram.amazonaws.com`。
- 允许可信访问时可在账户中创建的 IAM 服务相关角色的名称：`AWSResourceAccessManagerServiceRolePolicy`。

AWS Service Catalog 和 AWS Organizations

AWS Service Catalog 可让您创建和管理获准在 AWS 上使用的 IT 服务的目录。AWS Service Catalog 与 AWS Organizations 的集成简化了在整个组织中产品组合的共享和产品的复制。AWS Service Catalog 管理员可以在共享产品组合时在 AWS Organizations 中引用现有组织，而且可以与组织的树结构中的任何可信组织单元 (OU) 共享产品组合。这样就不再需要共享产品组合，并且在导入产品组合时不再需要接收账户手动引用产品组合 ID。通过此机制共享的产品组合在 AWS Service Catalog 中的管理员 Imported Portfolio (导入的产品组合) 视图的共享到账户中列出。有关 AWS Service Catalog 的更多信息，请参阅 [AWS Service Catalog Administrator Guide](#)。

以下列表提供您希望集成 AWS Service Catalog 和 AWS Organizations 时要了解的有用信息：

- 使用 AWS Organizations 启用可信访问：调用 `AWSServiceCatalog::EnableAWSOrganizationsAccess` 操作或从 [AWS Service Catalog 控制台](#) 的 Portfolio Sharing (产品组合共享) 页面执行此操作。有关更多信息，请参阅 AWS Service Catalog Administrator Guide 中的[产品组合共享](#)。

使用 AWS Organizations 禁用可信访问：调用 `AWSServiceCatalog::DisableAWSOrganizationsAccess` 操作或从 [AWS Service Catalog 控制台](#) 的 Portfolio Sharing (产品组合共享) 页面执行此操作。如果在使用

AWS Service Catalog 时使用 AWS Organizations 禁用可信访问，则它不会删除当前共享，但会阻止您在整个组织中创建新共享。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。

AWS Service Catalog 的服务委托人名称：`servicecatalog.amazonaws.com`。

Service Quotas 和 AWS Organizations

Service Quotas 是一项 AWS 服务，可让您从中心位置查看和管理您的配额。配额，也称为限制，是 AWS 账户中资源、操作和项目的最大值。当 Service Quotas 与 AWS Organizations 关联时，您可以创建一个配额请求模板，以在创建账户时自动请求提升配额。有关 Service Quotas 的更多信息，请参阅 [Service Quotas 用户指南](#)。

以下列表提供了您希望关联 Service Quotas 和 AWS Organizations 时要了解的实用信息：

- 要使用 AWS Organizations 启用可信访问：使用您的 AWS Organizations 主账户登录，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 Quota 模板](#)。
- 您也可以调用 [AssociateServiceQuotaTemplate](#) 操作。有关更多信息，请参阅 [Service Quotas API 参考](#)。
- 要使用 AWS Organizations 禁用可信访问：调用 [DisableAWSServiceAccess](#) 操作。
- Service Quotas 的服务委托人名称：`servicequotas.amazonaws.com`。
- 允许可信访问时可在账户中创建的 IAM 服务相关角色的名称：`AWSServiceRoleForServiceQuotas`。

AWS Single Sign-On 和 AWS Organizations

AWS Single Sign-On (AWS SSO) 为您的所有 AWS 账户和云应用程序提供单一登录服务。它通过 AWS Directory Service 与 Microsoft Active Directory 连接，以允许该目录中的用户使用其现有 Active Directory 用户名和密码登录个性化的用户门户。在该门户中，用户有权访问您在门户中提供的所有 AWS 账户和云应用程序。有关 AWS SSO 的更多信息，请参阅 [AWS Single Sign-On 用户指南](#)。

以下列表提供您希望集成 AWS SSO 和 AWS Organizations 时要了解的有用信息：

- 允许对 AWS Organizations 的可信访问：AWS SSO 需要对 AWS Organizations 的可信访问才能正常运行。在设置 AWS SSO 时允许可信访问。有关更多信息，请参阅 AWS Single Sign-On 用户指南中的 [入门 - 步骤 1：启用 AWS Single Sign-On](#) 部分。
- 禁止对 AWS Organizations 的可信访问：AWS SSO 需要对 AWS Organizations 的可信访问才能正常运行。如果您在使用 AWS SSO 时使用 AWS Organizations 禁止可信访问，则它将不再正常运行，因为它无法访问组织。用户无法使用 AWS SSO 访问账户。AWS SSO 创建的所有角色均将保留，但 AWS SSO 服务无法访问这些角色。AWS SSO 服务相关角色也将保留。如果您重新允许可信访问，则 AWS SSO 将继续像以前一样运行，而无需您重新配置该服务。

如果您删除组织中的某个账户，则 AWS SSO 将自动清除任何元数据和资源（例如，所删除账户的服务相关角色）。从组织中删除的独立账户将无法再与 AWS SSO 配合使用。

- AWS SSO 的服务委托人名称：`sso.amazonaws.com`。
- 允许可信访问时可在账户中创建的 IAM 服务相关角色的名称：`AWSServiceRoleForSSO`。

有关更多信息，请参阅 AWS Single Sign-On 用户指南中的 [对 AWS SSO 使用服务相关角色](#)。

AWS Organizations 中的安全性

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

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

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。作为 [AWS 合规性计划](#) 的一部分，第三方审计人员将定期测试和验证安全性的有效性。要了解适用于 AWS Organizations 的合规性计划，请参阅[合规性计划范围内的 AWS 服务](#)。
- 云中的安全性 – 您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您的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 组织 时应用责任共担模式。以下主题说明如何配置 组织 以实现您的安全性和合规性目标。您还将了解如何使用其他 AWS 服务来帮助您监控和保护您的 组织 资源。

主题

- [AWS Organizations 中的 AWS Identity and Access Management \(p. 84\)](#)
- [AWS Organizations 中的日志记录和监控 \(p. 89\)](#)
- [AWS Organizations 的合规性验证 \(p. 94\)](#)
- [AWS Organizations 中的弹性 \(p. 95\)](#)
- [AWS Organizations 中的基础设施安全 \(p. 95\)](#)

AWS Organizations 中的 AWS Identity and Access Management

访问 AWS Organizations 需要凭证。这些凭证必须有权访问 AWS 资源，例如 Amazon Simple Storage Service (Amazon S3) 存储桶、Amazon Elastic Compute Cloud (Amazon EC2) 实例或 AWS Organizations 组织单元 (OU)。以下部分提供了有关如何使用 AWS Identity and Access Management (IAM) 帮助确保安全访问组织和控制谁可以管理组织的详细信息。

为确定谁能够管理组织的哪些部分，AWS Organizations 使用与其他 AWS 服务相同的基于 IAM 的权限模型。作为组织的主账户中的管理员，您可以通过将策略附加到主账户中的用户、组和角色，授予基于 IAM 的权限以执行 AWS Organizations 任务。这些策略指定这些委托人可执行的操作。您将 IAM 权限策略附加到用户所属的组，或者直接附加到用户或角色。[作为最佳实践，我们建议您将策略附加到组而不是用户](#)。您还可以选择向其他人授予完整管理员权限。

对于 AWS Organizations 的大多数管理员操作，您需要将权限附加到主账户中的用户或组。如果某个成员账户中的用户需要为您的组织执行管理员操作，则需要将 AWS Organizations 权限授予主账户中的 IAM 角色，并且在成员账户中启用用户来代入该角色。有关 IAM 策略的更多一般信息，请参阅 IAM 用户指南 中的 [IAM 策略概述](#)。

主题

- [身份验证 \(p. 85\)](#)
- [访问控制 \(p. 85\)](#)

- [管理您的 AWS 组织的访问权限 \(p. 85\)](#)

身份验证

您可以以下面任一类型的身份访问 AWS：

- **AWS 账户根用户** – 注册 AWS 时，您需要提供与您的 AWS 账户关联的电子邮件地址和密码。这些是您的根凭证，它们提供对您所有 AWS 资源的完全访问权限。

Important

出于安全考虑，我们建议您仅使用根凭证创建管理员用户，此类用户对您的 AWS 账户具有完全访问权限的 IAM 用户。然后，您可以使用该管理员用户创建具有有限权限的其他 IAM 用户和角色。有关更多信息，请参阅 IAM 用户指南 中的 [IAM 最佳实践](#) 和 [创建您的第一个 IAM 管理员用户和组](#)。

- **IAM 用户** – [IAM 用户](#) 就是您的 AWS 账户中的一种身份，它具有特定的自定义权限（例如，用于在 Amazon Elastic File System 中创建文件系统的权限）。您可以使用 IAM 用户名和密码登录安全 AWS 网页，例如 [AWS 管理控制台](#)、[AWS 开发论坛](#) 或 [AWS 支持中心](#)。

除了用户名和密码之外，您还可以为每个用户生成 [访问密钥](#)。在通过 [多个开发工具包之一](#) 或使用 [AWS 命令行界面 \(AWS CLI\)](#) 以编程方式访问 AWS 服务时，可以使用这些密钥。开发工具包和 AWS CLI 工具使用访问密钥对您的请求进行加密签名。如果您不使用 AWS 工具，则必须自行对请求签名。AWS Organizations 支持签名版本 4，后者是一种用于对入站 API 请求进行身份验证的协议。有关验证请求的更多信息，请参阅 AWS General Reference 中的 [签名版本 4 签名流程](#)。

- **IAM 角色** – IAM 角色是可在账户中创建的另一种具有特定权限的 IAM 身份。它类似于 IAM 用户，但未与特定人员相关联。利用 IAM 角色，您可以获得可用于访问 AWS 服务和资源的临时访问密钥。具有临时凭证的 IAM 角色在以下情况下很有用：
 - **联合身份用户访问** – 您可以不创建 IAM 用户，而是使用来自 AWS Directory Service、您的企业用户目录或 Web 身份提供商的既有用户身份。这些用户被称为联合身份用户。在通过 [身份提供商](#) 请求访问权限时，AWS 将为联合身份用户分配角色。有关联合身份用户的更多信息，请参阅 IAM 用户指南中的 [联合身份用户和角色](#)。
 - **跨账户访问** – 可以使用您账户中的 IAM 角色向另一个 AWS 账户授予对您账户的资源的访问权限。有关示例，请参阅 IAM 用户指南 中的 [教程：使用 IAM 角色委派跨 AWS 账户的访问权限](#)。
 - **AWS 服务访问** – 可以使用您账户中的 IAM 角色向 AWS 服务授予对您账户的资源的访问权限。例如，您可以创建一个角色，此角色允许 Amazon Redshift 代表您访问 Amazon S3 存储桶，然后将存储在该存储桶中的数据加载到 Amazon Redshift 集群中。有关更多信息，请参阅 IAM 用户指南 中的 [创建角色以向 AWS 服务委派权限](#)。
 - **在 Amazon EC2 上运行的应用程序** – 您不用将访问密钥存储在 EC2 实例中以供实例上运行的应用程序使用并发出 AWS API 请求，而是可以使用 IAM 角色管理这些应用程序的临时凭证。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南 中的 [对 Amazon EC2 上的应用程序使用角色](#)。

访问控制

您可以使用有效的凭证来对自己的请求进行身份验证，但您还必须拥有权限才能管理或访问 AWS Organizations 资源。例如，您必须拥有权限来创建 OU 或者将 [服务控制策略 \(SCP\)](#) (p. 54) 附加到账户。

管理您的 AWS 组织的访问权限

所有 AWS 资源（包括组织中的根、OU、账户和策略）都归 AWS 账户所有，创建和访问资源的权限由权限策略进行管理。对于一个组织而言，其主账户拥有所有资源。账户管理员可通过将权限策略附加到 IAM 身份（用户、组和角色）来控制对 AWS 资源的访问。

Note

账户管理员 (或管理员用户) 是具有管理员权限的用户。有关更多信息, 请参阅 IAM 用户指南 中的 [IAM 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。作为组织主账户的管理员, 您可以执行管理任务或将管理员权限委派给主账户中的其他 IAM 用户或角色。为此, 您可以将 IAM 权限策略附加到 IAM 用户、组或角色。默认情况下, 用户没有权限; 这有时称为隐式拒绝。该策略将使用显式允许 覆盖隐式拒绝, 这将指定用户可以执行哪些操作以及可对哪些资源执行这些操作。如果将权限授予了角色, 则组织中其他账户的用户可以代入该角色。

AWS Organizations 资源和操作

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

资源

在 AWS Organizations 中, 您可以控制对以下资源的访问:

- 构成组织层次结构的根和 OU
- 组织的成员账户
- 您附加到组织中实体的账户
- 用于更改组织状态的握手

其中, 每种资源均有一个与之关联的唯一 Amazon 资源名称 (ARN)。您可以通过在 IAM 权限策略的 `Resource` 元素中指定资源的 ARN 来控制对资源的访问。有关 AWS Organizations 中所用资源的 ARN 格式的完整列表, 请参阅 IAM 用户指南 中的 [AWS Organizations 定义的资源](#)。

操作

AWS 提供了一组操作来处理组织中的资源。利用这些操作, 您可以对资源进行创建、列出、修改、访问其内容以及删除。可在 IAM 策略的 `Action` 元素中引用大多数操作来控制可使用操作的人员。有关可在 IAM 策略中用作权限的 AWS Organizations 操作的列表, 请参阅 IAM 用户指南 中的 [AWS Organizations 定义的 API 操作权限](#)。

在将 `Action` 和 `Resource` 组合到一个权限策略 `Statement` 中后, 可以准确控制可对哪些资源执行该组特定操作。

条件键

AWS 提供可供您进行查询以便对某些操作进行更精细控制的条件键。您可以在 IAM 策略的 `Condition` 元素中参考这些条件键, 以指定将语句视为匹配必须满足的其他条件。

以下条件键专门用 AWS Organizations:

- `organizations:ServicePrincipal` – 如果您使用 [EnableAWSServiceAccess](#) 或 [DisableAWSServiceAccess](#) 操作来对其他 AWS 服务启用或禁用可信访问 (p. 77), 则可用作条件。可以使用 `organizations:ServicePrincipal` 来将这些操作发出的请求限制为已批准的服务委托人名称列表。

例如, 下面的策略允许用户在启用和禁用对 AWS Organizations 的可信访问时仅指定 AWS Firewall Manager:

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

```
{
  "Sid": "AllowOnlyAWSFirewallIntegration",
  "Effect": "Allow",
  "Action": [
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
  ],
  "Resource": "*",
  "Condition": {
    "ForAllValues:StringLike": {
      "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
    }
  }
}
```

- `aws:PrincipalOrgID` – 简化在基于资源的策略中指定 `Principal` 元素的过程。此全局键提供了列出组织中的所有 AWS 账户的所有账户 ID 的替代方法。您可以在 `Condition` 元素中指定[组织 ID \(p. 27\)](#)，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 AWS 组织的主账户。

有关更多信息，请参阅 IAM 用户指南的 [AWS 全局条件上下文键](#) 中对 `PrincipalOrgID` 的说明。

有关可在 IAM 策略中用作权限的所有 AWS Organizations 特定条件键的列表，请参阅 IAM 用户指南中的[用于 AWS Organizations 的条件上下文键](#)。

了解资源所有权

AWS 账户对在该账户下创建的资源具有所有权，而无论创建资源的人员是谁。具体而言，资源所有者是对资源创建请求进行身份验证的[委托人实体](#)（即根账户、IAM 用户或 IAM 角色）的 AWS 账户。对于 AWS 组织，始终为主账户。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：

- 如果您使用主账户的根账户凭证创建 OU，您的主账户即为该资源的所有者。（在 AWS Organizations 中，该资源为 OU。）
- 如果您在主账户中创建 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，主账户（即该用户所属的账户）拥有 OU 资源。
- 如果您在主账户中创建的 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。主账户（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

本部分讨论如何在 AWS Organizations 范围内使用 IAM。它不提供有关 IAM 服务的详细信息。有关完整的 IAM 文档，请参阅 [IAM 用户指南](#)。有关 IAM 策略语法和说明的信息，请参阅 IAM 用户指南中的 [AWS IAM 策略参考](#)。

附加到 IAM 身份的策略称作基于身份的 策略（IAM 策略）。附加到资源的策略称作基于资源 的策略。AWS Organizations 仅支持基于身份的策略（IAM 策略）。

主题

- [基于身份的策略（IAM 策略）\(p. 88\)](#)

- [基于资源的策略 \(p. 88\)](#)

基于身份的策略 (IAM 策略)

您可以向 IAM 身份挂载策略。例如，您可以执行以下操作：

- 将权限策略附加到您的账户中的用户或组 – 要向用户授予创建 AWS Organizations 资源（例如，[服务控制策略 \(SCP\) \(p. 54\)](#) 或 OU）的权限，您可以将权限策略附加到用户或用户所属的组。用户或组必须位于组织的主账户中。
- 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，主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. 主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. 主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主账户和组织中创建和访问资源。如果您需要向 AWS 服务授予代入该角色的权限，则信任策略中的委托人也可以是 AWS 服务委托人。

有关使用 IAM 委派权限的更多信息，请参阅 IAM 用户指南 中的[访问权限管理](#)。

以下是允许用户在组织中执行 CreateAccount 操作的示例策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1OrgPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:CreateAccount"
      ],
      "Resource": "*"
    }
  ]
}
```

有关用户、组、角色和权限的更多信息，请参阅 IAM 用户指南 中的[身份 \(用户、组和角色\)](#)。

基于资源的策略

一些服务（如 Amazon S3）支持基于资源的权限策略。例如，您可以将策略附加到 Amazon S3 存储桶以管理对该存储桶的访问权限。AWS Organizations 目前不支持基于资源的策略。

指定策略元素：操作、条件、效果和资源

对于每项 AWS Organizations 资源，该服务定义一组 API 操作或可通过某种方式与该资源交互或操作该资源的操作。为授予这些操作的权限，AWS Organizations 定义了一组您可以在策略中指定的操作。例如，对于 OU 资源，AWS Organizations 定义了以下操作：

- AttachPolicy 和 DetachPolicy
- CreateOrganizationalUnit 和 DeleteOrganizationalUnit
- ListOrganizationalUnits 和 DescribeOrganizationalUnit

在有些情况下，执行 API 操作可能需要多个操作的权限，并且可能需要多个资源的权限。

以下是可在 IAM 权限策略中使用的最基本元素：

- Action – 使用此关键字标识要允许或拒绝的操作。例如，根据指定的 Effect，organizations:CreateAccount 允许或拒绝执行 AWS Organizations CreateAccount 操作的用户权限。有关更多信息，请参阅 IAM 用户指南 中的 [IAM JSON 策略元素：Action](#)。
- Resource – 使用此关键字指定策略语句适用于的资源 ARN。有关更多信息，请参阅 IAM 用户指南 中的 [IAM JSON 策略元素：Resource](#)。
- 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：Condition](#)。
- Effect – 使用此关键字指定策略语句是允许还是拒绝对资源进行的操作。如果没有明确授予（或允许）对资源的访问权，则隐式拒绝访问。您也可以明确拒绝对资源的访问权，这样做可确保用户无法对指定资源执行指定操作，即使其他策略授予了访问权也是如此。有关更多信息，请参阅 IAM 用户指南 中的 [IAM JSON 策略元素：Effect](#)。
- Principal – 在基于身份的策略（IAM 策略）中，附加了策略的用户会自动成为隐式委托人。对于基于资源的策略，您可以指定要接收权限的用户、账户、服务或其他实体（仅适用于基于资源的策略）。AWS Organizations 目前仅支持基于身份的策略，而不是基于资源的策略。

要了解有关 IAM 策略语法和说明的更多信息，请参阅 IAM 用户指南 中的 [AWS IAM 策略参考](#)。

AWS Organizations 中的日志记录和监控

您应对组织进行监控，确保对所做的更改进行记录，这是最佳实践。这有助于确保能够调查任何意外的更改，并回滚不需要的更改。AWS Organizations 目前支持两种 AWS 服务，帮您监控组织和组织内部的活动。

主题

- [使用 AWS CloudTrail 记录 AWS Organizations API 调用 \(p. 89\)](#)
- [Amazon CloudWatch Events \(p. 94\)](#)

使用 AWS CloudTrail 记录 AWS Organizations API 调用

AWS Organizations 与 AWS CloudTrail 集成，后者是一项在 AWS Organizations 中提供用户、角色或 AWS 服务所采取操作的记录的服务。CloudTrail 将对 AWS Organizations 的所有 API 调用作为事件捕获，包括来自 AWS Organizations 控制台的调用和对 AWS Organizations API 的代码调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 AWS Organizations 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台的 Event history（事件历史记录）中查看最新事件。通过使用 CloudTrail 收集的信息，您可以确定向 AWS Organizations 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅 [AWS CloudTrail User Guide](#)。

Important

您只能查看 美国东部（弗吉尼亚北部）区域中 AWS Organizations 的所有 CloudTrail 信息。如果无法在 CloudTrail 控制台中看到您的 AWS Organizations 活动，请使用右上角的菜单将控制台设为 美国东部（弗吉尼亚北部）。如果您使用 AWS CLI 或开发工具包工具查询 CloudTrail，请将您的查询引至美国东部（弗吉尼亚北部）终端节点。

CloudTrail 中的 AWS Organizations 信息

在您创建 CloudTrail 账户时，即针对该账户启用了 AWS。AWS Organizations 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在 Event history（事件历史记录）中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅 [使用 CloudTrail 事件历史记录查看事件](#)。

要持续记录 AWS 账户中的事件（包括 AWS Organizations 的事件），请创建跟踪。通过跟踪，CloudTrail 可将日志文件传送到 Amazon S3 存储桶。在您的 AWS 账户中启用了 CloudTrail 日志记录时，对 AWS Organizations 操作的 API 调用在 CloudTrail 日志文件中跟踪，它们随其他 AWS 服务记录一起写入到这些文件中。您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取措施。有关更多信息，请参阅以下内容：

- [创建跟踪概述](#)
- [CloudTrail 支持的服务和集成](#)
- [为 CloudTrail 配置 Amazon SNS 通知](#)

所有 AWS Organizations 操作均由 CloudTrail 记录下来并记载到 [AWS Organizations API 参考](#) 中。例如，对 `CreateAccount`（包括 `CreateAccountResult` 事件）、`ListHandshakesForAccount`、`CreatePolicy` 和 `InviteAccountToOrganization` 的调用将在 CloudTrail 日志文件中生成条目。

每个日志条目都包含有关生成请求的人员的信息。日志条目中的用户身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 IAM 用户凭证发出的
- 请求是使用 [IAM 角色](#) 还是 [联合身份用户](#) 的临时安全凭证发出的
- 请求是否由其他 AWS 服务发出

有关更多信息，请参阅 [CloudTrail userIdentity 元素](#)。

了解 AWS Organizations 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会以任何特定顺序显示。

示例日志条目：CreateAccount

下面的示例显示在调用 API 时生成的示例 `CreateAccount` 调用的 CloudTrail 日志条目。

```
{
  "eventVersion": "1.06",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAMVNPBQA3EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/diego",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "diego"
  },
  "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 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
  "requestParameters": {
    "email": "anaya@amazon.com",
    "accountName": "*****"
  },
  "responseElements": {
    "createAccountStatus": {
      "accountName": "*****",
      "state": "IN_PROGRESS",
```

```
        "id": "car-examplecreateaccountrequestid111",
        "requestedTimestamp": "Jun 21, 2018 10:06:27 PM"
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

下面的示例显示在 CreateAccount 调用成功完成后它的 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": "192.0.2.0",
  "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": "SUCCEEDED",
      "accountName": "*****",
      "accountId": "444455556666",
      "requestedTimestamp": "Jun 21, 2018 10:06:27 PM",
      "completedTimestamp": "Jun 21, 2018 10:07:15 PM"
    }
  }
}
```

下面的示例显示 CreateAccount 调用失败后生成的 CloudTrail 日志条目。

```
{
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
```

```
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

示例日志条目 : CreateOrganizationalUnit

以下示例演示示例 CreateOrganizationalUnit 调用的一个 CloudTrail 日志条目。

```
{
  "eventVersion": "1.06",
  "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-examplerootid111"
  },
  "responseElements": {
    "organizationalUnit": {
      "arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-examplerootid111-exampleouid111",
      "id": "ou-examplerootid111-exampleouid111",
      "name": "test-cloud-trail"
    }
  },
  "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

示例日志条目 : InviteAccountToOrganization

以下示例演示示例 InviteAccountToOrganization 调用的一个 CloudTrail 日志条目。

```
{
  "eventVersion": "1.06",
  "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-exampleorgid/invite/h-
examplehandshakeid111",
            "id": "h-examplehandshakeid111",
            "parties": [
                {
                    "type": "ORGANIZATION",
                    "id": "o-exampleorgid"
                },
                {
                    "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": "Master account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-exampleorgid"
                },
                {
                    "type": "ACCOUNT",
                    "value": "222222222222"
                },
                {
                    "type": "NOTES",
                    "value": "This is a request for Mary's account to join Diego's
organization."
                }
            ]
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
```

```
"eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
"eventType": "AwsApiCall",
"recipientAccountId": "111111111111"
}
```

示例日志条目：AttachPolicy

以下示例演示示例 AttachPolicy 调用的一个 CloudTrail 日志条目。该响应指示，在请求尝试附加到的根中，由于请求的策略类型未启用，调用失败。

```
{
  "eventVersion": "1.06",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAMVNPBQA3EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/diego",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "diego"
  },
  "eventTime": "2017-01-18T21:42:44Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "AttachPolicy",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
  "errorCode": "PolicyTypeNotEnabledException",
  "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the current view",
  "requestParameters": {
    "policyId": "p-examplepolicyid111",
    "targetId": "ou-examplerootid111-exampleouid111"
  },
  "responseElements": null,
  "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

Amazon CloudWatch Events

在组织中发生管理员指定的操作时，AWS Organizations 可以与 CloudWatch Events 配合生成事件。例如，大多数管理员希望每次在组织中创建新账户时，或成员账户的管理员尝试离开组织时收到提醒，因为这些都是敏感操作。您可以配置 CloudWatch Events 规则来监视这些操作，然后将生成的事件发送到管理员定义的目标。目标可以是 Amazon SNS 主题，向订阅者发送电子邮件或短信。您还可以创建一个 AWS Lambda 函数，记录操作的详细信息以备稍后查看。

有关如何使用 CloudWatch Events 监控组织中关键活动的教程，请参阅[教程：使用 CloudWatch Events 监控组织的重要更改](#) (p. 16)。

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

AWS Organizations 的合规性验证

作为多个 AWS 合规性计划的一部分，第三方审核员将评估 AWS Organizations 的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规性计划范围内的 AWS 服务的列表，请参阅[合规性计划范围内的 AWS 服务](#)。有关一般信息，请参阅[AWS 合规性计划](#)。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅[下载 AWS Artifact 中的报告](#)。

您在使用 组织 时的合规性责任由您数据的敏感性、您公司的合规性目标以及适用的法律法规决定。AWS 提供以下资源来帮助实现合规性：

- [安全性与合规性快速入门指南](#) – 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署基于安全性和合规性的基准环境的步骤。
- [《设计符合 HIPAA 安全性和合规性要求的架构》白皮书](#) – 此白皮书介绍公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。
- [AWS 合规性资源](#) – 此业务手册和指南集合可能适用于您的行业和位置。
- [AWS Config](#) – 此 AWS 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- [AWS Security Hub](#) – 此 AWS 服务提供了 AWS 中安全状态的全面视图，可帮助您检查是否符合安全行业标准 and 最佳实践。

AWS Organizations 中的弹性

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

有关 AWS 区域和可用区的更多信息，请参阅[AWS 全球基础设施](#)。

AWS Organizations 中的基础设施安全

作为一项托管服务，AWS Organizations 由 [Amazon Web Services：安全流程概述](#) 白皮书中所述的 AWS 全球网络安全程序提供保护。

您可以使用 AWS 发布的 API 调用通过网络访问 组织。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

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

AWS Organizations 参考

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

主题

- [AWS Organizations 的限制 \(p. 96\)](#)
- [可用于 AWS Organizations 的 AWS 托管策略 \(p. 97\)](#)

AWS Organizations 的限制

此部分指定影响 AWS Organizations 的限制。

名称的限制

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

- 名称必须由 Unicode 字符组成
- 其长度不能超过 250 个字符

最大值和最小值

以下是 AWS Organizations 中的实体的默认最大数量。

组织中的 AWS 账户数量	一个组织中允许的最大账户数是 4。如果要增加您的限制，请联系 AWS Support。在控制台右上角，选择支持，然后选择支持中心。在 Support Center (支持中心) 页面上，选择 Create Case (创建案例)。 发送到账户的邀请将计入此限制。如果受邀账户拒绝邀请、主账户取消邀请或邀请过期，则撤销此计数。
组织中的根数量	1。
组织中的 OU 数量	1000。
组织中的策略数量	1000。
服务控制策略 (SCP) (p. 54) 文档的最大大小	5120 字节。这包括所有字符，包括空格。要减小 SCP 的大小 (如果您接近该限制)，则可以删除引号之外的所有空格字符 (如空格和换行符)。
根中的最大 OU 嵌套数	根下方最深五层 OU。
您可在 24 小时内添加的待接受邀请数	20 — 已接受的邀请不计入此限制。一旦某个邀请被接受，您就可以发送另一个同一天的邀请。
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。
可以将策略附加到的实体数	无限制。

您可以附加到账户的标签数	50。
--------------	-----

握手的过期时间

以下是 AWS Organizations 中的握手超时时间。

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。

策略类型	每个根的策略数	每个 OU 的策略数	每个账户的策略数
服务控制策略	5	5	5

Note

目前，您的组织中只能有一个根。

最小值取决于策略类型。下表显示了各种策略类型以及可将每种类型附加到的最小实体数。

策略类型	允许附加到实体的数量下限
服务控制策略	1 — 每个实体始终必须至少附加一个 SCP。您无法从实体上删除最后一个 SCP。

可用于 AWS Organizations 的 AWS 托管策略

此部分介绍向您提供的、可用于管理您的管理事宜的 AWS 托管策略。您无法修改或删除 AWS 托管策略，但可以根据需要将其附加到组织中的实体或从这些实体上分离。

AWS Organizations 托管服务控制策略

[服务控制策略 \(SCP\)](#) (p. 54) 类似于 IAM 权限策略，但它是 AWS Organizations 而非 IAM 的功能。可以使用 SCP 来指定受影响的实体的最大权限数。您可以将 SCP 附加到组织的根、组织单位 (OU) 或账户。您可以创建自己的策略，也可以使用 IAM 定义的策略。您可以在 [组织 控制台的 Policies \(策略\)](#) 页面上查看组织中的策略列表。

Important

每个根、OU 和账户必须始终附加有至少一个 SCP。

策略名称	描述	ARN
FullAWSAccess	提供 AWS Organizations 主账户对成员账户的访问权。	arn:aws:iam::aws:policy/ AWSFullAccess

AWS Organizations 疑难解答

如果您在使用 AWS Organizations 时遇到问题，请查询本部分中的相关主题。

主题

- [排查一般问题](#) (p. 99)
- [排查AWS Organizations 策略问题](#) (p. 101)

排查一般问题

使用此处的信息可帮助您诊断并修复在使用 AWS Organizations 时可能遇到的拒绝访问或其他常见问题。

主题

- [当我向 AWS Organizations 发出请求时，收到了“access denied”\(访问被拒绝\) 消息](#) (p. 99)
- [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](#) (p. 99)
- [当我尝试以成员账户身份离开组织或以主账户身份删除成员账户时，收到“access denied”\(拒绝访问\) 消息](#) (p. 100)
- [尝试向组织中添加账户时，我收到“limit exceeded”消息](#) (p. 100)
- [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](#) (p. 100)
- [尝试向组织中添加账户时，我收到“organization is still initializing”消息](#) (p. 100)
- [我在创建了成员账户时使用了不正确的电子邮件地址](#) (p. 100)
- [我所做的更改不总是立即可见](#) (p. 100)

当我向 AWS Organizations 发出请求时，收到了“access denied”(访问被拒绝) 消息

- 验证您是否具有调用您请求的操作和资源的许可。管理员必须通过将 IAM 策略附加到您的 IAM 用户或您所属的组来授予权限。如果授予这些权限的策略语句包含任何条件 (例如，当日时间或 IP 地址限制)，则您还必须在发送请求时满足这些要求。有关查看或修改适用于 IAM 用户、组或角色的策略的信息，请参阅 IAM 用户指南 中的 [使用策略](#)。
- 如果您手动签署 API 请求 (不使用 [AWS 开发工具包](#))，请验证您已正确[签署请求](#)。

当我使用临时安全凭证发送请求时，收到了“access denied”(拒绝访问) 消息

- 请确认您用于发出请求的 IAM 用户或角色具有正确的权限。临时安全凭证权限派生自 IAM 用户或角色，因此权限范围仅限于相应 IAM 用户或角色的权限。有关临时安全凭证权限确定方式的更多信息，请参阅 IAM 用户指南 中的 [控制临时安全凭证的权限](#)。
- 验证您的请求是否采用了正确的签名和适当的格式。有关详细信息，请参阅所选开发工具包的 [工具包文档](#) 或 IAM 用户指南 中的 [使用临时安全凭证以请求对 AWS 资源的访问权限](#)。
- 验证您的临时安全凭证没有过期。有关更多信息，请参阅 IAM 用户指南 中的 [请求临时安全凭证](#)。

当我尝试以成员账户身份离开组织或以主账户身份删除成员账户时，收到“access denied”(拒绝访问) 消息

- 要删除成员账户，必须先在此成员账户中启用 IAM 用户访问账单的权限。有关更多信息，请参阅 AWS Billing and Cost Management 用户指南 中的[激活对 Billing and Cost Management 控制台的访问权限](#)。
- 仅当账户拥有作为独立账户运行所需的信息时，才能从组织中删除此账户。当您使用 AWS Organizations 控制台、API 或 AWS CLI 命令在组织中创建账户时，系统不会自动收集此类信息。对于您想用作独立账户的账户，您必须接受 AWS 客户协议，选择支持计划，提供和验证所需联系信息，并提供当前的付款方式。AWS 将使用该付款方式向账户未绑定到组织期间发生的任何可结算（非 AWS 免费套餐）AWS 活动收费。有关更多信息，请参阅[作为成员账户退出组织 \(p. 42\)](#)。

尝试向组织中添加账户时，我收到“limit exceeded”消息

组织存在账户数量限制。已删除或已关闭的账户会继续计入此限制。

加入邀请也计入组织的账户限制。如果受邀账户拒绝邀请、主账户取消邀请或邀请过期，则撤销此计数。

- 关闭或删除 AWS 账户前，[请从组织中删除它 \(p. 40\)](#)，以免其继续占用您的限额。
- 联系 [AWS Support](#) 以请求提高限制。

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。稍后重试此操作。如果您在添加和删除账户时遇到有关账户限制的问题，请联系 [AWS Support](#) 来请求提高限制。

尝试向组织中添加账户时，我收到“organization is still initializing”消息

如果您收到此类错误，而且距您创建组织已过了一个多小时，请联系 [AWS Support](#)。

我在创建了成员账户时使用了不正确的电子邮件地址

如果您在组织中创建了一个电子邮件地址不正确的成员账户，则无法以根用户身份登录该账户。在这种情况下，可尝试为该账户访问或创建主账户访问角色。有关更多信息，请参阅[访问具有主账户访问权角色的成员账户 \(p. 39\)](#)。如果您无法访问或创建角色，请参阅[Contact Us \(联系我们\)](#) 页面，选择账单相关事项联系 AWS Support。

我所做的更改不总是立即可见

作为全球数据中心的计算机要访问的服务，AWS Organizations 使用称为[最终一致性](#)的分布式计算模型。您在 AWS Organizations 中所做的任何更改需要一些时间才会在相关终端节点中可见。它在服务器与服务器之间或复制区域与复制区域之间发送数据需要时间，这会造成一定的延迟。AWS Organizations 也使用缓存来提高性能，但在某些情况下，这可能会增加时间。在之前缓存的数据超时之前，更改可能不可见。

在设计全球应用程序时，需要考虑这些可能的延迟，即使在一个位置所做的更改对另一个位置不是立即可见，也要确保按预期工作。

有关其他某些 AWS 服务如何受此影响的更多信息，请参阅以下资源：

- Amazon Redshift Database Developer Guide 中的[管理数据一致性](#)
- Amazon Simple Storage Service 开发人员指南 中的 [Amazon S3 数据一致性模型](#)
- AWS 大数据博客中的[在使用 Amazon S3 和 Amazon Elastic MapReduce 处理 ETL 工作流程时确保一致性](#)
- Amazon EC2 API Reference 中的 [EC2 最终一致性](#)。

排查AWS Organizations 策略问题

使用此处的信息可帮助您诊断和修复在 AWS Organizations 策略中找到的常见错误。

服务控制策略

AWS Organizations 中的服务控制策略 (SCP) 与 IAM 策略类似并有共用的语法。此语法以 [JavaScript 对象表示法 \(JSON\)](#) 的规则开头。JSON 描述对象 以及组成对象的名称和值对。[IAM 策略语法](#)通过定义有意义的名称和值进行构建，使用策略授予权限的 AWS 服务可以理解这些名称和值。

AWS Organizations 使用部分 IAM 句法和语法。有关详细信息，请参阅 [SCP 语法 \(p. 68\)](#)。

常见策略错误

- [多个策略对象 \(p. 101\)](#)
- [多个 Statement 元素 \(p. 102\)](#)
- [策略文档超出最大大小 \(p. 103\)](#)

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 字节。此限制包括所有字符，包括空格。要减小 SCP 的大小（如果您接近该限制），则可以删除引号之外的所有空格字符（如空格和换行符）。

通过提出 HTTP 查询请求来调用 API

本部分包含有关使用适用于 AWS Organizations 的查询 API 的常规信息。有关 API 操作和错误的详细信息，请参阅 [AWS Organizations API 参考](#)。

Note

您可以使用 AWS 开发工具包之一，代替对 AWS Organizations 查询 API 进行直接调用。AWS 开发工具包中包含适用于各种编程语言和平台（Java、Ruby、.NET、iOS、Android 等）的库和示例代码。开发工具包提供便捷的方式来创建对 AWS Organizations 和 AWS 的编程访问。例如，开发工具包执行以下类似任务：加密签署请求、管理错误以及自动重试请求。有关 AWS 开发工具包的信息（包括如何下载及安装），请参阅[适用于 Amazon Web Services 的工具](#)。

使用适用于 AWS Organizations 的查询 API 可以调用服务操作。查询 API 请求是 HTTPS 请求，必须包含 Action 参数，以指示要执行的操作。AWS Organizations 支持所有操作的 GET 和 POST 请求。也就是说，API 不要求您使用某些操作的 GET 请求和其他操作的 POST 请求。然而，GET 请求受 URL 的大小限制。尽管此限制与浏览器相关，不过通常为 2048 字节。因此，对于要求更高的查询 API 请求，您必须使用 POST 请求。

响应是 XML 文档。有关响应的详细信息，请参阅 [AWS Organizations API 参考](#) 中的各个操作页面。

主题

- [终端节点 \(p. 104\)](#)
- [必须使用 HTTPS \(p. 104\)](#)
- [签署 AWS Organizations API 请求 \(p. 104\)](#)

终端节点

AWS Organizations 在美国东部（弗吉尼亚北部）区域托管了一个全局 API 终端节点：<https://organizations.us-east-1.amazonaws.com>

有关所有服务的 AWS 终端节点和区域的更多信息，请参阅 AWS General Reference 中的[区域和终端节点](#)。

必须使用 HTTPS

由于查询 API 返回安全凭证等敏感信息，必须使用 HTTPS 对所有 API 请求加密。

签署 AWS Organizations API 请求

必须使用访问密钥 ID 和秘密访问密钥签署请求。我们强烈建议您不要使用 AWS 根账户凭证处理日常的 AWS Organizations 工作。您可以使用 IAM 用户的凭证或临时凭证，例如您用于 IAM 角色的凭证。

要对您的 API 请求进行签名，您必须使用 AWS 签名版本 4。有关使用签名版本 4 的信息，请参阅 AWS 一般参考中的[签名版本 4 签名流程](#)。

AWS Organizations 不支持早期版本，例如签名版本 2。

有关更多信息，请参阅下列内容：

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

AWS Organizations 文档历史记录

下表介绍了 AWS Organizations 的主要文档更新。

- API 版本：2016-11-28

update-history-change	update-history-description	update-history-date
与 AWS Config 规则集成	您可以使用 AWS Config API 在组织中跨所有 AWS 账户 来管理 AWS Config 规则。	July 8, 2019
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。	June 24, 2019
与 AWS Control Tower 集成	将 AWS Control Tower 作为可用于组织账户的服务添加。	June 24, 2019
与 AWS Identity and Access Management 集成	IAM 为您的组织实体（组织根、OU 和账户）提供服务上次访问数据。您可以使用此数据，将访问限制为仅您需要的 AWS 服务。	June 20, 2019
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。	June 6, 2019
服务控制策略 (SCP) 中的资源、条件和 NotAction 元素	现在，您可以指定 SCP 中的资源、条件和 NotAction 元素以拒绝跨组织或组织部门 (OU) 中账户的访问。	March 25, 2019
新增的可信访问服务	AWS License Manager 和 AWS Service Catalog 添加为可与您的组织中的账户一起使用的服务。	December 21, 2018
新增的可信访问服务	将 AWS CloudTrail 和 AWS RAM 作为可用于组织账户的服务添加。	December 4, 2018
新增的可信访问服务	将 AWS Directory Service 作为可用于组织账户的服务添加。	September 25, 2018
电子邮件地址验证	必须在验证您与主账户关联的电子邮件地址后，才能邀请现有账户加入您的组织。	September 20, 2018
CreateAccount 通知	CreateAccount 通知将发布到主账户的 CloudTrail 日志。	June 28, 2018
新增的可信访问服务	将 AWS Artifact 作为可用于组织账户的服务添加。	June 20, 2018
新增的可信访问服务	将 AWS Config 和 AWS Firewall Manager 作为可用于组织账户的服务添加。	April 18, 2018

可信服务访问	您现在可允许或禁止对要在组织账户中运行的精选 AWS 服务的访问。AWS SSO 是最初受支持的可信服务。	March 29, 2018
账户删除现在是自助服务	您现在可以删除在 AWS Organizations 内创建的账户，无需联系 AWS Support。	December 19, 2017
增加了对新服务 AWS Single Sign-On 的支持	AWS Organizations 现支持与 AWS Single Sign-On (AWS SSO) 的集成。	December 7, 2017
AWS 为所有组织账户添加了服务相关角色	名为 <code>AWSServiceRoleForOrganizations</code> 的服务相关角色已添加到组织中的所有账户，以实现 AWS Organizations 与其他 AWS 服务之间的集成。	October 11, 2017
您现在可以删除已创建的账户 (p. 106)	客户现在可以在 AWS Support 的帮助下从其组织中删除已创建的账户。	June 15, 2017
服务启动	新服务推出时随附的初始 AWS Organizations 文档版本。	February 17, 2017

AWS 词汇表

有关最新 AWS 术语，请参阅 AWS General Reference 中的 [AWS 词汇表](#)。