

Amazon 账户管理



Amazon 账户管理: 参考指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

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

Table of Contents

什么是 Amazon Web Services 账户？	1
Amazon Web Services 账户 功能	2
您是 Amazon 新用户吗？	3
相关 Amazon 服务	3
使用根用户	4
支持和反馈	5
其他 Amazon 资源	5
开始使用您的账户	6
查看先决条件	6
步骤 1：创建账户	7
步骤 2：为您的根用户激活 MFA	9
步骤 3：创建管理员用户	10
相关 主题	10
访问您的 账户	10
规划您的治理结构	12
使用多个 Amazon Web Services 账户 的好处	12
管理多个 Amazon Web Services 账户	13
何时使用 Amazon Organizations	13
启用信任访问权限	14
启用委托管理员账户	15
何时使用 Amazon Control Tower	16
了解 API 的操作模式	17
授予更新账户属性的权限	18
配置您的账户	20
创建或更新您的账户别名	20
在您的账户中启用或禁用 Amazon Web Services 区域	20
启用和禁用区域之前的注意事项	21
为独立账户启用或禁用区域	23
在组织中启用或禁用区域	25
更新 Amazon Web Services 账户 的账单	28
更新账户设置	28
更新 Amazon Web Services 账户 的备用联系人	30
电话号码和电子邮件地址要求	30
为独立 Amazon Web Services 账户 更新备用联系人	31

更新您组织中任意 Amazon Web Services 账户 的备用联系人	34
account:AlternateContactTypes 上下文键	37
更新 Amazon Web Services 账户 的主要联系人	38
电话号码和电子邮件地址要求	39
为独立 Amazon Web Services 账户 更新主要联系人	39
更新您组织中任意 Amazon Web Services 账户 的主要联系人	41
查看账户标识符	44
找到你的 Amazon Web Services 账户 身份证	44
查找 Amazon Web Services 账户 的规范用户 ID	47
保护您的账户	50
数据保护	50
Amazon PrivateLink	51
创建端点	52
Amazon VPC 端点策略	52
端点策略	52
身份和访问管理	53
受众	54
使用身份进行身份验证	54
使用策略管理访问	56
Amazon 账户管理和 IAM	58
基于身份的策略示例	65
使用基于身份的策略	68
故障排除	70
Amazon 托管策略	71
AWSAccountManagementReadOnlyAccess	72
AWSAccountManagementFullAccess	73
策略更新	73
合规性验证	74
弹性	74
基础设施安全性	75
监控您的账户	76
CloudTrail 日志	76
中的账户管理信息 CloudTrail	76
了解账户管理日志条目	77
使用 EventBridge 监控账户管理事件	81
账户管理事件	81

排查账户故障	84
账户创建问题	84
账户关闭问题	85
我不知道如何删除或取消我的账户	85
我在“账户”页面上看不到“关闭账户”按钮	85
我关闭了账户，但仍未收到确认电子邮件	85
我在尝试关闭账户时收到一条“ConstraintViolationException”错误	86
我在尝试关闭成员账户时收到一条“CLOSE_ACCOUNT_QUOTA_EXCEEDED”错误	86
我在关闭管理账户之前，需要删除我的 Amazon 组织吗？	86
其它问题	86
我需要变更我的 Amazon Web Services 账户 的信用卡	87
我需要举报 Amazon Web Services 账户 欺诈活动	87
我需要关闭我的 Amazon Web Services 账户	87
关闭您的账户	88
关闭账户前的注意事项	88
如何关闭您的账户	89
账户关闭后会发生什么	92
后关闭期	92
重新打开你的 Amazon Web Services 账户	93
API 参考	94
操作	95
AcceptPrimaryEmailUpdate	97
DeleteAlternateContact	101
DisableRegion	105
EnableRegion	108
GetAlternateContact	111
GetContactInformation	116
GetPrimaryEmail	120
GetRegionOptStatus	123
ListRegions	127
PutAlternateContact	131
PutContactInformation	136
StartPrimaryEmailUpdate	139
相关操作	142
CreateAccount	142
CreateGovCloudAccount	142

DescribeAccount	142
数据类型	142
AlternateContact	144
ContactInformation	146
Region	150
ValidationExceptionField	151
常见参数	151
常见错误	153
发出 HTTP 查询请求	155
端点	156
必须使用 HTTPS	156
签署 Amazon 账户管理 API 请求	156
配额	157
管理印度地区的账户	158
通过 Amazon 印度创建 Amazon Web Services 账户	158
管理您的客户验证信息	160
查看客户验证状态	160
创建您的客户验证信息	160
编辑您的客户验证信息	161
接受的用于客户验证的印度证件	162
管理您的 Amazon India 账户	163
文档历史记录	164
.....	clxvi

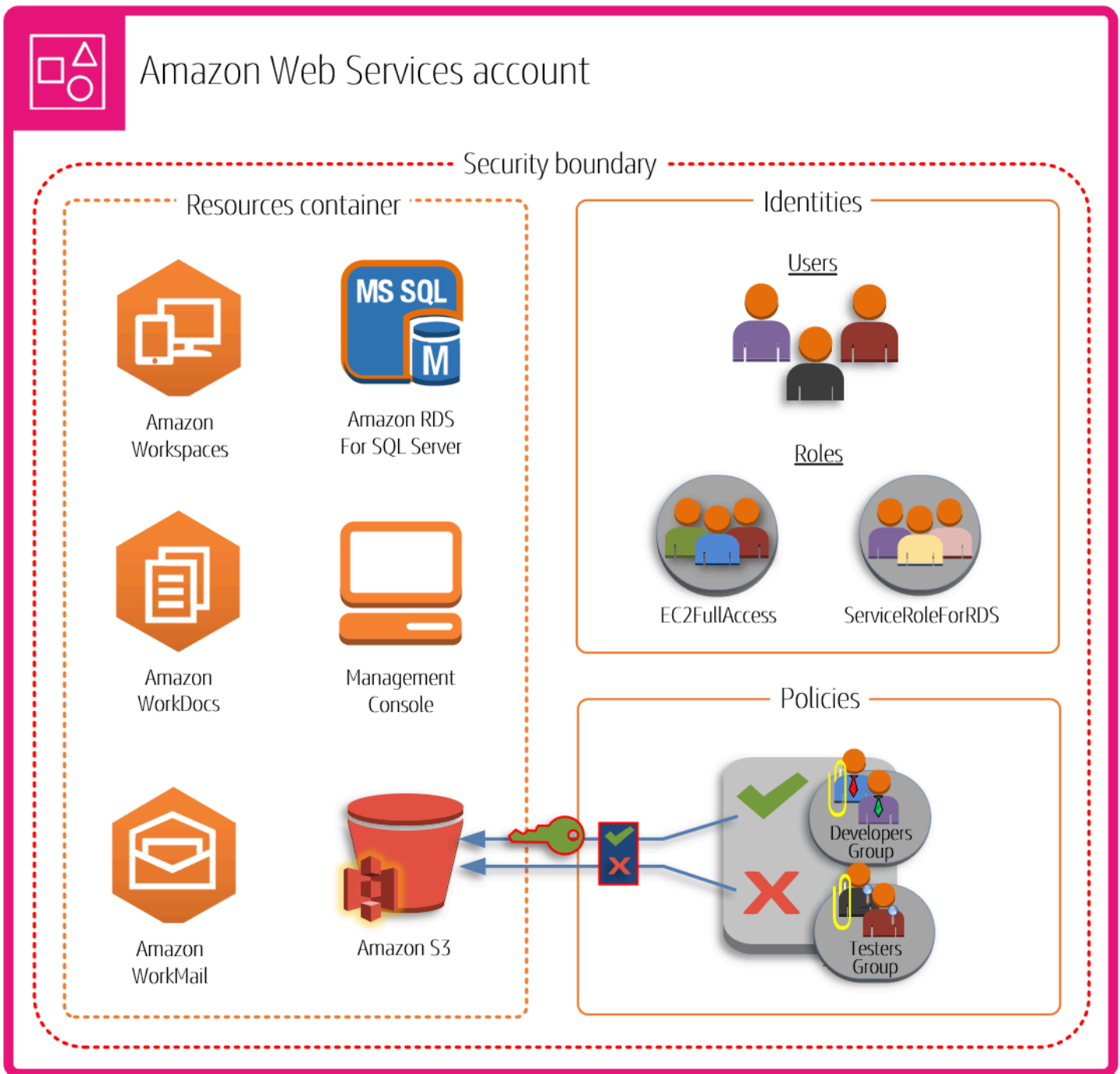
什么是 Amazon Web Services 账户？

Amazon Web Services 账户 代表您与 Amazon 建立的正式业务关系。您可以在 Amazon Web Services 账户 中创建和管理 Amazon 资源，您的账户为访问和计费提供身份管理功能。每个 Amazon Web Services 账户 都有唯一的 ID，用于将其与其他 Amazon Web Services 账户 区分开来。

您的云资源和数据包含在 Amazon Web Services 账户 中。账户充当身份和访问管理的隔离边界。当需要在两个账户之间共享资源 and 数据时，必须明确允许这种访问权限。默认不允许在账户之间进行访问。例如，如果指定不同的账户来存放生产和非生产资源 and 数据，则默认不允许在这些环境之间进行访问。

Amazon Web Services 账户 也是访问 Amazon 服务的基本组成部分。如下图所示，Amazon Web Services 账户 提供以下两大功能：

- **资源容器** — Amazon Web Services 账户 是您作为 Amazon 客户可以创建的所有 Amazon 资源的基本容器。例如，Amazon Simple Storage Service (Amazon S3) 存储桶、Amazon Relation Database Service (Amazon RDS) 数据库和 Amazon Elastic Compute Cloud (Amazon EC2) 实例都是资源。每个资源均由一个 Amazon 资源名称 (ARN) 进行唯一标识，该 ARN 包含或拥有该资源的账户 ID。
- **安全边界** - Amazon Web Services 账户 也是 Amazon 资源的基本安全边界。您在账户中创建的资源可供拥有账户凭证的用户使用。您可以在账户中创建的关键资源包括身份，例如用户和角色。这些身份具有用户可以用来登录 Amazon (进行身份验证) 的凭证。身份还拥有指定用户可以使用账户中的资源执行 (授权) 哪些操作的权限策略。



使用多个 Amazon Web Services 账户 是扩展环境的最佳做法，因为这可以为成本提供自然的计费边界，隔离资源确保安全，为个人和团队提供灵活性，此外还能适应新的业务流程。有关更多信息，请参阅 [使用多个 Amazon Web Services 账户 的好处](#)。

Amazon Web Services 账户 功能

Amazon Web Services 账户 包含以下核心功能：

- **监控和控制成本** - 账户是分配 Amazon 成本的默认方式。因此，针对不同的业务部门和工作负载组使用不同的账户有助于您更轻松地进行跟踪、控制、预测、编制预算和报告云支出。如果您选择在某个时候使用 Amazon Organizations，除了账户级的成本报告外，Amazon 还内置支持整合和报告您整个账户集的成本。您还可以使用 Amazon 服务配额来帮助防止意外的过度配置 Amazon 资源和恶意行为，这些可能会严重影响您的 Amazon 成本。
- **隔离单元** - Amazon Web Services 账户为您的 Amazon 资源提供安全性、访问权限和计费边界，有助于您实现资源自主权和隔离。根据设计，一个账户中配置的所有资源与其他账户配置的资源实现逻辑隔离，即使是在您自己的 Amazon 环境中。该隔离边界提供了一种限制应用程序相关问题、配置错误或恶意操作风险的方法。如果一个账户中出现问题，可以减轻或消除对其他账户中所含工作负载的影响。
- **镜像业务工作负载** - 使用多个账户将具有共同业务目的的工作负载分组到不同账户中。因此，您可以使所有权和决策与这些账户保持一致，避免相互依赖以及与其他账户中工作负载的保护和管理方式发生冲突。根据整体业务模式，您可以选择在不同的账户中隔离不同的业务单位或子公司。随着时间的推移，这种方法还可以减轻剥离这些部门的难度。

您是 Amazon 新用户吗？

如果您是首次使用 Amazon 的用户，第一步是注册 Amazon Web Services 账户。注册时，Amazon 使用您提供的详细信息创建一个账户，并将此账户分配给您。创建 Amazon Web Services 账户后，请以[根用户](#)身份登录，为根用户激活多重身份验证 (MFA)，然后为用户分配管理权限。

有关如何设置新账户的分步说明，请参阅 [Amazon Web Services 账户入门](#)。

相关 Amazon 服务

Amazon Web Services 账户无缝使用以下服务：

- IAM

您的 Amazon Web Services 账户与 Amazon Identity and Access Management (IAM) 紧密集成。您可以将 IAM 与您的账户结合使用，以确保使用您的账户工作的其他人只拥有完成其工作所需的访问权限。您也可以使用 IAM 来控制对所有 Amazon 资源（而不仅仅是特定账户信息）的访问。在您着手设置 Amazon Web Services 账户账户结构之前，首先熟悉 IAM 的主要概念和最佳实践十分重要。有关更多信息，请参阅 [《IAM 用户指南》](#) 中的 IAM 安全最佳实践。

- Amazon Organizations

如果公司规模很大或成长潜力大，您可能需要设置多个反映公司具体结构的 Amazon 账户。Amazon Organizations 为您构建和管理多账户环境提供底层基础设施和功能。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。有关更多信息，请参阅 [何时使用 Amazon Organizations](#)。

- Amazon Control Tower

Amazon Control Tower 提供了简化的方法来设置和管理安全的多账户 Amazon 环境。Amazon Control Tower 使用 Amazon Organizations 自动创建多账户环境，它实例化一组初始账户，并提供一些针对该环境的默认护栏和配置。只需几个步骤就可以使用 Amazon Control Tower 配置新的 Amazon Web Services 账户，同时确保账户符合组织策略。有关更多信息，请参阅 [何时使用 Amazon Control Tower](#)。

使用 Amazon Web Services 账户根用户

当您创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon Web Services 服务和资源拥有完全访问权限的登录身份。此身份称为 Amazon Web Services 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的 [需要根用户凭证的任务](#)。

Important

拥有您的 Amazon Web Services 账户的根用户账户凭证的任何用户都可以无限制地访问账户中的所有资源，包括账单信息。

Important

在北京和宁夏 Amazon Web Services 区域，没有根用户的概念。所有用户都是 IAM 用户，包括创建 Amazon Web Services 账户的用户。

您可以 [更改或重置根用户密码](#)，[创建或删除根用户的访问密钥](#)（访问密钥 ID 和秘密访问密钥）。要获取使用根用户登录方面的帮助，请参阅《Amazon 登录用户指南》中的 [以根用户身份登录 Amazon Web Services Management Console](#)。

对 Amazon 账户管理的支持

您可以使用 [Amazon 账户管理支持论坛](#) 发布反馈和问题。有关 Amazon 论坛的一般信息，请参阅 [Amazon Web Services re:Post](#)。

如果在 Amazon Web Services re:Post 上找不到想要的答案，可以使用 Amazon Web Services Management Console 创建与账户或账单相关的支持案例。有关更多信息，请参阅 [示例：创建账户和账单支持工单](#)。

其他 Amazon 资源

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

Amazon Web Services 账户 入门

如果您是 Amazon 的新手用户，第一步是注册 Amazon Web Services 账户。当您这样做时，Amazon 将使用您提供的详细信息创建一个账户并将其分配给您。

本节中的主题将帮助您开始了解和设置新的 Amazon Web Services 账户。

主题

- [创建新 Amazon Web Services 账户 的先决条件](#)
- [创建 Amazon Web Services 账户](#)
- [为您的根用户激活 MFA](#)
- [创建管理员用户](#)
- [访问 Amazon Web Services 账户](#)

创建新 Amazon Web Services 账户 的先决条件

要注册 Amazon Web Services 账户，您需要提供以下信息：

- 根用户电子邮件地址 – 此电子邮件地址用作[根用户](#)的登录名，也是账户恢复所必需的信息。您必须能够接收发送到此地址的电子邮件消息。在执行某些任务之前，必须验证您是否有权访问发送至此地址的电子邮件。

Important

如果此账户为企业账户，请使用安全的企业通讯组列表（例如 `it.admins@example.com`），这样即使员工更换岗位或离职，企业也可以保留对 Amazon Web Services 账户 的访问权限。由于电子邮件地址可用于重置账户的根用户凭证，因此需要对通讯组列表或地址的访问权限加以保护。

- Amazon 账户名称 - 账户名称出现在多个位置，例如在发票上以及控制台中（如“账单和成本管理”控制面板和 Amazon Organizations 控制台）。我们建议使用标准方法来命名账户，这样就可以为账户指定易于识别的名称。对于公司账户，请考虑使用组织-目的-环境之类的命名标准（例如，`AnyCompany-audit-prod`）。对于个人账户，可以考虑使用名字-姓氏-目的之类的命名标准（例如，`paulo-santos-testaccount`）。

有关更改账户名称的信息，请参阅[如何更改我的 Amazon Web Services 账户 账户名称？](#)。

- 地址 - 如果您的联系地址位于印度，则您账户的用户协议是与 Amazon Internet Services Private Limited (AISPL) 签订的，这是一家位于印度本地 Amazon 销售商。您必须在验证过程中提供 CVV。您可能还需要输入一次性密码，具体取决于您的银行。在验证过程中，AISPL 将对您提供的付款方式收取 2 INR。AISPL 将在验证完成后退回 2 INR。
- 电话号码 - 可以使用此号码确认账户的所有权。您必须能够通过此电话号码接听电话。

Important

如果此账户为企业账户，请使用企业电话号码，这样即使员工更换岗位或离职，企业也可以保留对 Amazon Web Services 账户 的访问权限。

创建 Amazon Web Services 账户

本主题介绍如何创建非由 Amazon Organizations 管理的独立 Amazon Web Services 账户。如果想创建属于 Amazon Organizations 管理组织的账户，请参阅《Amazon Organizations 用户指南》中的[在组织中创建成员账户](#)。

这些说明适用于在印度之外创建 Amazon Web Services 账户。有关在印度创建账户的信息，请参阅[通过 Amazon 印度创建 Amazon Web Services 账户](#)。

Amazon Web Services Management Console

创建 Amazon Web Services 账户

1. 打开[亚马逊云科技主页](#)。
2. 选择创建 Amazon Web Services 账户。

Note

如果您最近登录过 Amazon，则此选项可能不存在。请改为选择登录控制台。然后如果创建新 Amazon Web Services 账户 选项仍不可见，请先选择登录其他账户，然后选择创建新 Amazon Web Services 账户。

3. 输入您的账户信息，然后选择验证电子邮件地址。这将向您指定的电子邮件地址发送验证码。

⚠ Important

由于账户的**根用户**非常重要，因此我们强烈建议您使用可以由团体访问的电子邮件地址，而不是仅由个人访问的电子邮件地址。这样，如果注册 Amazon Web Services 账户的人离开了公司，仍然可以使用 Amazon Web Services 账户，因为电子邮件地址仍然可以访问。

如果无法访问与 Amazon Web Services 账户 关联的电子邮件地址，那么在丢失密码的情况下，就无法恢复对该账户的访问权限。

4. 输入您的验证码，然后选择验证。
5. 为根用户输入一个强密码并确认，然后选择继续。Amazon 要求您的密码满足以下条件：
 - 长度必须至少 8 个字符，最多 128 个字符。
 - 必须至少包含以下字符类型中三种的组合：大写字母、小写字母、数字，以及 ! @ # \$ % ^ & * () < > [] { } | _ + = 符号。
 - 不得与您的 Amazon Web Services 账户名称或电子邮件地址相同。
6. 选择企业或个人。个人账户和企业账户具有相同的特征和功能。
7. 输入您的公司或个人信息。

⚠ Important

对于企业 Amazon Web Services 账户，最佳做法是输入：

- 公司电话号码，而不是个人电话号码。
- 电子邮件地址，其域名属于将要使用该账户的公司或组织。

使用个人电子邮件地址或个人电话号码配置账户的根用户可能会使账户不安全。

8. 阅读并接受 [Amazon 客户协议](#)。请务必阅读并理解 Amazon 客户协议的条款。
9. 选择继续。此时，您将收到一个电子邮件消息，确认您的 Amazon Web Services 账户 已准备就绪。可以使用在注册时提供的电子邮件地址和密码登录新账户。但是，在完成账户激活操作之前，您无法使用任何 Amazon 服务。
10. 输入有关付款方式的信息，然后选择验证并继续。如果想使用不同的账单地址作为 Amazon 账单信息，请选择使用新地址。

在添加有效付款方式之前，您无法继续注册流程。

11. 请从列表中选择您的国家或区域代码，然后输入在接下来的几分钟内可以拨打的电话号码。
12. 输入验证码中显示的代码，然后提交。
13. 当自动系统与您联系时，请输入收到的 PIN，然后提交。
14. 选择一个可用的 Amazon Web Services Support 计划。有关可用支持计划的描述，请参阅[比较 Amazon Web Services Support 计划](#)。
15. 选择完成注册。此时会显示确认页面，表明您的账户正在激活。
16. 检查您的电子邮件和垃圾邮件文件夹是否有确认账户已激活的电子邮件消息。激活通常需要几分钟，但有时最长需要 24 小时。

收到此激活消息后，您就可以完全访问所有 Amazon 服务。

Amazon CLI & SDKs

在登录组织管理账户时，可以通过运行 [CreateAccount](#) 操作在 Amazon Organizations 管理的组织中创建成员账户。

您不能使用 Amazon Command Line Interface (Amazon CLI) 或 Amazon API 操作在组织之外创建独立 Amazon Web Services 账户。

为您的根用户激活 MFA

我们强烈建议您为根用户激活 MFA。多重身份验证大大降低了他人在未经授权的情况下访问您账户的风险。

1. 选择根用户并输入您的 Amazon Web Services 账户电子邮件地址，以账户所有者身份登录 [Amazon Web Services Management Console](#)。在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《Amazon 登录用户指南》中的[以根用户身份登录 Amazon Web Services Management Console](#)。

2. 为根用户启用 MFA。

有关说明，请参阅《IAM 用户指南》中的[为 Amazon Web Services 账户根用户启用虚拟 MFA 设备 \(控制台\)](#)。

创建管理员用户

由于您无法限制根用户可以执行的操作，我们强烈建议不要使用根用户执行任何未明确要求根用户的任务。相反，应在 IAM Identity Center 为管理用户分配管理访问权限，然后以该管理用户的身份登录执行日常管理任务。

有关说明，请参阅《IAM Identity Center 用户指南》中的[为 IAM Identity Center 管理用户设置 Amazon Web Services 账户 访问权限](#)。

相关主题

- 有关保护根用户凭证的信息，请参阅《IAM 用户指南》中的[保护根用户的凭证](#)。
- 有关需要根用户的任务的完整列表，请参阅《IAM 用户指南》中的[需要根用户凭证的任务](#)。

访问 Amazon Web Services 账户

您可以通过以下任何一种方式访问您的 Amazon Web Services 账户：

Amazon Web Services Management Console

[Amazon Web Services Management Console](#) 是一个基于浏览器的界面，您可以用它来管理您的 Amazon Web Services 账户 设置和您的 Amazon 资源。

Amazon 命令行工具

使用 Amazon 命令行工具，您可在系统的命令行中发出命令以执行 Amazon Web Services 账户 和 Amazon 任务。与使用控制台相比，使用命令行处理更快、更方便。如果要构建执行 Amazon 任务的脚本，命令行工具也会十分有用。Amazon 提供了两套命令行工具：

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

Amazon SDK

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

Amazon 账户管理 HTTPS 查询 API

Amazon 账户管理 HTTPS 查询 API 使您能够以编程方式访问 Amazon Web Services 账户 和 Amazon。HTTPS 查询 API 可让您直接向服务发布 HTTPS 请求。使用 HTTPS API 时，必须添加代码，才能使用您的凭证对请求进行数字化签名。有关更多信息，请参阅[通过提出 HTTP 查询请求来调用 API](#)。

规划您的 Amazon Web Services 账户 治理结构

尽管您可能使用一个账户开始了 Amazon 之旅，但 Amazon 建议您根据增加的工作负载规模和复杂性设置多个账户。无论是中型企业还是大型企业，都需要制定治理结构计划，以确保数据和工作负载需求都得到满足。

本节介绍了 Amazon 中提供的好处和治理服务，以帮助实现多账户治理结构。

主题

- [使用多个 Amazon Web Services 账户 的好处](#)
- [何时使用 Amazon Organizations](#)
- [何时使用 Amazon Control Tower](#)
- [了解 API 的操作模式](#)

使用多个 Amazon Web Services 账户 的好处

Amazon Web Services 账户 构成了 Amazon Web Services 云 中的基础安全边界。它们作为资源的容器，提供了一个关键的隔离层，这对于创建安全、治理良好的环境至关重要。有关更多信息，请参阅[什么是 Amazon Web Services 账户？](#)。

将资源分成不同的 Amazon Web Services 账户 有助于您在云环境中支持以下原则：

- **安全控制**：不同的应用程序可能具有不同的安全配置文件，这些配置文件需要不同的控制策略和机制。例如，可以更轻松地与审计员交谈，并能够指向单个 Amazon Web Services 账户，其中托管遵从[支付卡行业 \(PCI\) 安全标准](#)的所有工作负载元素。
- **隔离** — Amazon Web Services 账户 是安全保护的单位。应在不影响其他账户的情况下，遏制 Amazon Web Services 账户 中的潜在风险和安全威胁。由于采用不同的团队或不同的安全配置文件，可能会带来不同的安全需求。
- **许多团队**：不同的团队有不同的职责和资源需求。可以通过将团队移至单独的 Amazon Web Services 账户 来防止他们互相干扰。
- **数据隔离** – 除了隔离团队之外，将数据存储隔离到一个账户中也很重要。这有助于限制可以访问和管理该数据存储的人数。这有助于遏制高度私有数据的披露，因此有助于遵守[欧盟的《通用数据保护条例》 \(GDPR\)](#)。
- **业务流程** – 不同的业务单位或产品可能有完全不同的目的和流程。借助多个 Amazon Web Services 账户，您可以支持业务单位的特定需求。

- 账单 – 账户是在账单级别分开项目的唯一真正方式。多个账户有助于在账单级别上分开业务单位、职能团队或个人用户的项目。您仍然可以将所有账单合并为单个付款人（使用 Amazon Organizations 和整合账单），同时按 Amazon Web Services 账户分开行项目。
- 配额分配 — 分别为每个 Amazon Web Services 账户强制执行 Amazon 服务配额。将工作负载分成不同的 Amazon Web Services 账户可以防止它们相互占用配额。

本文中描述的所有建议和程序均符合 [Amazon Well-Architected Framework](#)。该框架旨在帮助您设计灵活、有弹性且可扩展的云基础设施。即使您从小规模起步，我们也建议您按照框架中的指导推进。这样做可以帮助您安全地扩展环境，而不会随着企业成长而影响您的持续运营。

管理多个 Amazon Web Services 账户

在开始添加多个账户之前，您需要制定管理这些账户的计划。为此，我们建议您使用 [Amazon Organizations](#)（一项免费 Amazon 服务）来管理组织中的所有 Amazon Web Services 账户。

Amazon 还提供 Amazon Control Tower，该工具为 Organizations 增加多层 Amazon 托管自动化，并自动将其与其他 Amazon 服务（例如 Amazon CloudTrail、Amazon Config、Amazon CloudWatch、Amazon Service Catalog 等）集成。这些服务可能会产生额外费用。有关更多信息，请参阅 [Amazon Control Tower 定价](#)。

另请参阅

- [何时使用 Amazon Organizations](#)
- [何时使用 Amazon Control Tower](#)

何时使用 Amazon Organizations

Amazon Organizations 是一项 Amazon 服务，可用于分组管理 Amazon Web Services 账户。这提供了类似于账单整合的功能，即所有账户的账单都归为一组，并由单一付款人处理。您还可以使用基于策略的控制来集中管理组织的安全。有关 Amazon Organizations 的更多信息，请参阅 [Amazon Organizations 用户指南](#)。

可信访问权限

当使用 Amazon Organizations 分组管理账户时，组织的大部分管理任务只能由组织的管理账户来执行。默认情况下，这只包括与组织自身管理相关的操作。您可以通过启用 Organizations 和其他 Amazon 服务之间的可信访问权限来将此附加功能扩展到此种服务。可信访问权限向指定 Amazon 服

务授予访问组织及其所含账户相关信息的权限。当启用账户管理可信访问权限时，账户管理服务会授予 Organizations 及其管理账户访问组织所有成员账户的元数据（比如主要或备用联系人信息）的权限。

有关更多信息，请参阅 [启用 Amazon 账户管理可信访问权限](#)。

委托管理员

启用可信访问权限后，还可以选择将其中一个成员账户指定为 Amazon 账户管理的委托管理员账户。这样，委托管理员账户就可以为组织中的成员账户执行账户管理元数据的管理任务，而以前只有管理账户才能执行此种任务。委托管理员账户只能访问账户管理服务的管理任务。委托管理员账户不像管理账户那样拥有对组织的所有管理权限。

有关更多信息，请参阅 [为 Amazon 账户管理功能启用委托管理员账户](#)。

启用 Amazon 账户管理可信访问权限

启用 Amazon 账户管理可信访问权限可以使管理账户的管理员修改 Amazon Organizations 中每个成员账户的特定信息和元数据（例如，主要或备用联系人详细信息）。有关更多信息，请参阅《Amazon Organizations 用户指南》中的 [Amazon 账户管理 Amazon Organizations](#)。有关可信访问权限如何运行的一般信息，请参阅 [将 Amazon Organizations 用于其他 Amazon 服务](#)。

启用可信访问权限后，可以在支持 accountID 参数的 [账户管理 API 操作](#) 中使用该参数。只有在使用来自管理账号或组织的委托管理员账号（如果启用）的凭证调用该操作时，才能成功使用此参数。有关更多信息，请参阅 [为 Amazon 账户管理功能启用委托管理员账户](#)。

请按照以下步骤在组织中启用账户管理的可信访问权限。

最小权限

要执行这些任务，您必须满足以下要求：

- 只能从组织的管理账户执行此操作。
- 您的组织必须 [已启用所有功能](#)。

Amazon Web Services Management Console

启用 Amazon 账户管理可信访问权限

1. 登录 [Amazon Organizations 控制台](#)。您必须以 IAM 用户身份登录、担任 IAM 角色，或以组织管理账户中的根用户身份登录（但不建议这样操作）。

2. 在导航窗格中，选择服务。
3. 在服务列表中选择 Amazon 账户管理。
4. 选择 Enable trusted access (启用可信访问)。
5. 在启用 Amazon 账户管理启用可信访问权限对话框中，键入启用进行确认，然后选择启用可信访问权限。

Amazon CLI & SDKs

启用 Amazon 账户管理可信访问权限

运行以下命令后，就可以使用组织管理账户中的凭证调用账户管理 API 操作，这些操作使用 `--accountId` 参数来引用组织中的成员账户。

- Amazon CLI : [enable-aws-service-access](#)

以下示例在调用账户的组织中启用了 Amazon 账户管理可信访问权限。

```
$ aws organizations enable-aws-service-access \  
--service-principal account.amazonaws.com
```

如果成功，此命令不会产生任何输出。

为 Amazon 账户管理功能启用委托管理员账户

请启用委托管理员账户，以便能够在 Amazon 中为其他成员账户调用 Amazon Organizations 账户管理 API 操作。为组织注册委托管理员账户之后，该账户中的用户和角色可以调用 `account` 命名空间中的 Amazon CLI 和 Amazon SDK 操作，这些操作支持可选的 `AccountId` 参数，可以在 Organizations 模式下运行。

要将组织中的成员账户注册为委托管理员账户，请按照以下步骤操作。

Amazon CLI & SDKs

为账户管理服务注册委托管理员账户

您可以使用以下命令，为账户管理服务启用委托管理员。

最小权限

要执行这些任务，您必须满足以下要求：

- 只能从组织的管理账户执行此操作。
- 您的组织必须 [已启用所有功能](#)。
- 您必须 [已经在组织中启用了账户管理的可信访问权限](#)。

您必须指定以下服务主体：

```
account.amazonaws.com
```

- Amazon CLI : [register-delegated-administrator](#)

以下示例将组织的成员账户注册为适用于账户管理服务的委托管理员。

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

如果成功，此命令不会产生任何输出。

运行此命令后，就可以使用账户 123456789012 中的凭证调用账户管理 Amazon CLI 和 SDK API 操作，这些操作使用 `--account-id` 参数来引用组织中的成员账户。

Amazon Web Services Management Console

Amazon 账户管理控制台不支持此任务。只能使用来自其中一个 Amazon SDK 的 Amazon CLI 或 API 操作来执行此任务。

何时使用 Amazon Control Tower

Amazon Organizations 基础服务使您能够集中管理和保护整个 Amazon 环境。这种以 Amazon Organizations 为中心的方法包含一个关键组件 Amazon Control Tower。Amazon Control Tower 用作组织中的管理控制台，通过应用规范性最佳实践，提供一种简化的方法来设置和管理安全的多账户 Amazon 环境。

Amazon Control Tower 提供的这种安全最佳实践方法扩展了 Amazon Organizations 的核心功能。Amazon Control Tower 应用一组预防和侦查性护栏，帮助确保您的组织和账户一直符合建议的安全和合规标准。

通过使用 Amazon Control Tower 建立架构良好的 Amazon Organizations 结构，就可以快速部署可扩展、安全且合规的 Amazon 环境。这种集中式云管理和治理方法对于希望充分利用 Amazon Web Services 云的强大功能，同时保持最高安全性和合规性标准的企业来说至关重要。

有关更多信息，请参阅 Amazon Control Tower 用户指南 中的 [什么是 Amazon Control Tower ?](#)。

了解 API 的操作模式

与 Amazon Web Services 账户 属性配合使用的 API 操作始终采用以下两种操作模式之一：

- 独立上下文 — 此模式用于某个账户用户或角色访问或更改同一账户中的账户属性时。如果在调用账户管理 Amazon CLI 或 Amazon SDK 操作时未包含 `AccountId` 参数，则会自动使用独立上下文模式。
- 组织上下文 — 此模式用于组织中某个账户用户或角色访问或更改同一组织中不同成员账户的账户属性时。如果在调用账户管理 Amazon CLI 或 Amazon SDK 操作时确实包含了 `AccountId` 参数，则会自动使用组织上下文模式。此模式下，只能通过组织的管理账户或账户管理的委托管理员账户调用操作。

Amazon CLI 和 Amazon SDK 操作可以在独立上下文或组织上下文中运行。

- 如果您未包含 `AccountId` 参数，则此操作运行在独立上下文中，并自动将请求应用到您用于发出请求的账户。无论账户是否为组织的成员账户，都是如此。
- 如果确实包含了 `AccountId` 参数，则此操作运行在组织上下文中，并且此操作还在指定的组织账户上运行。
 - 如果调用此操作的账户是管理账户或账户管理服务的委托管理员账户，则可以在 `AccountId` 参数中指定该组织的任何成员账户来更新指定的账户。
 - 组织中唯一可以调用备用联系人操作并在 `AccountId` 参数中指定其自有账号的账户是指定为账户管理服务 [委托管理员账户](#) 的账户。其他任何账户，包括管理账户，都会收到 `AccessDenied` 异常。
- 如果在独立模式下运行操作，则必须获准使用 IAM 策略运行该操作，该策略包含的 `Resource` 元素或者为允许所有资源的 "*"，或者为 [使用独立账户语法的 ARN](#)。
- 如果在组织模式下运行操作，则必须获准使用 IAM 策略运行该操作，该策略包含的 `Resource` 元素或者为允许所有资源的 "*"，或者为 [使用组织成员账户语法的 ARN](#)。

授予更新账户属性的权限

与大多数 Amazon 操作一样，您可以使用 [IAM 权限策略](#) 授予添加、更新或删除 Amazon Web Services 账户的账户属性的权限。在向 IAM 主体（用户或角色）附加 IAM 权限策略时，可以指定主体可以在哪些资源上以及在什么条件下执行哪些操作。

以下是创建权限策略时针对账户管理的一些注意事项。

Amazon Web Services 账户的 Amazon 资源名称格式

- 根据要引用的账户是独立账户还是组织账户，可以将其包含在策略语句的 resource 元素中的 Amazon Web Services 账户的 [Amazon 资源名称 \(ARN\)](#) 会呈现不同的构造。请参阅 [了解 API 的操作模式](#) 中的上一部分。
- 独立账户的账户 ARN：

```
arn:aws:account::{AccountId}:account
```

在不包括 AccountID 参数的独立模式下运行账户属性操作时，必须使用此种格式。

- 组织成员账户的账户 ARN：

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

在包括 AccountID 参数的组织模式下运行账户属性操作时，必须使用此种格式。

IAM 策略的上下文键

账户管理服务还提供多个 [账户管理服务专属条件键](#)，可对您授予的权限进行精细控制。

account:AccountResourceOrgPaths

上下文键 `account:AccountResourceOrgPaths` 允许指定一条通过组织层次结构到达特定组织单位 (OU) 的路径。只有该 OU 所包含的成员账户才符合条件。以下示例片段将策略限制为仅适用于两个指定 OU 中任一 OU 的账户。

由于 `account:AccountResourceOrgPaths` 是多值字符串类型，因此必须使用 [ForAnyValue](#) 或 [ForAllValues](#) 多值字符串运算符。另请注意，条件键的前缀是 `account`，即使您引用的是通往组织中 OU 的路径。


```
"Condition": {
  "ForAnyValue:StringLike": {
    "account:AccountResource0rgPaths": [
      "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",
      "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"
    ]
  }
}
```

account:AccountResource0rgTags

上下文键 `account:AccountResource0rgTags` 允许您引用可以附加到组织账户的标签。标签是可以用来说明账户中资源进行分类和标记的键值字符串对。有关更多信息，请参阅《Amazon Resource Groups 用户指南》中的[标签编辑器](#)。有关在基于属性的访问控制策略中使用标签的信息，请参阅《IAM 用户指南》中的[什么是 Amazon 的 ABAC](#)。以下示例片段将策略限制为仅适用于组织中具有键 `project` 和值 `blue` 或 `red` 的标签的账户。

由于 `account:AccountResource0rgTags` 是多值字符串类型，因此必须使用 [ForAnyValue 或 ForAllValues 多值字符串](#) 运算符。另请注意，条件键的前缀是 `account`，即使您引用的是组织成员账户上的标签。

```
"Condition": {
  "ForAnyValue:StringLike": {
    "account:AccountResource0rgTags/project": [
      "blue",
      "red"
    ]
  }
}
```

Note

您只能将标签附加到组织中的账户。您无法将标签附加到独立 Amazon Web Services 账户。

配置你的 Amazon Web Services 账户

本节包含的主题描述了如何管理您的 Amazon Web Services 账户。

Note

如果你 Amazon Web Services 账户 是在印度使用创建的 Amazon Internet Services Private Limited (AISPL)，还有其他注意事项。有关更多信息，请参阅 [管理印度地区的账户](#)。

主题

- [创建 Amazon Web Services 账户 别名](#)
- [在您的账户中启用或禁用 Amazon Web Services 区域](#)
- [更新 Amazon Web Services 账户 的账单](#)
- [更新根用户的 Amazon Web Services 账户 名称、电子邮件地址或密码](#)
- [更新 Amazon Web Services 账户 的备用联系人](#)
- [更新 Amazon Web Services 账户 的主要联系人](#)
- [查看 Amazon Web Services 账户 标识符](#)

创建 Amazon Web Services 账户 别名

如果您希望 IAM 用户的 URL 包含您的公司名称（或易于记忆的其他标识符）而不是 Amazon Web Services 账户 ID，则可以创建一个账户别名。

要了解如何创建或更新账户别名，请参阅《IAM 用户指南》中的[为您的 Amazon Web Services 账户 ID 使用别名](#)。

在您的账户中启用或禁用 Amazon Web Services 区域

Amazon Web Services 区域 是指全球范围内的某个物理位置，每个区域由多个可用区组成。可用区由一个或多个分散的 Amazon 数据中心组成，每个都拥有独立的配套设施，其中包括冗余电源、联网和连接。这意味着每个 Amazon Web Services 区域 都是物理隔离的，并独立于其他区域。区域提供容错能力、稳定性和弹性，还可以减少延迟。有关可用区域和即将推出区域的地图，请参阅 [区域和可用区](#)。

除非您明确使用 Amazon 服务提供的复制功能，否则在一个区域中创建的资源在任何其他区域中都不存在。例如，Amazon S3 和 Amazon EC2 支持跨区域复制。某些服务（例如 Amazon Identity and Access Management (IAM)）没有区域资源。

您的账户确定了适用于您的区域。

- Amazon Web Services 账户 提供多个区域，因此您可在满足您要求的位置启动 Amazon 资源。例如，您可能希望在欧洲区域启动 Amazon EC2 实例以更多符合欧洲客户的要求或满足法律要求。
- Amazon GovCloud (美国西部) 账户提供对 Amazon GovCloud (美国西部) 区域和 Amazon GovCloud (美国东部) 区域的访问。有关更多信息，请参阅 [Amazon GovCloud \(US\)](#)。
- 您只能通过 Amazon (Amazon 中国) 账户访问北京和宁夏区域。有关更多信息，请参阅 [中国的 Amazon Web Services](#)。

Important

Amazon 建议使用区域性 Amazon Security Token Service (Amazon STS) 端点来减小延迟，而不是使用全局端点。来自区域 Amazon STS 端点的会话令牌在所有 Amazon 区域中都有效。如果使用区域性 Amazon STS 端点，则无需进行任何更改。但是，来自全局 Amazon STS 端点 (<https://sts.amazonaws.com>) 的会话令牌仅适用于您所启用或默认启用的 Amazon Web Services 区域。如果打算为账户启用新的区域，您可以使用来自区域性 Amazon STS 端点的会话令牌或激活全局 Amazon STS 端点来发放适用于所有 Amazon Web Services 区域的会话令牌。适用于所有区域的会话令牌较大。如果存储会话令牌，这些较大的令牌可能会影响您的系统。有关 Amazon STS 端点如何使用 Amazon 区域的更多信息，请参阅 [在 Amazon 区域中管理 Amazon STS](#)。

主题

- [启用和禁用区域之前的注意事项](#)
- [为独立账户启用或禁用区域](#)
- [在组织中启用或禁用区域](#)

启用和禁用区域之前的注意事项

在启用或禁用区域之前，务必考虑以下几点：

- 默认启用 2019 年 3 月 20 日之前推出的区域 - Amazon 最初默认启用所有新的 Amazon Web Services 区域，这意味着您可以立即开始在这些区域中创建和管理资源。您无法启用或禁用默认已启用的区域。现在，当 Amazon 添加区域时，默认情况下禁用新区域。如果希望用户能够在新区域中创建和管理资源，您首先要启用该区域。默认情况下禁用以下区域。

名称	代码
Africa (Cape Town)	af-south-1
亚太地区 (香港)	ap-east-1
亚太地区 (海得拉巴)	ap-south-2
亚太地区 (雅加达)	ap-southeast-3
亚太地区 (墨尔本)	ap-southeast-4
加拿大 (卡尔加里)	ca-west-1
欧洲地区 (米兰)	eu-south-1
欧洲 (西班牙)	eu-south-2
欧洲 (苏黎世)	eu-central-2
以色列 (特拉维夫)	il-central-1
中东 (巴林)	me-south-1
中东 (阿联酋)	me-central-1

- 您可以使用 IAM 权限控制区域的访问权限 - Amazon Identity and Access Management (IAM) 包含四个可让您控制哪些用户可以启用、禁用、获取和列出区域的权限。有关更多信息，请参阅《IAM 用户指南》中的 [Amazon：允许启用和禁用 Amazon Web Services 区域](#)。您还可以使用 [aws:RequestedRegion](#) 条件键控制对 Amazon Web Services 区域中的 Amazon Web Services 服务的访问权限。
- 启用区域免费 - 启用区域无需付费。您只需为在新区域中创建的资源付费。
- 禁用区域可禁用对区域中资源的 IAM 访问权限 – 如果禁用了仍含有 Amazon 资源 (比如 Amazon Elastic Compute Cloud (Amazon EC2) 实例) 的区域，则会丧失对此区域内资源的 IAM 访问权限。

例如，您无法使用 Amazon Web Services Management Console 查看或更改该禁用区域中任何 EC2 实例的配置。

- 禁用区域后活动资源继续收费 – 如果禁用了仍含有 Amazon 资源的区域，这些资源（如有）继续按标准费率产生费用。例如，如果禁用包含 Amazon EC2 实例的区域，则即使实例不可访问，您仍然必须为这些实例支付费用。
- 禁用区域并非总是立即可见 - 禁用区域后，服务和控制台可能会暂时可见。禁用区域可能需要几分钟到几小时才能生效。
- 在某些情况下启用一个区域需要几分钟到几小时的时间 - 在启用一个区域时，Amazon 将执行操作以准备您在该区域内的账户，例如将您的 IAM 资源分发给该区域。对大多数账户而言，此过程需要几分钟时间，但有时可能需要几小时。在此过程完成之前，您无法使用区域。
- 整个 Amazon 组织可以在给定时间有 50 个开启的区域选择请求 - 管理账户可以在任何时间点有 50 个等待为其组织完成的请求。一个请求等于为一个账户启用或禁用一个特定区域。
- 一个账户在任何给定时间可以有 6 个处理中的区域选择请求 - 一个请求等于为一个账户启用或禁用一个特定区域。
- Amazon EventBridge 集成 — 客户可以在 EventBridge 中订阅区域选择状态更新通知。每次状态变化时将创建 EventBridge 通知，这样客户就可以自动执行工作流程。
- 直观的区域选择状态 - 由于启用/禁用选择加入区域的异步性质，因此区域选择请求有四种潜在状态：
 - ENABLING
 - DISABLING
 - ENABLED
 - DISABLED

当选择加入或选择退出处于 ENABLING 或 DISABLING 状态时，无法将其取消。否则将抛出 ConflictException。已完成（启用/禁用）区域选择请求取决于关键底层服务的配置。Amazon 尽管有些 Amazon 服务的状态为 ENABLED，但可能无法立即使用。

- 完全集成 Amazon Organizations - 管理账户可以为 Amazon 组织的任何成员账户修改或读取区域选择。成员账户也可以读取/写入其区域状态。

为独立账户启用或禁用区域

要更新 Amazon Web Services 账户 有权访问的区域，请执行以下流程中的步骤。以下 Amazon Web Services Management Console 流程仅在独立上下文中始终有效。可以使用 Amazon Web Services Management Console 只查看或更新操作调用账户中的可用区域。

Amazon Web Services Management Console

为独立 Amazon Web Services 账户 启用或禁用区域

最小权限

要执行下列程序中的步骤，IAM 用户或角色必须具有以下权限：

- `account:ListRegions` (需要查看 Amazon Web Services 区域 列表以及它们当前处于启用还是禁用状态)。
- `account:EnableRegion`
- `account:DisableRegion`

1. 以 Amazon Web Services 账户根用户 或者具有最低权限的 IAM 用户或角色身份登录 [Amazon Web Services Management Console](#)。
2. 在窗口的右上角，选择您的账户名称，然后选择账户。
3. 在[账户页面](#)，向下滚动至 Amazon Web Services 区域 部分。

Note

系统可能会提示您批准对此信息的访问权限。Amazon 向与账户关联的电子邮件地址和主要联系人电话号码发送请求。选择请求中的链接以在浏览器中将其打开，然后批准此访问权限。

4. 在操作列中带有选项的各个 Amazon Web Services 区域 旁边，选择启用或禁用，具体取决于是否希望账户中的用户能够在此区域中创建和访问资源。
5. 如果有提示，请确认选择。
6. 完成所有更改后，选择更新。

Amazon CLI & SDKs

您可以使用以下 Amazon CLI 命令或其 Amazon SDK 等效操作，启用、禁用、读取和列出区域选择状态：

- `EnableRegion`
- `DisableRegion`

- `GetRegionOptStatus`
- `ListRegions`

最小权限

要执行下列步骤，您必须拥有映射到此操作的权限：

- `account:EnableRegion`
- `account:DisableRegion`
- `account:GetRegionOptStatus`
- `account:ListRegions`

如果使用这些单独权限，就可以授予某些用户仅读取区域选择信息的权限，而授予其他用户同时读取和写入的权限。

以下示例为组织的指定成员账户启用了区域。所用凭证必须来自组织管理账户或账户管理委托管理员账户。

请注意，您也可以使用相同的命令禁用某个区域，然后将 `enable-region` 替换为 `disable-region`。

```
aws account enable-region --region-name af-south-1
```

如果成功，此命令不会产生任何输出。

该操作是异步的。以下命令可以使您查看请求的最新状态。

```
aws account get-region-opt-status --region-name af-south-1
{
  "RegionName": "af-south-1",
  "RegionOptStatus": "ENABLING"
}
```

在组织中启用或禁用区域

要更新 Amazon Organizations 成员账户的启用区域，请执行以下流程中的步骤。

Note

Amazon Organizations 托管策略 `AWSOrganizationsReadOnlyAccess` 或 `AWSOrganizationsFullAccess` 更新为提供访问 Amazon 账户管理 API 的权限，这样您就可以从 Amazon Organizations 控制台访问账户数据。要查看更新的托管策略，请参阅 [Organizations Amazon 托管策略的更新](#)。

Note

在通过管理账户或组织中的委托管理员账户为成员账户执行这些操作之前，您必须：

- 启用组织中的所有功能，管理成员账户的设置。这样管理员就可以控制成员账户。这是在创建组织时默认设置的。如果您的组织设置为仅整合账单，而您要启用所有功能，请参阅[在组织中启用所有功能](#)。
- 启用 Amazon 账户管理服务可信访问权限。要进行设置，请参阅 [启用 Amazon 账户管理可信访问权限](#)。

Amazon Web Services Management Console

在组织中启用或禁用区域

1. 使用您的组织的管理账户凭证登录 Amazon Organizations 控制台。
2. 在 Amazon Web Services 账户 页面上，选择要更新的账户。
3. 选择账户设置选项卡。
4. 在区域下，选择要启用或禁用的区域。
5. 选择操作，然后选择启用或禁用选项。
6. 如果选择了启用选项，请查看显示的文本，然后选择启用区域。
7. 如果选择了禁用选项，请查看显示的文本，键入 `disable` 进行确认，然后选择禁用区域”。

Amazon CLI & SDKs

您可以使用以下 Amazon CLI 命令或其 Amazon SDK 等效操作，为组织成员账户启用、禁用、读取和列出区域选择状态：

- `EnableRegion`

- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

最小权限

要执行下列步骤，您必须拥有映射到此操作的权限：

- `account:EnableRegion`
- `account:DisableRegion`
- `account:GetRegionOptStatus`
- `account:ListRegions`

如果使用这些单独权限，就可以授予某些用户仅读取区域选择信息的权限，而授予其他用户同时读取和写入的权限。

以下示例为组织的指定成员账户启用了区域。所用凭证必须来自组织管理账户或账户管理委托管理员账户。

请注意，您也可以使用相同的命令禁用某个区域，然后将 `enable-region` 替换为 `disable-region`。

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

如果成功，此命令不会产生任何输出。

Note

一个组织在给定时间最多只能有 20 个区域请求。否则，您会收到 `TooManyRequestsException`。

该操作是异步的。以下命令可以使您查看请求的最新状态。

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1  
{
```

```
"RegionName": "af-south-1",  
"RegionOptStatus": "ENABLING"  
}
```

更新 Amazon Web Services 账户 的账单

您可以使用 Amazon Billing 和成本管理控制台更新所有 Amazon Web Services 账户 账单首选项。要了解如何更新账户的账单相关设置，请参阅 [《Amazon Billing and Cost Management 用户指南》](#)：

更新根用户的 Amazon Web Services 账户 名称、电子邮件地址或密码

要编辑 Amazon Web Services 账户 的名称或更改根用户的密码或用户电子邮件地址，请执行以下流程中的步骤。此电子邮件地址和密码是您以 Amazon Web Services 账户根用户 身份登录的凭证。

Note

对 Amazon Web Services 账户 的更改最多可能需要四小时才能传播到任何地方。

Amazon Web Services Management Console

编辑您的 Amazon Web Services 账户 名称、根用户密码和根用户用户电子邮件地址

最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 您必须以 Amazon Web Services 账户根用户 登录，这将不需要其他 IAM 权限。您无法以 IAM 用户或角色身份执行这些步骤。

1. 使用您的 Amazon Web Services 账户 电子邮件地址和密码以 Amazon Web Services 账户根用户 身份登录到 [Amazon Web Services Management Console](#)。
2. 在控制台的右上角，选择您的账户名称或账号，然后选择 Account (账户)。
3. 在 [账户页面](#) 上的账户设置旁，选择编辑。出于安全考虑，系统会提示您重新验证身份。

Note

如果您没有看到编辑选项，则可能是因为你并非以账户根用户身份登录。以 IAM 用户或角色身份登录时，您无法修改账户设置。

4. 在更新账户设置页面上，选择要更新字段旁边的编辑。
 - a. 对于姓名 — 在更新您的账户名称页面中，在新账户名称中输入新的账户名称，然后选择保存更改。

Note

如果无法修改 Amazon Web Services 账户名称，请检查 Amazon Organizations 中是否存在限制访问 `account` 或设置为拒绝 `iam:UpdateAccountName` 操作的服务控制策略 (SCP)。

- b. 对于电子邮件 — 在更新您的电子邮件地址页面上，填写新电子邮件地址、确认新电子邮件地址和确认您的当前密码字段。然后选择 `Save changes` (保存更改)。`no-reply@verify.signin.aws` 将向新的电子邮件地址发送验证码。在验证您的新电子邮件地址页面，在验证码下输入从电子邮件中收到的验证码，然后选择保存更改。

Note

验证码可能需要最多 5 分钟时间才能到达。如果您在收件箱中未看到此邮件，请检查垃圾邮件文件夹。

- c. 对于密码 - 在更新密码页面上，填写当前密码、新密码和确认新密码字段。然后选择 `Save changes` (保存更改)。有关其他指导，包括设置根用户密码的最佳实践，请参阅《IAM 用户指南》中的[更改 Amazon Web Services 账户根用户的密码](#)。

5. 完成所有更改后，选择完成。

Amazon CLI & SDKs

Amazon CLI 或来自任何一种 Amazon 的 API 操作均不支持此任务。您只能使用 Amazon Web Services Management Console 执行此任务。

更新 Amazon Web Services 账户 的备用联系人

通过备用联系人，Amazon 最多可以联系三个与此账户关联的备用联系人。备用联系人不一定是特定人员。如果您拥有负责管理账单、运营和安全相关问题的团队，则可以添加电子邮件分发列表。除此之外，还有与账户的[根用户](#)关联的电子邮件地址。[主账户联系人](#)将继续接收发往根账户电子邮件的所有电子邮件通信。

您只能从与账户关联的以下联系人类型中指定一个类型。

- 账单联系人
- 操作联系人
- 安全联系人

您可以根据账户是独立账户还是组织的一部分，以不同方式添加或编辑备用联系人：

- 独立 Amazon Web Services 账户 - 对于未与组织关联的 Amazon Web Services 账户，您可以使用 Amazon 管理控制台或通过 Amazon CLI 和 SDK 更新自己的备用联系人。要了解如何执行此操作，请参阅[更新独立 Amazon Web Services 账户 备用联系人](#)。
- 组织内的 Amazon Web Services 账户 - 对于属于 Amazon 组织的成员账户，管理账户或委托管理员账户中的用户可以从 Amazon Organizations 控制台集中更新组织中的任何成员账户，也可以通过 Amazon CLI 和 SDK 以编程方式更新。要了解如何执行此操作，请参阅[更新您组织中的 Amazon Web Services 账户 备用联系人](#)。

主题

- [电话号码和电子邮件地址要求](#)
- [为独立 Amazon Web Services 账户 更新备用联系人](#)
- [更新您组织中任意 Amazon Web Services 账户 的备用联系人](#)
- [account:AlternateContactTypes 上下文键](#)

电话号码和电子邮件地址要求

在继续更新账户的备用联系人信息之前，我们建议在输入电话号码和电子邮件地址时先查看以下要求。

- 电话号码只能包含数字、空格和以下字符：“+-()”。

- 电子邮件地址最长可以有 254 个字符，除了标准的字母数字字符外，还可以在电子邮件地址的局部包含以下特殊字符：“+ = . # | ! & - _”。

为独立 Amazon Web Services 账户 更新备用联系人

要为独立 Amazon Web Services 账户 添加或编辑备用联系人，请执行以下流程中的步骤。以下 Amazon Web Services Management Console 流程仅在独立上下文中始终有效。可以使用 Amazon Web Services Management Console 只访问或更改操作调用账户中的备用联系人。

Amazon Web Services Management Console

为独立 Amazon Web Services 账户 添加或编辑备用联系人

最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- `account:GetAlternateContact` (查看备用联系人详细信息)
- `account:PutAlternateContact` (设置或更新备用联系人)
- `account>DeleteAlternateContact` (删除备用联系人)

1. 以具有最低权限的 IAM 用户或角色登录 [Amazon Web Services Management Console](#)。
2. 在窗口的右上角，选择您的账户名称，然后选择账户。
3. 在[账户页面](#)上，向下滚动到备用联系人，在标头右侧选择编辑。

Note

如果您没有看到编辑选项，则可能是因为你并非以账户根用户或具有上述最低权限之人的身份登录。

4. 更改任何可用字段中的值。

⚠ Important

对于企业 Amazon Web Services 账户，最佳做法是输入公司而非个人的电话号码和电子邮件地址。

5. 完成所有更改后，选择更新。

Amazon CLI & SDKs

您可以使用以下 Amazon CLI 命令或其 Amazon SDK 等效操作，检索、更新或删除备用联系人信息：

- [GetAlternateContact](#)
- [PutAlternateContact](#)
- [DeleteAlternateContact](#)

ⓘ 注意

- 要通过管理账户或组织中的委托管理员账户对成员账户执行这些操作，必须[启用账户服务可信访问权限](#)。

ⓘ 最小权限

对于各个操作，您必须具有映射到此操作的权限：

- `GetAlternateContact` (查看备用联系人详细信息)
- `PutAlternateContact` (设置或更新备用联系人)
- `DeleteAlternateContact` (删除备用联系人)

如果使用这些单独权限，就可以授予某些用户仅读取联系人信息的权限，而授予其他用户同时读取和写入的权限。

Example

以下示例检索了调用方账户的当前账单备用联系人。

```
$ aws account get-alternate-contact \
  --alternate-contact-type=BILLING
{
  "AlternateContact": {
    "AlternateContactType": "BILLING",
    "EmailAddress": "saanvi.sarkar@amazon.com",
    "Name": "Saanvi Sarkar",
    "PhoneNumber": "+1(206)555-0123",
    "Title": "CFO"
  }
}
```

Example

以下示例为调用方账户设置了新的操作备用联系人。

```
$ aws account put-alternate-contact \
  --alternate-contact-type=OPERATIONS \
  --email-address=mateo_jackson@amazon.com \
  --name="Mateo Jackson" \
  --phone-number="+1(206)555-1234" \
  --title="Operations Manager"
```

如果成功，此命令不会产生任何输出。

Example

Note

如果对相同 Amazon Web Services 账户 和相同联系人类型执行多次 PutAlternateContact 操作，则第一个操作会添加新联系人，而随后对相同 Amazon Web Services 账户 和联系人类型的所有调用会更新现有联系人。

Example

以下示例删除了调用方账户的安全备用联系人。

```
$ aws account delete-alternate-contact \  
--alternate-contact-type=SECURITY
```

如果成功，此命令不会产生任何输出。

Note

如果尝试多次删除同一个联系人，第一次会静默成功。之后所有尝试都会生成 ResourceNotFound 异常。

更新您组织中任意 Amazon Web Services 账户 的备用联系人

要为组织中的任何 Amazon Web Services 账户 添加或编辑备用联系人详细信息，请执行以下流程中的步骤。

要求

要使用 Amazon Organizations 控制台更新备用联系人，您需要进行一些初步设置：

- 您的组织必须启用所有功能才能管理成员账户的设置。这样管理员就可以控制成员账户。这是在创建组织时默认设置的。如果您的组织设置为仅整合账单，而您要启用所有功能，请参阅[在组织中启用所有功能](#)。
- 您需要启用 Amazon 账户管理服务可信访问权限。要进行此设置，请参阅[启用 Amazon 账户管理可信访问权限](#)。

Note

Amazon Organizations 托管策略 `AWSOrganizationsReadOnlyAccess` 或 `AWSOrganizationsFullAccess` 更新为提供访问 Amazon 账户管理 API 的权限，这样您就可以从 Amazon Organizations 控制台访问账户数据。要查看更新的托管策略，请参阅[Organizations Amazon 托管策略的更新](#)。

Amazon Web Services Management Console

为组织中的任何 Amazon Web Services 账户 添加或编辑备用联系人

1. 使用组织的管理账户凭证登录 [Amazon Organizations 控制台](#)。
2. 从 Amazon Web Services 账户 中，选择要更新的账户。
3. 选择联系人信息，然后在备用联系人下找到联系人类型：账单联系人、安全联系人或运营联系人。
4. 要添加新联系人，请选择添加。或者要更新现有联系人，请选择编辑。
5. 更改任何可用字段中的值。

Important

对于企业 Amazon Web Services 账户，最佳做法是输入公司而非个人的电话号码和电子邮件地址。

6. 完成所有更改后，选择更新。

Amazon CLI & SDKs

您可以使用以下 Amazon CLI 命令或其 Amazon SDK 等效操作，检索、更新或删除备用联系人信息：

- [GetAlternateContact](#)
- [PutAlternateContact](#)
- [DeleteAlternateContact](#)

注意

- 要通过管理账户或组织中的委托管理员账户对成员账户执行这些操作，必须 [启用账户服务可信访问权限](#)。
- 您无法访问与您的操作调用组织不同的组织中的账户。

i 最小权限

对于各个操作，您必须具有映射到此操作的权限：

- `GetAlternateContact` (查看备用联系人详细信息)
- `PutAlternateContact` (设置或更新备用联系人)
- `DeleteAlternateContact` (删除备用联系人)

如果使用这些单独权限，就可以授予某些用户仅读取联系人信息的权限，而授予其他用户同时读取和写入的权限。

Example

以下示例检索了组织中调用方账户的当前账单备用联系人。所用凭证必须来自组织管理账户或账户管理委托管理员账户。

```
$ aws account get-alternate-contact \
  --alternate-contact-type=BILLING \
  --account-id 123456789012
{
  "AlternateContact": {
    "AlternateContactType": "BILLING",
    "EmailAddress": "saanvi.sarkar@amazon.com",
    "Name": "Saanvi Sarkar",
    "PhoneNumber": "+1(206)555-0123",
    "Title": "CFO"
  }
}
```

Example

以下示例为组织中的指定成员账户设置了操作备用联系人。所用凭证必须来自组织管理账户或账户管理委托管理员账户。

```
$ aws account put-alternate-contact \
  --account-id 123456789012 \
```

```
--alternate-contact-type=OPERATIONS \  
--email-address=mateo_jackson@amazon.com \  
--name="Mateo Jackson" \  
--phone-number="+1(206)555-1234" \  
--title="Operations Manager"
```

如果成功，此命令不会产生任何输出。

Note

如果对相同 Amazon Web Services 账户 和相同联系人类型执行多次 PutAlternateContact 操作，则第一个操作会添加新联系人，而随后对相同 Amazon Web Services 账户 和联系人类型的所有调用会更新现有联系人。

Example

以下示例删除了组织中指定成员账户的安全备用联系人。所用凭证必须来自组织管理账户或账户管理委托管理员账户。

```
$ aws account delete-alternate-contact \  
--account-id 123456789012 \  
--alternate-contact-type=SECURITY
```

如果成功，此命令不会产生任何输出。

Example

Note

如果尝试多次删除同一个联系人，第一次会静默成功。之后所有尝试都会生成 ResourceNotFound 异常。

account:AlternateContactTypes 上下文键

可以使用上下文键 `account:AlternateContactTypes` 指定 IAM 策略允许（或拒绝）的三种账单类型中之一。例如，以下示例 IAM 权限策略使用此条件键，允许附加的主体仅检索组织中特定账户的 BILLING 备用联系人，但不能进行修改。

由于 `account:AlternateContactTypes` 是多值字符串类型，因此必须使用 [ForAnyValue](#) 或 [ForAllValues](#) 多值字符串运算符。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "account:GetAlternateContact",
      "Resource": [
        "arn:aws:account::123456789012:account/o-aa111bb222/111111111111"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "account:AlternateContactTypes": [
            "BILLING"
          ]
        }
      }
    }
  ]
}
```

更新 Amazon Web Services 账户 的主要联系人

您可更新与账户相关联的主要联系人信息，包括您的联系人全名、公司名称、邮寄地址、电话号码和网址。

您可以根据账户是独立账户还是组织的一部分，以不同方式编辑主账户联系人：

- 独立 Amazon Web Services 账户 - 对于未与组织关联的 Amazon Web Services 账户，您可以使用 Amazon 管理控制台或通过 Amazon CLI 和 SDK 更新自己的主账户联系人。要了解如何执行此操作，请参阅[更新独立 Amazon Web Services 账户 主要联系人](#)。
- 组织内的 Amazon Web Services 账户 - 对于属于 Amazon 组织的成员账户，管理账户或委托管理员账户中的用户可以从 Amazon Organizations 控制台集中更新组织中的任何成员账户，也可以通过 Amazon CLI 和 SDK 以编程方式更新。要了解如何执行此操作，请参阅[更新您组织中的 Amazon Web Services 账户 主要联系人](#)。

主题

- [电话号码和电子邮件地址要求](#)
- [为独立 Amazon Web Services 账户 更新主要联系人](#)
- [更新您组织中任意 Amazon Web Services 账户 的主要联系人](#)

电话号码和电子邮件地址要求

在继续更新账户的主要联系人信息之前，我们建议在输入电话号码和电子邮件地址时先查看以下要求。

- 电话号码只能包含数字。
- 电话号码必须以 + 和国家/地区代码开头，并且国家/地区代码后面不得有任何前导零或多余的空格。例如，+1（美国/加拿大）或 +44（英国）。
- 电话号码不得在区号、局号和本地代码之间包含连字符“-”或空格。例如，+12025550179。
- 出于安全起见，电话号码必须能够接收来自 Amazon 的短信。不接受免费电话号码，因为大多数免费电话都不支持短信。
- 对于企业 Amazon Web Services 账户，最佳做法是输入公司而非个人的电话号码和电子邮件地址。如果使用个人电子邮件地址或电话号码配置账户的[根用户](#)，那么在相关人员离开公司后就难以恢复账户。

为独立 Amazon Web Services 账户 更新主要联系人

要为独立 Amazon Web Services 账户 编辑主要联系人的详细信息，请执行以下流程中的步骤。以下 Amazon Web Services Management Console 流程仅在独立上下文中始终有效。可以使用 Amazon Web Services Management Console 只访问或更改操作调用账户中的主要联系人信息。

Amazon Web Services Management Console

为独立 Amazon Web Services 账户 编辑主要联系人

最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- `account:GetContactInformation`（查看主要联系人详细信息）
- `account:PutContactInformation`（更新主要联系人详细信息）

1. 以具有最低权限的 IAM 用户或角色登录 [Amazon Web Services Management Console](#)。
2. 在窗口的右上角，选择您的账户名称，然后选择账户。
3. 向下滚动到联系人信息部分，在其旁边选择编辑。
4. 更改任何可用字段中的值。
5. 完成所有更改后，选择更新。

Amazon CLI & SDKs

您可以使用以下 Amazon CLI 命令或其 Amazon SDK 等效操作，检索、更新或删除主要联系人信息：

- [GetContactInformation](#)
- [PutContactInformation](#)

注意

- 要通过管理账户或组织中的委托管理员账户对成员账户执行这些操作，必须[启用账户服务可信访问权限](#)。

最小权限

对于各个操作，您必须具有映射到此操作的权限：

- `account:GetContactInformation`
- `account:PutContactInformation`

如果使用这些单独权限，就可以授予某些用户仅读取联系人信息的权限，而授予其他用户同时读取和写入的权限。

Example

以下示例检索了调用方账户的当前主要联系人信息。

```
$ aws account get-contact-information
```

```
{
  "ContactInformation": {
    "AddressLine1": "123 Any Street",
    "City": "Seattle",
    "CompanyName": "Example Corp, Inc.",
    "CountryCode": "US",
    "DistrictOrCounty": "King",
    "FullName": "Saanvi Sarkar",
    "PhoneNumber": "+15555550100",
    "PostalCode": "98101",
    "StateOrRegion": "WA",
    "WebsiteUrl": "https://www.examplecorp.com"
  }
}
```

Example

以下示例为调用方账户设置了新的主要联系人信息。

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
"StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

如果成功，此命令不会产生任何输出。

更新您组织中任意 Amazon Web Services 账户 的主要联系人

要在组织中的任何 Amazon Web Services 账户 中编辑主要联系人的详细信息，请执行以下流程中的步骤。

其他要求

要使用 Amazon Organizations 控制台更新主要联系人，您需要进行一些初步设置：

- 您的组织必须启用所有功能才能管理成员账户的设置。这样管理员就可以控制成员账户。这是在创建组织时默认设置的。如果您的组织设置为仅整合账单，而您要启用所有功能，请参阅[在组织中启用所有功能](#)。
- 您需要启用 Amazon 账户管理服务可信访问权限。要进行此设置，请参阅[启用 Amazon 账户管理可信访问权限](#)。

Amazon Web Services Management Console

为组织中的任何 Amazon Web Services 账户 编辑主要联系人

1. 使用组织的管理账户凭证登录 [Amazon Organizations 控制台](#)。
2. 从 Amazon Web Services 账户 中，选择要更新的账户。
3. 选择联系人信息，然后找到主要联系人，
4. 选择编辑。
5. 更改任何可用字段中的值。
6. 完成所有更改后，选择更新。

Amazon CLI & SDKs

您可以使用以下 Amazon CLI 命令或其 Amazon SDK 等效操作，检索、更新或删除主要联系人信息：

- [GetContactInformation](#)
- [PutContactInformation](#)

注意

- 要通过管理账户或组织中的委托管理员账户对成员账户执行这些操作，必须 [启用账户服务可信访问权限](#)。
- 您无法访问与您的操作调用组织不同的组织中的账户。

最小权限

对于各个操作，您必须具有映射到此操作的权限：

- `account:GetContactInformation`
- `account:PutContactInformation`

如果使用这些单独权限，就可以授予某些用户仅读取联系人信息的权限，而授予其他用户同时读取和写入的权限。

Example

以下示例检索了组织中指定成员账户的当前主要联系人信息。所用凭证必须来自组织管理账户或账户管理委托管理员账户。

```
$ aws account get-contact-information --account-id 123456789012
{
  "ContactInformation": {
    "AddressLine1": "123 Any Street",
    "City": "Seattle",
    "CompanyName": "Example Corp, Inc.",
    "CountryCode": "US",
    "DistrictOrCounty": "King",
    "FullName": "Saanvi Sarkar",
    "PhoneNumber": "+15555550100",
    "PostalCode": "98101",
    "StateOrRegion": "WA",
    "WebsiteUrl": "https://www.examplecorp.com"
  }
}
```

Example

以下示例为组织中的指定成员账户设置了主要联系人信息。所用凭证必须来自组织管理账户或账户管理委托管理员账户。

```
$ aws account put-contact-information --account-id 123456789012 \
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",
"CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":
"King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
"StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

如果成功，此命令不会产生任何输出。

查看 Amazon Web Services 账户 标识符

Amazon 为每 Amazon Web Services 账户人分配以下唯一标识符：

[Amazon Web Services 账户 ID](#)

一个 12 位数字（如 012345678901）用于唯一标识 Amazon Web Services 账户。许多 Amazon 资源的 [Amazon 资源名称中都包含账户 ID \(ARNs\)](#)。账户 ID 部分将一个账户中的资源与另一个账户中的资源区分开来。如果您是 Amazon Identity and Access Management (IAM) 用户，则可以使用账户 ID 或账户别名登录。Amazon Web Services Management Console 虽然帐户与任何识别信息一样 IDs，应谨慎使用和共享，但它们不被视为机密、敏感或机密信息。

[规范用户 ID](#)

一种字母数字标识符，例

如 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be，它是 ID 的混淆形式。Amazon Web Services 账户 在使用亚马逊简单存储服务 (Amazon S3) 授予对存储桶和对象的跨账户访问权限 Amazon Web Services 账户 时，您可以使用此 ID 来识别。您可以 [root 用户或用户的身份检索您的 Amazon Web Services 账户 规范用户 ID IAM](#)。

您必须通过身份验证 Amazon 才能查看这些标识符。

Warning

请勿将您的 Amazon 凭证（包括密码和访问密钥）提供给需要您的 Amazon Web Services 账户 标识符才能与您共享 Amazon 资源的第三方。这样做可以让他们获得与你相同的访问权限。
Amazon Web Services 账户

找到你的 Amazon Web Services 账户 身份证

您可以使用 Amazon Web Services Management Console 或 Amazon Command Line Interface (Amazon CLI) 来查找 Amazon Web Services 账户 ID。在控制台中，账户 ID 的位置取决于您是以 root 用户还是用户身份登录。IAM 无论您是以 root 用户还是用户身份登录，账户 ID 都是一 IAM 样的。

以根用户身份查找您的账户 ID

Amazon Web Services Management Console

在以 root 用户 Amazon Web Services 账户 身份登录时查找你的 ID

最小权限

要执行以下步骤，您必须至少具有以下IAM权限：

- 当您以 root 用户身份登录时，不需要任何IAM权限。

1. 在右上角的导航栏中，请选择您的账户名称或编号，然后选择安全凭证。

Tip

如果您看不到安全证书选项，则可能是以具有IAM角色的联合用户身份登录，而不是以IAM用户身份登录。在这种情况下，请查找账户条目及其旁边的账户 ID 号。

2. 在账户详细信息部分下，账号显示在 Amazon Web Services 账户 ID 旁边。

Amazon CLI & SDKs

要查找您的 Amazon Web Services 账户 身份证，请使用 Amazon CLI

最小权限

要执行以下步骤，您必须至少具有以下IAM权限：

- 当你以 root 用户身份运行命令时，你不需要任何IAM权限。

按照如下所示使用 [get-caller-identity](#) 命令。

```
$ aws sts get-caller-identity \  
  --query Account \  
  --output text  
123456789012
```

以IAM用户身份查找您的账户 ID

Amazon Web Services Management Console

以IAM用户 Amazon Web Services 账户 身份登录时查找您的 ID

最小权限

要执行以下步骤，您必须至少具有以下IAM权限：

- `account:GetAccountInformation`

1. 在右上角的导航栏中，选择您的用户名，然后选择 Security credentials (安全凭证)。

Tip

如果您看不到安全证书选项，则可能是以具有IAM角色的联合用户身份登录，而不是以IAM用户身份登录。在这种情况下，请查找账户条目及其旁边的账户 ID 号。

2. 在页面顶部的账户详细信息下，账号显示在 Amazon Web Services 账户 ID 旁边。

Amazon CLI & SDKs

要查找您的 Amazon Web Services 账户 身份证，请使用 Amazon CLI

最小权限

要执行以下步骤，您必须至少具有以下IAM权限：

- 当你以IAM用户或角色的身份运行命令时，你必须具备：
 - `sts:GetCallerIdentity`

按照如下所示使用 [get-caller-identity](#) 命令。

```
$ aws sts get-caller-identity \  
  --query Account \  
  --output text
```

123456789012

查找 Amazon Web Services 账户的规范用户 ID

您可以使用 Amazon Web Services Management Console 或找到适合您的 Amazon Web Services 账户规范用户 ID。Amazon CLI的规范用户 ID Amazon Web Services 账户 是该账户所特有的。您可以以 root 用户、联合用户或用户 Amazon Web Services 账户 身份检索规范用户 ID。IAM

以 root 用户或用户身份查找规范 ID IAM

Amazon Web Services Management Console

在以 root 用户或用户身份登录控制台时查找账户的规范用户 ID IAM

最小权限

要执行以下步骤，您必须至少具有以下IAM权限：

- 当你以 root 用户身份运行命令时，你不需要任何IAM权限。
- 当你以IAM用户身份登录时，你必须：
 - `account:GetAccountInformation`

1. 以 root 用户或用户身份登录。 Amazon Web Services Management Console IAM
2. 在右上角的导航栏中，请选择您的账户名称或编号，然后选择安全凭证。

Tip

如果您看不到安全证书选项，则可能是以具有IAM角色的联合用户身份登录，而不是以IAM用户身份登录。在这种情况下，请查找账户条目及其旁边的账户 ID 号。

3. 在账户详情部分下，规范用户 ID 显示在规范用户 ID 旁边。您可以使用您的规范用户 ID 来配置 Amazon S3 访问控制列表 (ACLs)。

Amazon CLI & SDKs

要查找规范用户 ID，请使用 Amazon CLI

同样 Amazon CLI 的 API and 命令适用于 Amazon Web Services 账户根用户、IAM用户或IAM角色。

按如下方式使用 [list-buckets](#) 命令。

```
$ aws s3api list-buckets \  
  --max-items 10 \  
  --page-size 10 \  
  --query Owner.ID \  
  --output text  
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

以具有角色的联合用户身份查找规范 ID IAM

Amazon Web Services Management Console

以具有角色的联合用户身份登录控制台时查找账户的规范 ID IAM

最小权限

- 您必须拥有列出和查看 Amazon S3 存储桶的权限。

1. 以具有IAM角色的 Amazon Web Services Management Console 联合用户身份登录。
2. 在 Amazon S3 控制台中，请选择存储桶名称，来查看存储桶详细信息。
3. 选择 Permissions (权限) 选项卡。
4. 在访问控制列表部分的存储桶所有者下，将显示 Amazon Web Services 账户 的规范 ID。

Amazon CLI & SDKs

要查找规范用户 ID，请使用 Amazon CLI

同样 Amazon CLI 的 API and 命令适用于 Amazon Web Services 账户根用户、IAM用户或IAM角色。

按如下方式使用 [list-buckets](#) 命令。

```
$ aws s3api list-buckets \  
  --max-items 10 \  
  --page-size 10 \  
  --query Owner.ID \  
  --output text  
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

```
--max-items 10 \  
--page-size 10 \  
--query Owner.ID \  
--output text  
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Amazon 账户管理中的安全性

Amazon 十分重视云安全性。作为 Amazon 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

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

- 云的安全性 – Amazon 负责保护在 Amazon Web Services 云中运行 Amazon 服务的基础设施。Amazon 还向您提供可安全使用的服务。第三方审核员定期测试和验证我们的安全性的有效性，作为 [Amazon Compliance Programs](#) 的一部分。要了解适用于账户管理的合规性计划，请参阅[合规性计划范围内的 Amazon Web Services 服务](#)。
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您的公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 Amazon 账户管理时应用责任共担模式。它说明了如何配置账户管理以实现您的安全性和合规性目标。您还会了解如何使用其他 Amazon 服务来帮助您监控和保护账户管理资源。

主题

- [Amazon 账户管理中的数据保护](#)
- [适用于 Amazon 账户管理的 Amazon PrivateLink](#)
- [用于 Amazon 账户管理的 Identity and Access Management](#)
- [适用于 Amazon 账户管理的 Amazon 托管策略](#)
- [Amazon 账户管理的合规性验证](#)
- [Amazon 账户管理的弹性](#)
- [Amazon Account Management 中的基础设施安全性](#)

Amazon 账户管理中的数据保护

Amazon [责任共担模式](#) 适用于 Amazon 账户管理中的数据保护。如该模式中所述，Amazon 负责保护运行所有 Amazon Web Services 云的全球基础架构。您负责维护对托管在此基础架构上的内容的控制。您还负责您所使用的 Amazon Web Services 服务的安全配置和管理任务。有关数据隐私的更多信息，请参阅[数据隐私常见问题](#)。

出于数据保护目的，我们建议您保护 Amazon Web Services 账户凭证并使用 Amazon IAM Identity Center 或 Amazon Identity and Access Management (IAM) 设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与 Amazon 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 Amazon CloudTrail 设置 API 和用户活动日记账记录。有关使用 CloudTrail 跟踪来捕获 Amazon 活动的信息，请参阅《Amazon CloudTrail 用户指南》中的 [Working with CloudTrail trails](#)。
- 使用 Amazon 加密解决方案以及 Amazon Web Services 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅[美国联邦信息处理标准 \(FIPS \) 140-3](#)。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括使用控制台、API、Amazon CLI 或 Amazon SDK 处理账户管理或其他 Amazon Web Services 服务时。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

适用于 Amazon 账户管理的 Amazon PrivateLink

如果使用 Amazon Virtual Private Cloud (Amazon VPC) 托管 Amazon 资源，则可以从 VPC 内访问 Amazon 账户管理服务，而无需通过公共 Internet。

Amazon VPC 允许您在自定义虚拟网络中启动 Amazon 资源。可以使用 VPC 控制您的网络设置，例如 IP 地址范围、子网、路由表和网络网关。有关 VPC 的更多信息，请参阅 [《Amazon VPC 用户指南》](#)。

要将 Amazon VPC 连接到账户管理，您必须先定义一个接口 VPC 端点，该端点可让您将 VPC 连接到其他 Amazon 服务。该端点提供了可靠且可扩展的连接，无需互联网网关、网络地址转换 (NAT) 实例或 VPN 连接。有关更多信息，请参阅 Amazon VPC 用户指南中的[接口 VPC 端点 \(Amazon PrivateLink\)](#)。

创建端点

您可以使用 Amazon Web Services Management Console、Amazon Command Line Interface (Amazon CLI)、Amazon SDK、Amazon 账户管理 API 或 Amazon CloudFormation 在 VPC 中创建 Amazon 账户管理端点。

有关使用 Amazon VPC 控制台或 Amazon CLI 创建和配置端点的信息，请参阅 Amazon VPC 用户指南中的[创建接口端点](#)。

Note

在创建端点时，请使用以下格式将账户管理指定为您希望 VPC 连接到的服务：

```
cn.com.amazonaws.cn-northwest-1.account
```

您必须完全按照说明使用字符串，并指定 cn-northwest-1 区域。作为一项全球性服务，账户管理仅托管在这样一个 Amazon 区域。

有关使用 Amazon CloudFormation 创建和配置端点的信息，请参阅《Amazon CloudFormation 用户指南》中的[AWS::EC2::VPCEndpoint](#) 资源。

Amazon VPC 端点策略

通过在创建 Amazon VPC 端点时附加端点策略，您可以控制借助于此服务端点执行的操作。您可以通过附加多个端点策略来创建复杂的 IAM 规则。有关更多信息，请参阅：

- [适用于账户管理的 Amazon Virtual Private Cloud 的端点策略](#)
- 《Amazon PrivateLink 指南》中的[使用 VPC 端点控制对服务的访问](#)

适用于账户管理的 Amazon Virtual Private Cloud 的端点策略

您可以为账户管理创建 Amazon VPC 端点策略，并在其中指定以下内容：

- 可执行操作的主体。
- 主体可以执行的操作。
- 可对其执行操作的资源。

以下示例显示了一项 Amazon VPC 端点策略，该策略允许账户 123456789012 中名为 Alice 的 IAM 用户检索和更改任何 Amazon Web Services 账户的备用联系人信息，但拒绝所有 IAM 用户删除任何账户中任何备用联系人信息的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "account:GetAlternateContact",
        "account:PutAlternateContact"
      ],
      "Resource": "arn:aws::iam:*:account",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws::iam:123456789012:user/Alice"
      }
    },
    {
      "Action": "account>DeleteAlternateContact",
      "Resource": "*",
      "Effect": "Deny",
      "Principal": "arn:aws::iam:*:root"
    }
  ]
}
```

如果要属于 Amazon 组织的账户的访问权限授予其中一个组织成员账户的主体，则 Resource 元素必须使用以下格式：

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

有关创建端点策略的更多信息，请参阅《Amazon PrivateLink 指南》中的[使用 VPC 端点控制对服务的访问](#)。

用于 Amazon 账户管理的 Identity and Access Management

Amazon Identity and Access Management (IAM) Amazon Web Services 服务可以帮助管理员安全地控制对 Amazon 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用账户管理资源。IAM 无需支付额外费用即可使用。Amazon Web Services 服务

主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [Amazon 账户管理如何使用 IAM](#)
- [账户管理基于身份的策略示例 Amazon 例](#)
- [使用基于身份的策略 \(IAM政策 \) 进行账户管理 Amazon](#)
- [Amazon 账户管理身份和访问权限疑难解答](#)

受众

您使用 Amazon Identity and Access Management (IAM) 的方式会有所不同，具体取决于您在账户管理中所做的工作。

服务用户 - 如果使用账户管理服务来完成任务，则您的管理员会为您提供所需的凭证和权限。当您使用更多账户管理功能来完成工作时，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问账户管理中的功能，请参阅[Amazon 账户管理身份和访问权限疑难解答](#)。

服务管理员 - 如果您在公司负责管理账户管理资源，则您可能具有账户管理的完全访问权限。您有责任确定您的服务用户应访问哪些账户管理功能和资源。然后，您必须向 IAM 管理员提交请求，这样才能更改您的服务用户的权限。查看此页面的信息，了解 IAM 的基本概念。要详细了解贵公司如何 IAM 使用账户管理，请参阅[Amazon 账户管理如何使用 IAM](#)。

IAM 管理员 - 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理账户管理的访问权限。要查看可在中使用的账户管理基于身份的策略示例 IAM，请参阅。[账户管理基于身份的策略示例 Amazon 例](#)

使用身份进行身份验证

身份验证是您 Amazon 使用身份凭证登录的方式。您必须以 Amazon Web Services 账户根用户、IAM 用户身份或通过担任 IAM 角色进行身份验证（登录 Amazon）。

如果您 Amazon 以编程方式访问，则会 Amazon 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 Amazon 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的[API 请求 Amazon 签名版本 4](#)。

无论使用何种身份验证方法，您可能都需要提供其他安全信息。例如，Amazon 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》IAM 中的[Amazon 多重身份验证](#)。

Amazon Web Services 账户 root 用户

创建时 Amazon Web Services 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 Amazon Web Services 服务和资源。此身份被称为 Amazon Web Services 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的[需要根用户凭证的任务](#)。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 Amazon Web Services 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C 或者任何使用 Amazon Web Services 服务 通过身份源提供的凭据进行访问的用户。Amazon Directory Service 当联合身份访问时 Amazon Web Services 账户，他们将扮演角色，角色提供临时证书。

IAM 用户和组

[IAM 用户](#)是您内部 Amazon Web Services 账户 对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时证书，而不是创建拥有密码和访问密钥等长期凭证的 IAM 用户。但是，如果您有需要 IAM 用户长期凭证的特定用例，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的[对于需要长期凭证的使用场景定期轮换访问密钥](#)。

[IAM 组](#)是指定一个 IAM 用户集合的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins 并授予该群组管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅用户指南中的 IAM IAM 用户 [用例](#)。

IAM 角色

[IAM 角色](#)是您内部具有特定权限 Amazon Web Services 账户 的身份。它类似于 IAM 用户，但未与特定人员关联。要在中临时扮 IAM 演角色 Amazon Web Services Management Console，可以[从用户切换到 IAM 角色（控制台）](#)。您可以通过调用 Amazon CLI 或 Amazon API 操作或使用自定义操作来代入角色 URL。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的[代入角色的方法](#)。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建一个角色，并为该角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM用户指南》中的[为第三方身份提供商（联合）创建角色](#)。
- 临时IAM用户权限-IAM 用户或角色可以代入一个IAM角色，为特定任务临时获得不同的权限。
- 跨账户存取 - 您可以使用 IAM 角色允许其他账户中的某个人（可信任主体）访问您账户中的资源。角色是授予跨账户存取权限的主要方式。但是，对于某些资源 Amazon Web Services 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅IAM用户指南[IAM中的跨账户资源访问权限](#)。
- 跨服务访问 — 有些 Amazon Web Services 服务 使用其他 Amazon Web Services 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序EC2或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
- 转发访问会话 (FAS)-当您使用IAM用户或角色在中执行操作时 Amazon，您被视为委托人。当你使用某些服务时，你可能会执行一个操作，然后在不同的服务中启动另一个操作。FAS使用调用委托人的权限 Amazon Web Services 服务以及 Amazon Web Services 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 Amazon Web Services 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两项操作的权限。有关提出FAS请求时的政策详情，请参阅[转发访问会话](#)。
- 服务角色-服务[IAM角色](#)是服务代替您执行操作的角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM用户指南》 Amazon Web Services 服务中的[创建角色以向委派权限](#)。
- 服务相关角色-服务相关角色是一种与服务相关联的服务角色。Amazon Web Services 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 Amazon Web Services 账户，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon 上运行的应用程序 EC2 — 您可以使用IAM角色管理在EC2实例上运行并发出 Amazon CLI 或 Amazon API请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要为EC2实例分配 Amazon 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅IAM用户指南中的[使用IAM角色向在 Amazon EC2 实例上运行的应用程序授予权限](#)。

使用策略管理访问

您可以 Amazon 通过创建策略并将其附加到 Amazon 身份或资源来控制中的访问权限。策略是其中的一个对象 Amazon，当与身份或资源关联时，它会定义其权限。Amazon 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以

JSON文档 Amazon 形式存储在中。有关JSON策略文档结构和内容的更多信息，请参阅 [《IAM用户指南》中的JSON策略概述](#)。

管理员可以使用 Amazon JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入这些角色。

IAM 策略定义操作的权限，无论您使用哪种方法执行操作。例如，假设您有一个允许 iam:GetRole 操作的策略。拥有该策略的用户可以从 Amazon Web Services Management Console Amazon CLI、或获取角色信息 Amazon API。

基于身份的策略

基于身份的策略是可以附加到身份（例如IAM用户、用户组或角色）的JSON权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅IAM用户指南中的[使用客户托管策略定义自定义IAM权限](#)。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 Amazon Web Services 账户。托管策略包括 Amazon 托管策略和客户托管策略。要了解如何在托管策略或内联策略之间进行[选择](#)，请参阅 [《IAM用户指南》中的在托管策略和内联策略之间](#)进行选择。

基于资源的策略

基于资源的JSON策略是您附加到资源的策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。委托人可以包括账户、用户、角色、联合用户或 Amazon Web Services 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略IAM中使用 Amazon 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

Amazon S3 Amazon WAF、和亚马逊VPC就是支持的服务示例ACLs。要了解更多信息ACLs，请参阅 [《亚马逊简单存储服务开发者指南》中的访问控制列表 \(ACL\) 概述](#)。

其他策略类型

Amazon 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- **权限边界**-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向IAM实体（IAM用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 [IAM 实体的权限边界](#)。
- **服务控制策略 (SCPs)**-SCPs 是为中的组织或组织单位 (OU) 指定最大权限的JSON策略 Amazon Organizations。Amazon Organizations 是一项用于对您的企业拥有的多 Amazon Web Services 账户项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。对成员账户中的实体（包括每个实体）的权限进行了SCP限制 Amazon Web Services 账户根用户。有关 Organization SCPs 的更多信息，请参阅《Amazon Organizations 用户指南》中的 [服务控制策略](#)。
- **资源控制策略 (RCPs)** — RCPs 这些JSON策略可用于设置账户中资源的最大可用权限，而无需更新附加到您拥有的每项资源的IAM策略。这会RCP限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 Amazon Web Services 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息RCPs，包括 Amazon Web Services 服务 该支持的列表RCPs，请参阅《Amazon Organizations 用户指南》中的 [资源控制策略 \(RCPs\)](#)。
- **会话策略**：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的 [会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 Amazon 确定是否允许请求，请参阅IAM用户指南中的 [策略评估逻辑](#)。

Amazon 账户管理如何使用 IAM

在使用管理账户管理IAM访问权限之前，请先了解账户管理有哪些IAM功能可供使用。

IAM您可以在 Amazon 账户管理中使用的功能

IAM 功能	账户管理支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键	是
ACLs	否
ABAC (策略中的标签)	是
临时凭证	是
主体权限	是
服务角色	否
服务相关角色	否

要全面了解账户管理和其他 Amazon 服务如何与大多数IAM功能配合使用，请参阅《IAM用户指南》IAM中[与之配合使用的Amazon 服务](#)。

适用于账户管理的基于身份的策略

支持基于身份的策略：是

基于身份的策略是可以附加到身份（例如IAM用户、用户组或角色）的JSON权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅IAM用户指南中的[使用客户托管策略定义自定义IAM权限](#)。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可以在JSON策略中使用的所有元素，请参阅IAM用户指南中的[IAMJSON策略元素参考](#)。

适用于账户管理的基于身份的策略示例

要查看账户管理基于身份的策略的示例，请参阅[账户管理基于身份的策略示例 Amazon 例](#)。

账户管理内基于资源的策略

支持基于资源的策略：否

基于资源的JSON策略是您附加到资源的策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。委托人可以包括账户、用户、角色、联合用户或 Amazon Web Services 服务。

要启用跨账户存取，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 Amazon Web Services 账户，可信账户中的IAM管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM用户指南》IAM中的[跨账户资源访问权限](#)。

账户管理的策略操作

支持策略操作：是

管理员可以使用 Amazon JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON策略Action元素描述了可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 Amazon API操作同名。也有一些例外，例如没有匹配API操作的仅限权限的操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看账户管理操作列表，请参阅《服务授权参考》中[Amazon 账户管理定义的操作](#)。

账户管理中的策略操作在操作前使用以下前缀：

```
account
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [  
  "account:action1",  
  "account:action2"  
]
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定与备用联系人配合使用的所有操作，请包括以下操作。 Amazon Web Services 账户

```
"Action": "account:*AlternateContact"
```

要查看账户管理基于身份的策略的示例，请参阅[账户管理基于身份的策略示例 Amazon 例](#)。

账户管理的策略资源

支持策略资源：是

管理员可以使用 Amazon JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

ResourceJSON策略元素指定要应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。最佳做法是，使用资源的 [Amazon 资源名称 \(ARN\)](#) 来指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

账户管理服务支持IAM政策Resources元素中的以下特定资源类型，以帮助您筛选策略并区分以下类型 Amazon Web Services 账户：

- account

此 resource 类型仅匹配不属于 Amazon Organizations 服务管理组织中的成员账户的独立 Amazon Web Services 账户。

- accountInOrganization

此resource类型仅匹配由 Amazon Web Services 账户 该 Amazon Organizations 服务管理的组织中的成员帐户。

要查看账户管理资源类型及其列表ARNs，请参阅服务授权参考中的[Amazon 账户管理定义的资源](#)。要了解您可以为每ARN种资源指定哪些操作，请参阅[Amazon 账户管理定义的操作](#)。

要查看账户管理基于身份的策略的示例，请参阅[账户管理基于身份的策略示例 Amazon 例](#)。

账户管理的策略条件键

支持特定于服务的策略条件键：是

管理员可以使用 Amazon JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素 (或 Condition 块) 中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用[条件运算符](#) (例如，等于或小于) 的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 Amazon 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 Amazon 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，仅当 IAM 用户使用其 IAM 用户名进行标记时，您才可为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的[IAM 策略元素：变量和标签](#)。

Amazon 支持全局条件密钥和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅《IAM 用户指南》中的[Amazon 全局条件上下文密钥](#)。

账户管理服务支持以下条件密钥，您可以使用这些条件键对您的IAM政策进行精细筛选：

- 账户:TargetRegion

此条件键的参数由一系列 [Amazon 区域代码](#) 组成。它允许筛选策略，从而只影响适用于指定区域的操作。

- 账户:AlternateContactTypes

此条件键采用备用联系人类型的列表：

- BILLING
- OPERATIONS
- SECURITY

使用此键，您可以将请求筛选为仅针对指定备用联系人类型的操作。

- 账户:AccountResourceOrgPaths

此条件键采用一个参数，该参数由一个ARNs带有通配符的列表组成，这些通配符代表组织中的帐户。它允许您筛选策略，使其仅影响那些针对具有该匹配项的账户ARNs的操作。例如，以下内容仅ARN匹配指定组织和指定组织单位 (OU) 中的那些帐户。

```
arn:aws:account::111111111111:ou/o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
```

- 账户:AccountResourceOrgTags

此条件键的参数由一系列标签键和值组成。它允许筛选策略，从而只影响那些属于组织成员且标有指定标签键和值的帐户。

要查看账户管理条件密钥列表，请参阅服务授权参考中的[Amazon 账户管理条件密钥](#)。要了解您可以使用条件键的操作和资源，请参阅[Amazon 账户管理定义的操作](#)。

要查看账户管理基于身份的策略的示例，请参阅[账户管理基于身份的策略示例 Amazon 例](#)。

账户管理中的访问控制列表

支持ACLs：否

访问控制列表 (ACLs) 控制哪些委托人 (帐户成员、用户或角色) 有权访问资源。ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

使用账户管理的基于属性的访问权限控制

支持ABAC (策略中的标签)：是

基于属性的访问控制 (ABAC) 是一种基于属性定义权限的授权策略。在中 Amazon，这些属性称为标签。您可以将标签附加到IAM实体 (用户或角色) 和许多 Amazon 资源。为实体和资源添加标签是的第一步。ABAC然后，您可以设计ABAC策略，允许在委托人的标签与他们尝试访问的资源上的标签匹配时进行操作。

ABAC在快速增长的环境中很有用，也有助于解决策略管理变得繁琐的情况。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的[条件元素](#)中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关更多信息ABAC，请参阅《IAM用户指南》中的[使用ABAC授权定义权限](#)。要查看包含设置步骤的教程ABAC，请参阅IAM用户指南中的[使用基于属性的访问控制 \(ABAC\)](#)。

将临时凭证用于账户管理

支持临时凭证：是

当你使用临时证书登录时，有些 Amazon Web Services 服务 不起作用。有关其他信息，包括哪些 Amazon Web Services 服务 适用于临时证书 [Amazon Web Services 服务](#)，请参阅《IAM用户指南》IAM中的“[适用于临时证书](#)”。

如果您使用除用户名和密码之外的任何方法登录，则 Amazon Web Services Management Console 使用的是临时证书。例如，当您 Amazon 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《[用户指南](#)》中的[从IAM用户切换到IAM角色 \(控制台\)](#)。

您可以使用 Amazon CLI 或手动创建临时证书 Amazon API。然后，您可以使用这些临时证书进行访问 Amazon。Amazon 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅[中的临时安全证书IAM](#)。

账户管理的跨服务主体权限

支持转发访问会话 (FAS)：是

当您使用IAM用户或角色在中执行操作时 Amazon，您被视为委托人。当你使用某些服务时，你可能会执行一个操作，然后在不同的服务中启动另一个操作。FAS使用调用委托人的权限 Amazon Web Services 服务以及 Amazon Web Services 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 Amazon Web Services 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两项操作的权限。有关提出FAS请求时的政策详情，请参阅[转发访问会话](#)。

账户管理的服务角色

支持服务角色：否

服务角色是由一项服务代入、代表您执行操作的 [IAM 角色](#)。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM用户指南》Amazon Web Services 服务中的[创建角色以向委派权限](#)。

账户管理的服务相关角色

支持服务相关角色：否

服务相关角色是一种链接到的服务角色。Amazon Web Services 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的 Amazon Web Services 账户，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅[使用 IAM 的 Amazon 服务](#)。在表中查找服务相关角色列中包含 Yes 的服务。选择是链接以查看该服务的服务相关角色文档。

账户管理基于身份的策略示例 Amazon 例

默认情况下，用户和角色没有创建或修改账户管理资源的权限。他们也无法使用 Amazon Web Services Management Console、Amazon Command Line Interface (Amazon CLI) 或来执行任务 Amazon API。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入这些角色。

要了解如何使用这些示例策略文档创建 IAM 基于身份的 JSON 策略，请参阅 IAM 用户指南中的[创建 IAM 策略 \(控制台\)](#)。

有关账户管理定义的操作和资源类型（包括每种资源类型的格式）的 ARNs 详细信息，请参阅《服务授权参考》中的[“Amazon 账户管理的操作、资源和条件密钥”](#)。

主题

- [策略最佳实践](#)
- [使用中的“账户”页面 Amazon Web Services Management Console](#)
- [提供对账户页面的只读访问权限 Amazon Web Services Management Console](#)
- [提供对“账户”页面的完全访问权限 Amazon Web Services Management Console](#)

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的账户管理资源。这些操作可能会使 Amazon Web Services 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 Amazon 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的 Amazon 托管策略。它们在你的版本中可用 Amazon Web Services 账户。我们建议您通过定义针对您的用例的 Amazon 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的[Amazon 托管式策略](#)或[工作职能的 Amazon 托管式策略](#)。
- 应用最低权限许可 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的[IAM 中的策略和权限](#)。

- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写一个策略条件来指定所有请求都必须使用发送SSL。如果服务操作是通过特定 Amazon Web Services 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 Amazon CloudFormation。有关更多信息，请参阅《IAM用户指南》中的[IAMJSON策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的IAM策略以确保权限的安全性和功能性 — IAM Access Analyzer 会验证新的和现有的策略，以便策略符合IAM策略语言 (JSON) 和IAM最佳实践。IAM Access Analyzer 提供了 100 多项策略检查和可行的建议，可帮助您制定安全和实用的策略。有关更多信息，请参阅《IAM用户指南》中的[使用 IAM Access Analyzer 验证策略](#)。
- 需要多重身份验证 (MFA)-如果您的场景需要IAM用户或 root 用户 Amazon Web Services 账户，请打开MFA以提高安全性。要要求MFA何时调用API操作，请在策略中添加MFA条件。有关更多信息，请参阅《IAM用户指南》MFA中的使用[进行安全API访问](#)。

有关 IAM 中最佳实践的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的安全最佳实践](#)。

使用中的“账户”页面 Amazon Web Services Management Console

要访问中的[账户页面](#) Amazon Web Services Management Console，您必须拥有最低限度的权限。这些权限必须允许您列出和查看有关您的详细信息 Amazon Web Services 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（IAM 用户或角色），控制台将无法按预期正常运行。

为确保用户和角色可以使用账户管理控制台，您可以选择将AWSAccountManagementReadOnlyAccess或AWSAccountManagementFullAccess Amazon 托管策略附加到实体。有关更多信息，请参阅 IAM 用户指南中的[为用户添加权限](#)。

您无需为仅拨打 Amazon CLI或的用户设置最低控制台权限 Amazon API。相反，在许多情况下，您可以选择只允许访问与您尝试执行的API操作相匹配的操作。

提供对账户页面的只读访问权限 Amazon Web Services Management Console

在以下示例中，您想授予IAM用户对中账户页面的 Amazon Web Services 账户 只读访问权限 Amazon Web Services Management Console。附加此策略的用户无法进行任何更改。

account:GetAccountInformation 操作授予在“账户”页面查看大部分设置的权限。但是，要查看当前启用的 Amazon 区域，还必须包括 account:ListRegions 操作。

```
{
```



```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "GrantReadOnlyAccessToAccountSettings",
    "Effect": "Allow",
    "Action": [
      "account:GetAccountInformation",
      "account:ListRegions"
    ],
    "Resource": "*"
  }
]
```

提供对“账户”页面的完全访问权限 Amazon Web Services Management Console

在以下示例中，您想向IAM用户授予对中“帐户”页面的 Amazon Web Services 账户 完全访问权限 Amazon Web Services Management Console。附加了此政策的用户可以修改账户的设置。

此示例策略以前面的示例策略为基础，添加了每个可用的写入权限（除外 CloseAccount），允许用户更改账户的大部分设置，包括account:EnableRegion和account:DisableRegion权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GrantFullAccessToAccountSettings",
      "Effect": "Allow",
      "Action": [
        "account:GetAccountInformation",
        "account:ListRegions",
        "account:PutContactInformation",
        "account:PutChallengeQuestions",
        "account:PutAlternateContact",
        "account>DeleteAlternateContact",
        "account:EnableRegion",
        "account:DisableRegion"
      ],
      "Resource": "*"
    }
  ]
}
```

使用基于身份的策略 (IAM政策) 进行账户管理 Amazon

有关 Amazon Web Services 账户 和IAM用户的完整讨论，请参阅[什么是IAM?](#) 在《IAM用户指南》中。

有关如何更新客户托管策略的说明，请参阅《IAM用户指南》中的[编辑客户托管策略 \(控制台 \)](#)。

Amazon 账户管理操作政策

此表概述了允许访问账户设置的权限。有关使用这些权限的策略示例，请参阅[Amazon 账户管理策略示例](#)。

Note

要向IAM用户授予对“帐户”页面中特定[账户](#)设置的写入GetAccountInformation权限 Amazon Web Services Management Console，除了要用于修改该设置的权限（或权限）之外，您还必须允许该权限。

权限名称	访问级别	描述
account:ListRegions	列表	授予权限以列出可用区域。
account:GetAccountInformation	读取	授予检索账户信息的权限。
account:GetAlternateContact	读取	授予权限以检索账户的备用联系人。
account:GetContactInformation	读取	授予权限以检索账户的主要联系人信息。
account:GetRegionOptStatus	读取	授予获取区域的加入状态的权限。
account:AcceptPrimaryEmailUpdate	写入	授予接受 Amazon 组织中成员账户主电子邮件地址更新的权限。

权限名称	访问级别	描述
<code>account:CloseAccount</code>	写入	授予关闭账户的权限。 <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;">Note 此权限仅适用于控制台。此权限没有API访问权限。</div>
<code>account>DeleteAlternateContact</code>	写入	授予权限以删除账户的备用联系人。
<code>account:DisableRegion</code>	写入	授予权限以禁用使用区域。
<code>account:EnableRegion</code>	写入	授予权限以启用使用区域。
<code>account:PutAlternateContact</code>	写入	授予权限以修改账户的备用联系人。
<code>account:PutChallengeQuestions</code>	写入	授予修改账户质询问题的权限。 <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;">Note 此权限仅适用于控制台。此权限没有API访问权限。</div>
<code>account:PutContactInformation</code>	写入	授予权限以更新账户的主要联系人信息。
<code>account:StartPrimaryEmailUpdate</code>	写入	授予启动 Amazon 组织中成员账户主电子邮件地址更新的权限。

Amazon 账户管理身份和访问权限疑难解答

使用以下信息来帮助您诊断和修复在使用账户管理时可能遇到的常见问题，以及IAM。


主题

- [我没有在“账户”页面中执行操作的权限](#)
- [我无权执行 iam:PassRole](#)
- [我想允许我以外的人 Amazon Web Services 账户 访问我的账户信息](#)

我没有在“账户”页面中执行操作的权限

如果 Amazon Web Services Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是指提供用户名和密码的人员。

当mateojacksonIAM用户尝试使用控制台在的“帐户”页面 Amazon Web Services 账户 中查看有关他的详细信息 Amazon Web Services Management Console 但没有account:GetAccountInformation权限时，就会出现以下示例错误。

**You Need Permissions**

You don't have permission to access billing information for this account. Contact your administrator if you need help. If you are an administrator, you can provide permissions for your users or groups by making sure that (1) [this account allows IAM and federated users to access billing information](#) and (2) [you have the required IAM permissions](#).

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 `account:GetWidget` 操作访问 `my-example-widget` 资源。

我无权执行 iam:PassRole

如果您收到错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给账户管理。

有些 Amazon Web Services 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的IAM用户marymajor尝试使用控制台在“账户管理”中执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 Amazon Web Services 账户 访问我的账户信息

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解账户管理是否支持这些功能，请参阅[Amazon 账户管理如何使用 IAM](#)。
- 要了解如何提供对您拥有的资源的访问权限，请参阅《IAM用户指南》中的[Amazon Web Services 账户 向其他IAM用户提供访问权限](#)。 Amazon Web Services 账户
- 要了解如何向第三方提供对您的资源的访问权限 [Amazon Web Services 账户](#)，请参阅IAM用户指南中的[向第三方提供访问权限](#)。 Amazon Web Services 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的[为经过外部身份验证的用户 \(身份联合验证 \) 提供访问权限](#)。
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅IAM用户指南[IAM中的跨账户资源访问权限](#)。

适用于 Amazon 账户管理的 Amazon 托管策略

Amazon 账户管理目前提供两种可供您使用的 Amazon 托管政策：

- [Amazon 托管策略：AWSAccountManagementReadOnlyAccess](#)
- [Amazon 托管策略：AWSAccountManagementFullAccess](#)
- [账户管理根据 Amazon 托管策略进行更新](#)

Amazon 托管式策略是由 Amazon 创建和管理的独立策略。Amazon 托管式策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住，Amazon 托管式策略可能不会为您的特定使用场景授予最低权限，因为它们可供所有 Amazon 客户使用。我们建议通过定义特定于您的使用场景的[客户托管式策略](#)来进一步减少权限。

您无法更改 Amazon 托管式策略中定义的权限。如果 Amazon 更新在 Amazon 托管式策略中定义的权限，则更新会影响该策略所附加到的所有主体身份（用户、组和角色）。当新的 Amazon Web Services 服务启动或新的 API 操作可用于现有服务时，Amazon 最有可能更新 Amazon 托管式策略。

有关更多信息，请参阅《IAM 用户指南》中的 [Amazon 托管式策略](#)。

Amazon 托管策略：AWSAccountManagementReadOnlyAccess

您可以将 AWSAccountManagementReadOnlyAccess 策略附加到 IAM 身份。

该策略提供了仅查看以下内容的只读权限：

- 关于 Amazon Web Services 账户的元数据
- 为 Amazon Web Services 账户启用或禁用的 Amazon Web Services 区域（只能使用 Amazon 控制台查看账户中区域的状态）

方法为：授予运行任何 Get* 或 List* 操作的权限。不提供修改账户元数据或为账户启用或禁用 Amazon Web Services 区域的任何功能。

权限详细信息

该策略包含以下权限。

- account-允许主体检索有关 Amazon Web Services 账户的元数据信息。它还允许主体列出为 Amazon Web Services Management Console 中的账户启用的 Amazon Web Services 区域。

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

Amazon 托管策略 : AWSAccountManagementFullAccess

您可以将 AWSAccountManagementFullAccess 策略附加到 IAM 身份。

该策略提供查看或修改以下内容的完全管理权限：

- 关于 Amazon Web Services 账户 的元数据
- 为 Amazon Web Services 账户 启用或禁用的 Amazon Web Services 区域 (只能使用 Amazon 控制台查看状态或者启用或禁用账户的区域)

方法为：授予运行任何 account 操作的权限。

权限详细信息

该策略包含以下权限。

- account-允许主体查看或修改有关 Amazon Web Services 账户 的元数据信息。它还允许主体列出为账户启用的 Amazon Web Services 区域 以及在 Amazon Web Services Management Console 中启用或禁用。

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

账户管理根据 Amazon 托管策略进行更新

查看有关自此服务开始跟踪这些更改以来账户管理的 Amazon 托管策略更新的详细信息。有关此页面更改的自动提示，请订阅账户管理文档历史记录页面上的 RSS 源。

更改	描述	日期
Amazon 账户管理推出了新的 Amazon 托管策略并开启了跟踪更改	<p>账户管理最初推出了以下 Amazon 托管策略：</p> <ul style="list-style-type: none"> • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess 	2021 年 9 月 30 日

Amazon 账户管理的合规性验证

作为多个 Amazon 合规性计划的一部分，第三方审计员评测可以在 Amazon Web Services 账户中运行的 Amazon 服务的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规性计划范围内的 Amazon 服务列表，请参阅[合规性计划范围内的 Amazon Web Services 服务](#)。有关常规信息，请参阅[Amazon 合规性计划](#)。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅《Amazon Artifact 用户指南》中的[在 Amazon Artifact 中下载报告](#)。

您在使用 Amazon Web Services 账户中的服务时的合规性责任由您数据的敏感性、贵公司的合规性目标以及适用的法律法规决定。Amazon 提供以下资源来帮助满足合规性：

- [安全性与合规性快速入门指南](#) – 这些部署指南讨论了架构注意事项，并提供了在 Amazon 上部署以安全性和合规性为重点的基准环境的步骤。
- [Amazon 合规性资源](#) – 此业务手册和指南集合可能适用于您的行业和位置。
- Amazon Config 开发人员指南中的[使用规则评估资源](#) – 此 Amazon Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- [Amazon Security Hub](#)：此 Amazon Web Services 服务提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践规范。

Amazon 账户管理的弹性

Amazon 全球基础设施围绕 Amazon Web Services 区域和可用区而构建。区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可

以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

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

Amazon Account Management 中的基础设施安全性

作为托管服务，在 Amazon Web Services 账户中运行的 Amazon 服务受到 Amazon 全球网络安全的保护。有关 Amazon 安全服务以及 Amazon 如何保护基础设施的信息，请参阅[Amazon 云安全](#)。要按照基础架构安全最佳实践设计您的 Amazon 环境，请参阅《安全性支柱 Amazon Well-Architected Framework》中的[基础架构保护](#)。

您可以使用 Amazon 发布的 API 调用，通过网络访问账户设置。客户端必须支持以下内容：

- 传输层安全性协议 (TLS) 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE (临时 Diffie-Hellman) 或 ECDHE (临时椭圆曲线 Diffie-Hellman)。大多数现代系统 (如 Java 7 及更高版本) 都支持这些模式。

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

监控您的 Amazon Web Services 账户

监控是保持 Amazon 账户管理和其他 Amazon 解决方案的可靠性、可用性和性能的重要组成部分。Amazon 提供了以下一些监控工具来监控账户管理，在出现错误时进行报告，并适时自动执行操作。

- Amazon CloudTrail 捕获（记录）由您的 Amazon Web Services 账户 或代表该账户进行的 API 调用和相关事件，并将日志文件写入您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶。这可以让您标识哪些用户和账户调用了 Amazon、发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 [《Amazon CloudTrail 用户指南》](#)。
- Amazon EventBridge 为您的 Amazon 服务额外增添自动化功能，它自动响应系统事件，例如应用程序可用性问题或资源更改。Amazon 服务中的事件将近乎实时传输到 EventBridge。您可以编写简单的规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。有关更多信息，请参阅 [Amazon EventBridge 用户指南](#)。

使用记录 Amazon 账户管理 API 呼叫 Amazon CloudTrail

Amazon 账户管理 APIs 与一项服务集成 Amazon CloudTrail，该服务提供用户、角色或调用账户管理操作的 Amazon 服务所采取的操作的记录。CloudTrail 将所有账户管理 API 电话捕获为事件。捕获的调用包括对账户管理操作的所有调用。如果您创建跟踪，则可以开启向 Amazon S3 存储桶持续传输事件，包括账户管理操作的事件。CloudTrail 如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的事件历史记录中查看最新的事件。使用收集到的信息 CloudTrail，您可以确定调用账户管理操作的请求、用于发出请求的 IP 地址、发出请求的人和时间的以及其他详细信息。

要了解更多信息 CloudTrail，请参阅 [Amazon CloudTrail 用户指南](#)。

中的账户管理信息 CloudTrail

CloudTrail 在您创建账户 Amazon Web Services 账户 时已在您的账户中处于启用状态。当账户管理操作发生活动时，会在 CloudTrail 事件历史 CloudTrail 记录中记录该活动以及其他 Amazon 服务事件。您可以在中查看、搜索和下载最近发生的事件 Amazon Web Services 账户。有关更多信息，请参阅 [使用事件历史记录查看 CloudTrail 事件](#)。

要持续记录您的事件 Amazon Web Services 账户，包括账户管理操作的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在创建跟踪时 Amazon Web Services Management Console，该跟踪将应用于所有跟踪 Amazon Web Services 区域。此跟踪记录在 Amazon 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage

Service (Amazon S3) 存储桶。您可以配置其他 Amazon 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- [创建跟踪记录概述](#)
- [CloudTrail 支持的服务和集成](#)
- [为以下各项配置亚马逊SNS通知 CloudTrail](#)
- [接收来自多个区域的 CloudTrail 日志文件](#)
- [从多个账户接收 CloudTrail 日志文件](#)

Amazon CloudTrail 记录本指南[API参考](#)部分中的所有账户管理API操作。例如，对CreateAccountDeleteAlternateContact、和PutAlternateContact操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用 root 用户还是 Amazon Identity and Access Management (IAM) 用户凭据发出
- 请求是使用 IAM 角色还是联合身份用户的临时安全凭证发出的
- 请求是否由其他 Amazon 服务发出

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

了解账户管理日志条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关所请求的操作、操作的日期和时间、请求参数等的信息。CloudTrail 日志文件不是公共API调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

示例 1：以下示例显示了调用GetAlternateContact操作以检索账户当前OPERATIONS备用联系人的 CloudTrail 日志条目。该记录信息不含此操作返回的值。

Example 示例 1

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
```

```
"arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "ARO1234567890EXAMPLE",
    "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
    "accountId": "123456789012",
    "userName": "ServiceTestRole"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-04-30T19:25:53Z"
  }
},
"eventTime": "2021-04-30T19:26:15Z",
"eventSource": "account.amazonaws.com",
"eventName": "GetAlternateContact",
"awsRegion": "us-east-1",
"sourceIPAddress": "10.24.34.250",
"userAgent": "Mozilla/5.0",
"requestParameters": {
  "alternateContactType": "SECURITY"
},
"responseElements": null,
"requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
"eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012"
}
```

示例 2：以下示例显示了调用PutAlternateContact操作以向账户添加新的BILLING备用联系人的CloudTrail 日志条目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
```

```
"type": "AssumedRole",
"principalId": "ARO0A1234567890EXAMPLE:AccountAPITests",
"arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "ARO0A1234567890EXAMPLE",
    "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
    "accountId": "123456789012",
    "userName": "ServiceTestRole"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-04-30T18:33:00Z"
  }
},
"webIdFederationData": {},
"attributes": {
  "mfaAuthenticated": "false",
  "creationDate": "2021-04-30T18:33:00Z"
}
},
"eventTime": "2021-04-30T18:33:08Z",
"eventSource": "account.amazonaws.com",
"eventName": "PutAlternateContact",
"awsRegion": "us-east-1",
"sourceIPAddress": "10.24.34.250",
"userAgent": "Mozilla/5.0",
"requestParameters": {
  "name": "*Alejandro Rosalez*",
  "emailAddress": "alrosalez@example.com",
  "title": "CFO",
  "alternateContactType": "BILLING"
},
"responseElements": null,
"requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
"eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012"
}
```

示例 3：以下示例显示了呼叫DeleteAlternateContact操作以删除当前OPERATIONS备用联系人的 CloudTrail 日志条目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "DeleteAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "OPERATIONS"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

```
}
```

使用 EventBridge 监控账户管理事件

Amazon EventBridge (以前称为 CloudWatch Events) 可帮助您监控特定的事件, 并启动将会使用其他 Amazon Web Services 服务的目标操作。来自 Amazon Web Services 服务的事件将近乎实时传输到 EventBridge。

借助 EventBridge, 您可以创建用于匹配传入事件的规则并将事件路由到目标以进行处理。

有关更多信息, 请参阅 Amazon EventBridge 用户指南中的 [Amazon EventBridge 入门](#)。

账户管理事件

以下示例显示了账户管理的事件。事件会尽可能生成。

目前只有通过 CloudTrail 启用和禁用区域和 API 调用的特定事件才可用于账户管理。

事件类型

- [启用和禁用区域的事件](#)

启用和禁用区域的事件

当通过控制台或 API 启用或禁用账户中的区域时, 会启动异步任务。初始请求将作为 CloudTrail 事件记录到目标账户中。此外, 当启用或禁用过程启动时, 将向调用账户发送 EventBridge 事件, 并在任一过程完成后再次发送。

以下示例事件显示如何发送请求, 表示在 2020-09-30 为 123456789012 账户ENABLED了 ap-east-1 区域。

```
{
  "version": "0",
  "id": "11112222-3333-4444-5555-666677778888",
  "detail-type": "Region Opt-In Status Change",
  "source": "aws.account",
  "account": "123456789012",
  "time": "2020-09-30T06:51:08Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:account::123456789012:account"
```

```
],
  "detail":{
    "accountId":"123456789012",
    "regionName":"ap-east-1",
    "status":"ENABLED"
  }
}
```

有四种可能的状态与 GetRegionOptStatus 和 ListRegions API 返回状态相匹配：

- ENABLED— 已成功为指示 accountId 启用了此区域
- ENABLING— 正在为指示 accountId 启用此区域
- DISABLED— 已成功为指示 accountId 禁用了此区域
- DISABLING— 正在为指示 accountId 禁用此区域

以下示例事件模式创建了捕获所有区域事件的规则。

```
{
  "source":[
    "aws.account"
  ],
  "detail-type":[
    "Region Opt-In Status Change"
  ]
}
```

以下示例事件模式创建了仅捕获 ENABLED 和 DISABLED 区域事件的规则。

```
{
  "source":[
    "aws.account"
  ],
  "detail-type":[
    "Region Opt-In Status Change"
  ],
  "detail":{
    "status":[
      "DISABLED",
      "ENABLED"
    ]
  }
}
```


}

排除 Amazon Web Services 账户 的故障

使用以下主题中的信息帮助诊断和解决 Amazon Web Services 账户 问题。如需根用户的帮助，请参阅《IAM 用户指南》中的[排查根用户问题](#)。如需登录过程的帮助，请参阅《Amazon 登录用户指南》中的[排查 Amazon Web Services 账户 登录问题](#)。

故障排除主题

- [排查 Amazon Web Services 账户 创建问题](#)
- [排查 Amazon Web Services 账户 关闭的问题](#)
- [排查其他 Amazon Web Services 账户 问题](#)

排查 Amazon Web Services 账户 创建问题

使用下表中的参考链接来帮助诊断和修复创建新 Amazon Web Services 账户 时遇到的问题。

问题	参考链接	来源
我不知道如何注册或创建账户	创建 Amazon Web Services 账户	本指南
如果我没有接到 Amazon 验证新账户的电话或者输入的 PIN 不起作用，该怎么办？	https://repost.aws/knowledge-center/phone-verify-no-call	Amazon Web Services re:Post
当我尝试通过电话验证自己的 Amazon Web Services 账户时，如何解决“最大失败尝试次数”的错误？	https://repost.aws/knowledge-center/maximum-failed-attempts	Amazon Web Services re:Post
已经过去 24 小时，但我的账户还没有激活	https://repost.aws/knowledge-center/create-and-activate-aws-account	Amazon Web Services re:Post
我创建了新账户后无法登录	https://docs.aws.amazon.com/signin/latest/userguide/tr	Amazon 登录用户指南

问题	参考链接	来源
	troubleshooting-sign-in-issues.html	

如需其他帮助，我们建议搜索 [Amazon Web Services re:Post](#) 获取与特定问题相关的内容。如果仍需帮助，请联系 [Amazon Web Services Support](#)。

排查 Amazon Web Services 账户 关闭的问题

使用以下信息帮助诊断和修复在账户关闭过程中发现的常见问题。有关账户关闭流程的一般信息，请参阅 [关闭一个 Amazon Web Services 账户](#)。

主题

- [我不知道如何删除或取消我的账户](#)
- [我在“账户”页面上看不到“关闭账户”按钮](#)
- [我关闭了账户，但仍未收到确认电子邮件](#)
- [我在尝试关闭账户时收到一条“ConstraintViolationException”错误](#)
- [我在尝试关闭成员账户时收到一条“CLOSE_ACCOUNT_QUOTA_EXCEEDED”错误](#)
- [我在关闭管理账户之前，需要删除我的 Amazon 组织吗？](#)

我不知道如何删除或取消我的账户

要关闭账户，请按照 [关闭一个 Amazon Web Services 账户](#) 中的说明操作。

我在“账户”页面上看不到“关闭账户”按钮

如果您不是以根用户身份登录，账户页面上不会显示关闭账户按钮。您必须 [以根用户身份登录 Amazon Web Services Management Console](#) 才能关闭您的账户。如果无法登录，请参阅 [排查根用户问题](#)。

我关闭了账户，但仍未收到确认电子邮件

该确认电子邮件仅发送至 Amazon Web Services 账户 的根用户电子邮件地址。如果在几个小时内未收到此电子邮件，您可以以 [根用户身份登录 Amazon Web Services Management Console](#)，查看您的账户是否关闭。如果您的账户已成功关闭，您将看到一条显示账户已关闭的信息。如果关闭的账户是成员账户，可以通过查看所关闭的账户在 Amazon Organizations 控制台中是否标记为 SUSPENDED 来验证

关闭是否成功。有关更多信息，请参阅《Amazon Organizations 用户指南》中的[关闭组织中的成员账户](#)。

如果您在尝试关闭管理账户，但没有收到有关账户关闭的确认电子邮件，则您的组织很可能有活跃的成員账户。只有当组织没有任何活跃的成員账户时，您才能关闭管理账户。要确认组织中没有剩余的活跃成員账户，请转到 Amazon Organizations 控制台，确保所有成員账户在其账户名称旁边显示 Suspended。然后就可以关闭管理账户。

我在尝试关闭账户时收到一条“ConstraintViolationException”错误

您在尝试使用 Amazon Organizations 控制台关闭管理账户，这是不可能实现的。要关闭管理账户，您需要以管理账户的[根用户身份登录 Amazon Web Services Management Console](#)，然后从账户页面中将其关闭。有关更多信息，请参阅《Amazon Organizations 用户指南》中的[关闭组织中的管理账户](#)。

我在尝试关闭成员账户时收到一条“CLOSE_ACCOUNT_QUOTA_EXCEEDED”错误

在连续 30 天的周期内，您只能关闭 10% 的成員账户。此限额不受日历月的限制，而是在您关闭账户时开始。在首次关闭账户后的 30 天内，您不能超过 10% 的账户关闭限额。最小账户关闭数量为 10 个，最大账户关闭数量为 1000 个，即使 10% 的账户在数量上超过 1000 个亦是如此。有关 Organizations 配额的更多信息，请参阅《Amazon Organizations 用户指南》中的[Amazon Organizations 配额](#)。

我在关闭管理账户之前，需要删除我的 Amazon 组织吗？

不，在关闭管理账户之前，您无需删除您的 Amazon 组织。但是只有当组织没有任何活跃的成員账户时，您才能关闭管理账户。要确认组织中没有剩余的活跃成員账户，请转到 Amazon Organizations 控制台，确保所有成員账户在其账户名称旁边显示 Suspended。然后就可以关闭管理账户。

排查其他 Amazon Web Services 账户问题

使用此处的信息有助于排查与 Amazon Web Services 账户相关的问题。

问题

- [我需要变更我的 Amazon Web Services 账户的信用卡](#)
- [我需要举报 Amazon Web Services 账户 欺诈活动](#)
- [我需要关闭我的 Amazon Web Services 账户](#)

我需要变更我的 Amazon Web Services 账户 的信用卡

若要更改您 Amazon Web Services 账户 的信用卡，您必须能够登录。Amazon 设有保护，要求您证明自己是账户所有者。有关说明，请参阅《Amazon Billing 用户指南》中的[管理您的信用卡付款方式](#)。

我需要举报 Amazon Web Services 账户 欺诈活动

如果您怀疑有欺诈活动正在使用您的 Amazon Web Services 账户，并想进行举报，请参阅[如何报告 Amazon 资源来用](#)。

如果您在 Amazon.com 上购买商品时遇到问题，请参阅[Amazon 客户服务](#)。

我需要关闭我的 Amazon Web Services 账户

如需排查 Amazon Web Services 账户 关闭问题的帮助，请参阅[关闭一个 Amazon Web Services 账户](#)。

关闭一个 Amazon Web Services 账户

如果您不再需要您的 Amazon Web Services 账户，可以按照本节中的说明随时将其关闭。关闭账户后，您可以自账户关闭之日起 90 天内将其重新打开。从关闭账户之日到 Amazon 永久关闭账户之间的时间跨度称为[后关闭期](#)。

关闭账户前的注意事项

在关闭之前 Amazon Web Services 账户，应考虑以下几点：

- 关闭账户将视作您通知终止该账户的 Amazon 客户协议。
- 在关闭资源 Amazon Web Services 账户之前，您无需删除其中的资源。但是，我们建议备份要所有保留的资源或数据。有关如何备份特定资源的说明，请参阅该服务的相应 [Amazon 文档](#)。
- 您可以在[后关闭期](#)重新打开账户。如果重新打开账户，则账户中剩余的服务将重新开始收费。您仍需对任何未付的发票以及未结的[预留实例](#)和[节省计划](#)付款。
- 您仍需对账户关闭前所用服务的所有未结费用和收费付款。关闭账户后，您将在下个月收到 Amazon 单。例如，如果您在 1 月 15 日关闭了账户，则您将在 2 月初收到 1 月 1 日至 15 日期间所产生使用量的账单。关闭账户后，您将继续收到[预留实例](#)和[节省计划](#)的发票，直至发票过期。
- 您将无法再访问您账户中以前提供的 Amazon 服务。您可以在[后关闭期](#)登录和访问已关闭的 Amazon Web Services 账户，但只能查看账单信息、访问账户设置或联系 [Amazon Web Services Support](#)。
- 您不能在关闭时将注册到 Amazon Web Services 账户的电子邮件地址用作其他 Amazon Web Services 账户的主要电子邮件。如果想在不同的 Amazon Web Services 账户使用相同的电子邮件地址，我们建议在关闭之前对其进行更新。有关更新电子邮件地址的说明，请参阅[更新根用户的 Amazon Web Services 账户名称、电子邮件地址或密码](#)。
- 如果您在 Amazon Web Services 账户 root 用户上[启用了多重身份验证 \(MFA\)](#)，或者在用户身上[配置了 MFA 设备](#)，则在您关闭账户时 MFA 不会自动删除。IAM 如果您选择在[关闭后的 90 天内](#)保持开 MFA 启状态，请保持 MFA 设备处于活动状态，直到关闭后的期限到期，以防您需要在此期间访问帐户。请注意，您的账户永久关闭后，硬件 TOTP 令牌设备无法与其他用户关联。如果您想稍后与其他用户一起使用硬件 TOTP 令牌，则可以选择在关闭账户之前[停用硬件 MFA 设备](#)。MFA [IAM 用户](#)设备必须由帐户管理员删除。

成员账户的其他注意事项

- 当您关闭成员账户时，该账户会在[后关闭期结束](#)后从组织中删除。在后关闭期内，已关闭的成员账户仍会计入组织中的账户配额。为了避免将账户计数计入账户限额，请在关闭账户之前，参阅[从您的组织中删除成员账户](#)。
- 在连续 30 天的周期内，您只能关闭 10% 的成员账户。此限额不受日历月的限制，而是在您关闭账户时开始。在首次关闭账户后的 30 天内，您不能超过 10% 的账户关闭限额。最小账户关闭数量为 10 个，最大账户关闭数量为 1000 个，即使 10% 的账户在数量上超过 1000 个亦是如此。有关 Organizations 限额的更多信息，请参阅 [Amazon Organizations 的限额](#)。
- 如果您使用 Cont Amazon rol Tower，则需要先取消对成员账户的管理，然后再尝试关闭该账户。请参阅《Amazon Control Tower 用户指南》中的 [取消管理成员账户](#)。

特定服务的注意事项

- Amazon Web Services Marketplace 账户关闭后，订阅不会自动取消。如果有任何订阅，首先[终止订阅中软件的所有实例](#)。然后，前往 Amazon Web Services Marketplace 控制台的“[管理订阅](#)”页面并取消您的订阅。
- 账户关闭后，我们 Amazon 将在最多五天内每天发送电子邮件，然后我们才会暂停该域名。域被暂停后，根据域的注册商，我们将在 30 天内删除域或将其释放给其注册商。有关更多信息，请参阅[“我的 Amazon Web Services 账户 已关闭或永久关闭”](#)，以及[我的域名已在 Route 53 中注册](#)。
- Amazon CloudTrail 是一项基础安全服务。这意味着，用户创建的跟踪即使在关闭后仍可以继续存在并传递事件，除非用户在关闭 Amazon Web Services 账户 之前明确删除了其中的跟踪。Amazon Web Services 账户 有关如何在关闭后请求删除跟踪的更多信息，请参阅《CloudTrail 用户指南》中的[Amazon Web Services 账户 闭包和跟踪](#)。Amazon Web Services 账户

如何关闭您的账户

您可以使用以下步骤关闭您 Amazon Web Services 账户 的。请注意，根据您要关闭的账户类型 [独立账户、成员账户、管理账户和 Amazon GovCloud (US)]，每个选项卡中都提供了不同的指导。

如果在关闭账户的过程中遇到任何问题，请参阅[排查 Amazon Web Services 账户 关闭的问题](#)。

Standalone account

独立账户是个人管理的账户，不是其中的一部分 Amazon Organizations。

从“账户”页面关闭独立账户

1. 以在要关闭的 Amazon Web Services 账户中，以具有所需最低权限 `portal:ModifyAccount` 的用户或角色登录。
2. 在右上角的导航栏中，选择账户名称或账号，然后选择账户。
3. 在[账户页面](#)上，选择关闭账户按钮。
4. 键入账户 ID（显示在关闭对话框的顶部），以确认您已阅读并理解账户关闭流程。
5. 选择关闭账户按钮，启动账户关闭流程。
6. 几分钟后，您应该会收到一封确认账户已注销的电子邮件。

Note

Amazon CLI 或其中一个的 API 操作不支持此任务 Amazon SDKs。您只能使用来执行此任务 Amazon Web Services Management Console。

Member account

成员帐户是 Amazon Web Services 账户 其中的一部分 Amazon Organizations。

通过 Amazon Organizations 控制台关闭成员账户

1. 登录 [Amazon Organizations 控制台](#)。
2. 在 Amazon Web Services 账户 页面上，找到并选择您想要关闭的成员账户的名称。您可以导航 OU 层次结构，或查看没有 OU 结构的账户的平面列表。
3. 选择页面顶部的账户名称旁边的 Close（关闭）。只有当 Amazon 组织处于“[所有功能](#)”模式时，此选项才可用。

Note

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

4. 阅读并确保理解账户关闭指南。
5. 输入成员账户 ID，然后选择关闭账户，启动账户关闭流程。

Note

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

从“账户”页面注销成员账户

或者，您可以直接从中的[账户页面](#)关闭 Amazon 成员账户 Amazon Web Services Management Console。如需 step-by-step 指导，请按照“独立账户”选项卡中的说明进行操作。

使用 Amazon CLI 和关闭成员账户 SDKs

有关如何使用 Amazon CLI 和关闭成员账户的说明 SDKs，请参阅 Amazon Organizations 用户指南中的[关闭组织中的成员账户](#)。

Management account

管理账户是充当 Amazon Web Services 账户 其父账户或主账号的账户 Amazon Organizations。

Note

您无法直接从 Amazon Organizations 控制台关闭管理账户。

从“账户”页面关闭管理账户

1. 在要注销的管理账户中，以具有所需最低权限 `portal:ModifyAccount` 的用户或角色身份登录。
2. 确认组织中没有剩余的活跃成员账户。为此，请前往 [Amazon Organizations 控制台](#)，确保所有成员账户在其账户名称旁边显示 `Suspended`。如果成员账户仍处于活跃状态，您需要遵循成员账户选项卡中提供的账户关闭指南，然后才能进入下一步。
3. 在右上角的导航栏中，选择账户名称或账号，然后选择账户。
4. 在[账户页面](#)上，选择关闭账户按钮。
5. 键入账户 ID（显示在关闭对话框的顶部），以确认您已阅读并理解账户关闭流程。
6. 选择关闭账户按钮，启动账户关闭流程。
7. 几分钟后，您应该会收到一封确认账户已注销的电子邮件。

Note

Amazon CLI 或其中一个的API操作不支持此任务 Amazon SDKs。您只能使用来执行此任务 Amazon Web Services Management Console。

Amazon GovCloud (US) account

出于计费 and 付款目的，Amazon GovCloud (US) 账户始终与单一标准 Amazon Web Services 账户关联。

关闭 Amazon GovCloud (US) 账户

如果您有与账户关联 Amazon Web Services 账户的 Amazon GovCloud (US) 账户，则需要先关闭标准账户，然后再关闭该 Amazon GovCloud (US) 账户。有关更多详细信息，包括如何备份数据和避免意外 Amazon GovCloud (US) 收费，请参阅 Amazon GovCloud (US) 用户指南中的[关闭 Amazon GovCloud \(US\) 账户](#)。

账户关闭后会发生什么

在关闭账户后，会立即发生以下情况：

- 您将收到一封确认账户已关闭的电子邮件，发送至根用户的电子邮件地址。如果在几个小时内未收到此电子邮件，请参阅[排查 Amazon Web Services 账户 关闭的问题](#)。
- 您关闭的任何成员账户都将在 Amazon Organizations 控制台中账户名称旁边显示一个SUSPENDED标签，有效期最长为原始关闭日期后的 90 天。90 天后，Amazon Organizations 控制台中将不再显示成员账户。
- 如果您已 Amazon Web Services 账户 向其他账户授予访问您中服务的权限，则账户关闭后，从这些账户发出的任何访问请求都将失败。如果您重新打开 Amazon Web Services 账户，如果您向其他人授予了必要的权限，则他们 Amazon Web Services 账户 可以再次访问您账户的 Amazon 服务和资源。

后关闭期

关闭后期是指从您关闭账户之日到 Amazon 永久关闭账户 Amazon Web Services 账户之间的时间长度。后关闭期为 90 天。在后关闭期间，您只能通过重新开立账户来访问内容或 Amazon 服务。关闭后期过后，将 Amazon 永久关闭您的 Amazon Web Services 账户，您将无法再重新开放。

Amazon 还将删除您账户中的内容和资源（CloudTrail 路径除外）。账户永久关闭后，其 [Amazon Web Services 账户 ID](#) 将永远无法重复使用。

重新打开你的 Amazon Web Services 账户

您的账户将在 90 天后永久关闭，之后您将无法重新打开账户，Amazon 并将删除账户中剩余的内容。要在账户永久关闭之前将其重新打开，(1) 您必须尽快联系 [Amazon Web Services Support](#)；(2) 我们必须自账户关闭之日起 60 天内收到所有未付余额的全额付款，包括根据发票上的规定提供必要信息。

Note

如果重新打开账户，则账户中剩余的服务将重新开始收费。

API 参考

借助账户管理 (account) 命名空间中的 API 操作，您可以修改自己的 Amazon Web Services 账户。

每个 Amazon Web Services 账户 都支持包含账户信息的元数据，包括与账户关联的最多三个备用联系人的信息。除此之外，还有与账户的[根用户](#)关联的电子邮件地址。您只能从与账户关联的以下联系人类型中指定一个类型。

- 账单联系人
- 操作联系人
- 安全联系人

默认情况下，本指南中所述的 API 操作直接适用于调用此操作的账户。操作调用账户中的[身份](#)通常是 IAM 角色或 IAM 用户，它必须拥有 IAM 策略应用的权限才能调用 API 操作。或者，可以通过 Amazon Organizations 管理账户中的身份调用这些 API 操作，并为属于组织成员的任何 Amazon Web Services 账户 指定账户 ID 号。

API 版本

本版《账户 API 参考》记录了 2021-02-01 版的账户管理 API。

Note

除了直接使用 API 之外，您还可以使用其中一个 Amazon 软件开发工具包：其中包含各种编程语言和平台（Java、Ruby、.NET、iOS、Android 等）的库和示例代码。这些开发工具包提供了一种简便方法，以使用编程方式访问 Amazon 组织。例如，软件开发工具包处理加密签署请求、管理错误以及自动重试请求工作。有关 Amazon 开发工具包的更多信息（包括如何下载和安装这些工具包），请参阅[适用于 Amazon Web Services 的工具](#)。

我们建议使用 Amazon 软件开发工具包对账户管理服务进行编程 API 调用。但是，您也可以使用账户管理查询 API 直接调用账户管理的 Web 服务。要了解有关账户管理查询 API 的更多信息，请参阅《账户管理用户指南》中的[通过提出 HTTP 查询请求来调用 API](#)。组织支持所有操作的 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。因此，对于需要更大规模的操作，请使用 POST 请求。

签署请求

当您将 HTTP 请求发送到 Amazon 时，您必须签署请求，以便 Amazon 能够识别发送它们的用户。您将使用您的 Amazon 访问密钥来签署请求，该访问密钥包含访问密钥 ID 和秘密访问密钥。我们强烈建议您不要为根账户创建访问密钥。拥有您的根账户的访问密钥的任何人都可以无限制地访问您账户中的所有资源。相反，应为具有管理权限的 IAM 用户创建访问密钥。另外一个选项是使用 Amazon Security Token Service 生成临时安全凭证，并使用这些凭证对请求进行签名。

如需对请求进行签名，建议您使用签名版本 4。如果现有应用程序使用签名版本 2，则无需将其更新即可使用签名版本 4。但是，目前某些操作需要签名版本 4。需要版本 4 的操作的文档指出了这一要求。有关更多信息，请参阅《IAM 用户指南》中的[签署 Amazon API 请求](#)。

当您使用 Amazon 命令行界面 (Amazon CLI) 或其中一个 Amazon 开发工具包来向 Amazon 发出请求时，这些工具会自动使用您在配置工具时指定的访问密钥为您签署请求。

对账户管理的支持和反馈

我们欢迎您提供反馈。请将您的意见发送至 feedback-awsaccounts@amazon.com，或将反馈和问题发布在[账户管理支持论坛](#)上。有关 Amazon 支持论坛的更多信息，请参阅[论坛帮助](#)。

示例呈现方式

作为对请求的响应，账户管理返回的 JSON 将以单个长字符串形式返回，不含换行符或格式化空格。为提高可读性，本指南中的示例同时显示了换行符和空格。当示例输入参数也会产生超出屏幕范围的长字符串时，我们会插入换行符以增强可读性。您应始终以单个 JSON 文本字符串的形式提交输入。

记录 API 请求

账户管理支持 CloudTrail，该服务可以轻松地记录 Amazon Web Services 账户的 Amazon API 调用并将日志文件传输至 Amazon S3 存储桶。通过使用 CloudTrail 收集的信息，您可以确定成功向账户管理提出的请求、谁提出请求以及何时提出等信息。有关账户管理及其支持 CloudTrail 的更多信息，请参阅[使用记录 Amazon 账户管理 API 呼叫 Amazon CloudTrail](#)。要了解有关 CloudTrail 的更多信息 (包括如何启用该服务及如何查找日志文件)，请参阅[Amazon CloudTrail 用户指南](#)。

操作

支持以下操作：

- [AcceptPrimaryEmailUpdate](#)
- [DeleteAlternateContact](#)
- [DisableRegion](#)

- [EnableRegion](#)
- [GetAlternateContact](#)
- [GetContactInformation](#)
- [GetPrimaryEmail](#)
- [GetRegionOptStatus](#)
- [ListRegions](#)
- [PutAlternateContact](#)
- [PutContactInformation](#)
- [StartPrimaryEmailUpdate](#)

AcceptPrimaryEmailUpdate

接受来自 [StartPrimaryEmailUpdate](#) 的要求为指定账户更新亚马逊科技电子邮件地址的请求。

请求语法

```
POST /acceptPrimaryEmailUpdate HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "Otp": "string",
  "PrimaryEmail": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

[AccountId](#)

指定要通过此操作访问或修改的 Amazon Web Services 账户 账户的 12 位账户 ID 号。要使用此参数，调用方必须具有[组织管理账户](#)或委托管理员账户中的身份。指定账户 ID 必须是同一组织内的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

此操作只能由组织的管理账户或委托管理员账户为成员账户调用。

Note

管理账户无法指定自己的 AccountId。

类型：字符串

模式：`^\d{12}$`

必需：是

Otp

发送到 StartPrimaryEmailUpdate API 调用指定 PrimaryEmail 的 OTP 代码。

类型：字符串

模式：`^[a-zA-Z0-9]{6}$`

必需：是

PrimaryEmail

与指定账户一起使用的新的亚马逊云科技电子邮件地址。这必须与 StartPrimaryEmailUpdate API 调用中的 PrimaryEmail 一致。

类型：字符串

长度限制：最小长度为 5。长度上限为 64。

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
  "Status": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

Status

检索已接受的亚马逊云科技电子邮件更新请求的状态。

类型：字符串

有效值：PENDING | ACCEPTED

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

ConflictException

由于资源的当前状态存在冲突，因此无法处理该请求。例如，如果尝试启用当前已禁用（处于“禁用”状态）的区域，或者尝试将账户的亚马逊云科技电子邮件更改为已在使用的电子邮件地址，就会发生这种情况。

HTTP 状态代码：409

InternalServerErrorException

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

ResourceNotFoundException

操作失败，找不到指定的资源。

HTTP 状态代码：404

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)
- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

DeleteAlternateContact

从 Amazon Web Services 账户 中删除指定的备用联系人。

关于如何使用备用联系人操作的完整详细信息，请参阅[访问或更新备用联系人](#)。

Note

在更新由 Amazon Organizations 管理的 Amazon Web Services 账户 的备用联系人信息之前，必须先启用 Amazon 账户管理和组织之间的集成。有关更多信息，请参阅[对 Amazon 账户管理启用可信的访问权限](#)。

请求语法

```
POST /deleteAlternateContact HTTP/1.1
Content-type: application/json
```

```
{
  "AccountId": "string",
  "AlternateContactType": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

AccountId

指定要通过此操作访问或修改的 Amazon 账户的 12 位账户 ID 号。

如果未指定此参数，则默认为调用此操作使用的身份的 Amazon 账户。

要使用此参数，调用方必须具有[组织管理账户](#)或委托管理员账户中的身份，并且指定的账户 ID 必须是同一组织中的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

Note

管理账户无法自行指定其 AccountId；它必须在不包括 AccountId 参数的情况下，在独立上下文中调用此操作。

要对不是组织成员的账户调用此操作，不要指定此参数，请以属于要检索或修改其联系人的账户的身份调用此操作。

类型：字符串

模式：`^\d{12}$`

必需：否

AlternateContactType

指定要删除的备用联系人。

类型：字符串

有效值：BILLING | OPERATIONS | SECURITY

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerErrorException

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

ResourceNotFoundException

操作失败，找不到指定的资源。

HTTP 状态代码：404

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

示例

示例 1

以下示例删除了其凭证用于调用操作的账户的安全备用联系人。

示例请求

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AlternateContactType": "SECURITY" }
```

示例响应

```
HTTP/1.1 200 OK
Content-Type: application/json
```

示例 2

以下示例删除了组织中指定成员账户的账单备用联系人。必须使用来自组织管理账户或账户管理服务的委托管理员账户的证书。

示例请求

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "BILLING" }
```

示例响应

```
HTTP/1.1 200 OK
Content-Type: application/json
```

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)
- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

DisableRegion

禁用 (选择退出) 账户的特定区域。

Note

禁用区域的行为会移除对该区域内任何资源的所有 IAM 访问权限。

请求语法

```
POST /disableRegion HTTP/1.1
Content-type: application/json
```

```
{
  "AccountId": "string",
  "RegionName": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

AccountId

指定要通过此操作访问或修改的 Amazon Web Services 账户 账户的 12 位账户 ID 号。如果未指定此参数，则默认为调用此操作使用的身份的亚马逊云科技账户。要使用此参数，调用方必须具有[组织管理账户](#)或委托管理员账户中的身份。指定账户 ID 必须是同一组织内的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

Note

管理账户无法指定自己的 AccountId。它必须在不包括 AccountId 参数的情况下，在独立上下文中调用此操作。

要对不是组织成员的账户调用此操作，不要指定此参数。相反，请以属于要检索或修改其联系人的账户的身份调用此操作。

类型：字符串

模式：`^\d{12}$`

必需：否

RegionName

为给定区域名称指定区域代码（例如，af-south-1）。在禁用一个区域时，Amazon 将执行操作以在您账户中停用此区域，例如销毁此区域的 IAM 资源。对大多数账户而言，此过程需要几分钟时间，但也有可能要用数小时的时间。在禁用过程彻底完成之前，您无法启用该区域。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

ConflictException

由于资源的当前状态存在冲突，因此无法处理该请求。例如，如果尝试启用当前已禁用（处于“禁用”状态）的区域，或者尝试将账户的亚马逊云科技电子邮件更改为已在使用的电子邮件地址，就会发生这种情况。

HTTP 状态代码：409

InternalServerError

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)
- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

EnableRegion

为账户启用 (选择加入) 特定区域。

请求语法

```
POST /enableRegion HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "RegionName": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

AccountId

指定要通过此操作访问或修改的 Amazon Web Services 账户 账户的 12 位账户 ID 号。如果未指定此参数，则默认为调用此操作使用的身份的亚马逊云科技账户。要使用此参数，调用方必须具有[组织管理账户](#)或委托管理员账户中的身份。指定账户 ID 必须是同一组织内的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

Note

管理账户无法指定自己的 AccountId。它必须在不包括 AccountId 参数的情况下，在独立上下文中调用此操作。

要对不是组织成员的账户调用此操作，不要指定此参数。相反，请以属于要检索或修改其联系人的账户的身份调用此操作。

类型：字符串

模式：`^\d{12}$`

必需：否

RegionName

为给定区域名称指定区域代码（例如，af-south-1）。在启用一个区域时，Amazon 将执行操作以准备您在该区域内的账户，例如将您的 IAM 资源分发给该区域。对大多数账户而言，此过程需要几分钟时间，但也有可能要用数小时的时间。在此过程完成之前，您无法使用区域。此外，在启用过程彻底完成之前，您无法禁用该区域。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

ConflictException

由于资源的当前状态存在冲突，因此无法处理该请求。例如，如果尝试启用当前已禁用（处于“禁用”状态）的区域，或者尝试将账户的亚马逊云科技电子邮件更改为已在使用的电子邮件地址，就会发生这种情况。

HTTP 状态代码：409

InternalServerError

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)
- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

GetAlternateContact

检索附加到 Amazon Web Services 账户 的指定备用联系人。

关于如何使用备用联系人操作的完整详细信息，请参阅[访问或更新备用联系人](#)。

Note

在更新由 Amazon Organizations 管理的 Amazon Web Services 账户 的备用联系人信息之前，必须先启用 Amazon 账户管理和组织之间的集成。有关更多信息，请参阅[对 Amazon 账户管理启用可信的访问权限](#)。

请求语法

```
POST /getAlternateContact HTTP/1.1
```

```
Content-type: application/json
```

```
{  
  "AccountId": "string",  
  "AlternateContactType": "string"  
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

[AccountId](#)

指定要通过此操作访问或修改的 Amazon 账户的 12 位账户 ID 号。

如果未指定此参数，则默认为调用此操作使用的身份的 Amazon 账户。

要使用此参数，调用方必须具有[组织管理账户](#)或委托管理员账户中的身份，并且指定的账户 ID 必须是同一组织中的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

Note

管理账户无法自行指定其 AccountId；它必须在不包括 AccountId 参数的情况下，在独立上下文中调用此操作。

要对不是组织成员的账户调用此操作，不要指定此参数，请以属于要检索或修改其联系人的账户的身份调用此操作。

类型：字符串

模式：`^\d{12}$`

必需：否

AlternateContactType

指定要检索的备用联系人。

类型：字符串

有效值：BILLING | OPERATIONS | SECURITY

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
  "AlternateContact": {
    "AlternateContactType": "string",
    "EmailAddress": "string",
    "Name": "string",
    "PhoneNumber": "string",
    "Title": "string"
  }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

AlternateContact

包含指定备用联系人详细信息的结构。

类型：[AlternateContact](#) 对象

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerError

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

ResourceNotFoundException

操作失败，找不到指定的资源。

HTTP 状态代码：404

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

示例

示例 1

以下示例检索其凭证用于调用操作的账户的安全备用联系人。

示例请求

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AlternateContactType": "SECURITY" }
```

示例响应

```
HTTP/1.1 200 OK
Content-Type: application/json{
  "AlternateContact": {
    "Name": "Anika",
    "Title": "COO",
    "EmailAddress": "anika@example.com",
    "PhoneNumber": "206-555-0198"
    "AlternateContactType": "Security"
  }
}
```

示例 2

以下示例检索组织中指定成员账户的操作备用联系人。必须使用来自组织管理账户或账户管理服务的委托管理员账户的证书。

示例请求

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "Operations" }
```

示例响应

```
HTTP/1.1 200 OK
```



```
Content-Type: application/json{
  "AlternateContact": {
    "Name": "Anika",
    "Title": "COO",
    "EmailAddress": "anika@example.com",
    "PhoneNumber": "206-555-0198"
    "AlternateContactType": "Operations"
  }
}
```

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)
- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

GetContactInformation

检索 Amazon Web Services 账户 的主要联系人信息。

关于如何使用主要联系人操作的完整详细信息，请参阅[更新主要和备用联系人信息](#)。

请求语法

```
POST /getContactInformation HTTP/1.1
Content-type: application/json

{
  "AccountId": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

[AccountId](#)

指定要通过此操作访问或修改的 Amazon Web Services 账户 账户的 12 位账户 ID 号。如果未指定此参数，则默认为调用此操作使用的身份的亚马逊云科技账户。要使用此参数，调用方必须具有[组织管理账户](#)或委托管理员账户中的身份。指定账户 ID 必须是同一组织内的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

Note

管理账户无法指定自己的 AccountId。它必须在不包括 AccountId 参数的情况下，在独立上下文中调用此操作。

要对不是组织成员的账户调用此操作，不要指定此参数。相反，请以属于要检索或修改其联系人的账户的身份调用此操作。

类型：字符串

模式：`^\d{12}$`

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
  "ContactInformation": {
    "AddressLine1": "string",
    "AddressLine2": "string",
    "AddressLine3": "string",
    "City": "string",
    "CompanyName": "string",
    "CountryCode": "string",
    "DistrictOrCounty": "string",
    "FullName": "string",
    "PhoneNumber": "string",
    "PostalCode": "string",
    "StateOrRegion": "string",
    "WebsiteUrl": "string"
  }
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

[ContactInformation](#)

包含与 Amazon Web Services 账户 相关的主要联系人信息的详细信息。

类型：[ContactInformation](#) 对象

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerErrorException

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

ResourceNotFoundException

操作失败，找不到指定的资源。

HTTP 状态代码：404

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)
- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)

- [适用于 Ruby V3 的 Amazon SDK](#)

GetPrimaryEmail

检索指定账户的亚马逊云科技电子邮件地址。

请求语法

```
POST /getPrimaryEmail HTTP/1.1
Content-type: application/json

{
  "AccountId": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

AccountId

指定要通过此操作访问或修改的 Amazon Web Services 账户 账户的 12 位账户 ID 号。要使用此参数，调用方必须具有[组织管理账户](#)或委托管理员账户中的身份。指定账户 ID 必须是同一组织内的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

此操作只能由组织的管理账户或委托管理员账户为成员账户调用。

Note

管理账户无法指定自己的 AccountId。

类型：字符串

模式：`^\d{12}$`

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
  "PrimaryEmail": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

PrimaryEmail

检索与指定账户关联的亚马逊云科技电子邮件地址。

类型：字符串

长度限制：最小长度为 5。长度上限为 64。

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerError

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

ResourceNotFoundException

操作失败，找不到指定的资源。

HTTP 状态代码：404

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)
- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

GetRegionOptStatus

检索特定区域的选择加入状态。

请求语法

```
POST /getRegionOptStatus HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "RegionName": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

AccountId

指定要通过此操作访问或修改的 Amazon Web Services 账户 账户的 12 位账户 ID 号。如果未指定此参数，则默认为调用此操作使用的身份的亚马逊云科技账户。要使用此参数，调用方必须具有[组织管理账户](#)或委托管理员账户中的身份。指定账户 ID 必须是同一组织内的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

Note

管理账户无法指定自己的 AccountId。它必须在不包括 AccountId 参数的情况下，在独立上下文中调用此操作。

要对不是组织成员的账户调用此操作，不要指定此参数。相反，请以属于要检索或修改其联系人的账户的身份调用此操作。

类型：字符串

模式：`^\d{12}$`

必需：否

RegionName

为给定区域名称指定区域代码（例如，af-south-1）。此函数将返回您传递此参数的任何目标区域的状态。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
  "RegionName": "string",
  "RegionOptStatus": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

RegionName

传入的区域代码。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

RegionOptStatus

区域可能处于以下潜在状态之一（已启用、启用、已禁用、禁用、默认已启用）。

类型：字符串

有效值：ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerErrorException

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)
- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

ListRegions

列出给定账户的所有区域及其各自的选择加入状态。也可以选择按 `region-opt-status-contains` 参数筛选此列表。

请求语法

```
POST /listRegions HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "MaxResults": number,
  "NextToken": "string",
  "RegionOptStatusContains": [ "string" ]
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

AccountId

指定要通过此操作访问或修改的 Amazon Web Services 账户 12 位账户 ID 号。如果未指定此参数，则默认为调用此操作使用的身份的亚马逊云科技账户。要使用此参数，调用方必须具有[组织管理账户](#)或委托管理员账户中的身份。指定账户 ID 必须是同一组织内的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

Note

管理账户无法指定自己的 AccountId。它必须在不包括 AccountId 参数的情况下，在独立上下文中调用此操作。

要对不是组织成员的账户调用此操作，不要指定此参数。相反，请以属于要检索或修改其联系人的账户的身份调用此操作。

类型：字符串

模式：`^\d{12}$`

必需：否

MaxResults

命令的输出中要返回的项目总数。如果可用的总项目数超过指定的值，则命令的输出中会提供 NextToken。要恢复分页，请在后续命令的 `starting-token` 参数中提供 NextToken 值。请勿在 Amazon CLI 之外直接使用 NextToken 响应元素。有关用法示例，请参阅《Amazon 命令行用户指南》中的[分页](#)。

类型：整数

有效范围：最小值为 1。最大值为 50。

必需：否

NextToken

用于指定从何处开始分页的令牌。这是先前截断的响应中的 NextToken。有关用法示例，请参阅《Amazon 命令行用户指南》中的[分页](#)。

类型：字符串

长度约束：最小长度为 0。最大长度为 1000。

必需：否

RegionOptStatusContains

区域状态列表（启用、已启用、禁用、已禁用、默认已启用），用于筛选给定账户的区域列表。例如，传入值为“启用”时将仅返回区域状态为“启用”的区域列表。

类型：字符串数组

有效值：`ENABLED` | `ENABLING` | `DISABLING` | `DISABLED` | `ENABLED_BY_DEFAULT`

必需：否

响应语法

```
HTTP/1.1 200
Content-type: application/json
```

```
{
  "NextToken": "string",
  "Regions": [
    {
      "RegionName": "string",
      "RegionOptStatus": "string"
    }
  ]
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

NextToken

如果要返回更多数据，则会填充该数据。它应该传到的 `list-regions` 的请求参数 `next-token` 中。

类型：字符串

Regions

这是给定账户的区域列表，或与 `filter` 参数中设置的筛选条件相匹配的区域列表（如果使用了筛选参数）。

类型：[Region](#) 对象数组

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerError

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)
- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

PutAlternateContact

修改附加到 Amazon Web Services 账户 的指定备用联系人。

关于如何使用备用联系人操作的完整详细信息，请参阅[访问或更新备用联系人](#)。

Note

在更新由 Amazon Organizations 管理的 Amazon Web Services 账户 的备用联系人信息之前，必须先启用 Amazon 账户管理和组织之间的集成。有关更多信息，请参阅[对 Amazon 账户管理启用可信的访问权限](#)。

请求语法

```
POST /putAlternateContact HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "AlternateContactType": "string",
  "EmailAddress": "string",
  "Name": "string",
  "PhoneNumber": "string",
  "Title": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体


请求接受采用 JSON 格式的以下数据。

AccountId

指定要通过此操作访问或修改的 Amazon 账户的 12 位账户 ID 号。

如果未指定此参数，则默认为调用此操作使用的身份的 Amazon 账户。

要使用此参数，调用方必须具有[组织管理账户](#)或委托管理员账户中的身份，并且指定的账户 ID 必须是同一组织中的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

 Note

管理账户无法自行指定其 AccountId；它必须在不包括 AccountId 参数的情况下，在独立上下文中调用此操作。

要对不是组织成员的账户调用此操作，不要指定此参数，请以属于要检索或修改其联系人的账户的身份调用此操作。

类型：字符串

模式：`^\d{12}$`

必需：否

[AlternateContactType](#)

指定要创建或更新的备用联系人。

类型：字符串

有效值：BILLING | OPERATIONS | SECURITY

必需：是

[EmailAddress](#)

为备用联系人指定电子邮件地址。

类型：字符串

长度限制：长度下限为 1。最大长度为 254。

模式：`^[\\s]*[\\w+=.#!&-]+@[\\w.-]+\\. [\\w]+[\\s]*$`

必需：是

[Name](#)

为备用联系人指定姓名。

类型：字符串

长度限制：长度下限为 1。长度上限为 64。

必需：是

PhoneNumber

为备用联系人指定电话号码。

类型：字符串

长度限制：长度下限为 1。最大长度为 25。

模式：`^\s0-9()+-]+$`

必需：是

Title

为备用联系人指定职务。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerError

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

示例

示例 1

以下示例为其凭证用于调用操作的账户设置账单备用联系人。

示例请求

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
  "AlternateContactType": "Billing",
  "Name": "Carlos Salazar",
  "Title": "CFO",
  "EmailAddress": "carlos@example.com",
  "PhoneNumber": "206-555-0199"
}
```

示例响应

```
HTTP/1.1 200 OK
Content-Type: application/json
```

示例 2

以下示例为组织的指定成员账户设置或改写账单备用联系人。必须使用来自组织管理账户或账户管理服务的委托管理员账户的证书。

示例请求

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
  "AccountId": "123456789012",
  "AlternateContactType": "Billing",
  "Name": "Carlos Salazar",
  "Title": "CFO",
  "EmailAddress": "carlos@example.com",
  "PhoneNumber": "206-555-0199"
}
```

示例响应

```
HTTP/1.1 200 OK
Content-Type: application/json
```

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)
- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

PutContactInformation

更新 Amazon Web Services 账户 的主要联系人信息。

关于如何使用主要联系人操作的完整详细信息，请参阅[更新主要和备用联系人信息](#)。

请求语法

```
POST /putContactInformation HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "ContactInformation": {
    "AddressLine1": "string",
    "AddressLine2": "string",
    "AddressLine3": "string",
    "City": "string",
    "CompanyName": "string",
    "CountryCode": "string",
    "DistrictOrCounty": "string",
    "FullName": "string",
    "PhoneNumber": "string",
    "PostalCode": "string",
    "StateOrRegion": "string",
    "WebsiteUrl": "string"
  }
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

AccountId

指定要通过此操作访问或修改的 Amazon Web Services 账户 账户的 12 位账户 ID 号。如果未指定此参数，则默认为调用此操作使用的身份的亚马逊云科技账户。要使用此参数，调用方必须具有[组](#)

[组织管理账户](#)或委托管理员账户中的身份。指定账户 ID 必须是同一组织内的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

Note

管理账户无法指定自己的 AccountId。它必须在不包括 AccountId 参数的情况下，在独立上下文中调用此操作。

要对不是组织成员的账户调用此操作，不要指定此参数。相反，请以属于要检索或修改其联系人的账户的身份调用此操作。

类型：字符串

模式：`^\d{12}$`

必需：否

[ContactInformation](#)

包含与 Amazon Web Services 账户 相关的主要联系人信息的详细信息。

类型：[ContactInformation](#) 对象

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 200 响应。

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerError

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)
- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

StartPrimaryEmailUpdate

启动为指定账户更新亚马逊科技电子邮件地址的流程。

请求语法

```
POST /startPrimaryEmailUpdate HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "PrimaryEmail": "string"
}
```

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

AccountId

指定要通过此操作访问或修改的 Amazon Web Services 账户 账户的 12 位账户 ID 号。要使用此参数，调用方必须具有[组织管理账户](#)或委托管理员账户中的身份。指定账户 ID 必须是同一组织内的成员账户。组织必须[启用所有功能](#)，且组织必须为账户管理服务启用[可信访问权限](#)，可选择分配[委托管理员](#)账户。

此操作只能由组织的管理账户或委托管理员账户为成员账户调用。

Note

管理账户无法指定自己的 AccountId。

类型：字符串

模式：`^\d{12}$`

必需：是

PrimaryEmail

在指定账户中使用的新亚马逊云科技电子邮件地址。

类型：字符串

长度限制：最小长度为 5。长度上限为 64。

必需：是

响应语法

```
HTTP/1.1 200
Content-type: application/json

{
  "Status": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

Status

亚马逊云科技电子邮件更新请求的状态。

类型：字符串

有效值：PENDING | ACCEPTED

错误

有关所有操作的常见错误的信息，请参阅[常见错误](#)。

AccessDeniedException

操作失败，调用身份没有所需的最低权限。

HTTP 状态代码：403

ConflictException

由于资源的当前状态存在冲突，因此无法处理该请求。例如，如果尝试启用当前已禁用（处于“禁用”状态）的区域，或者尝试将账户的亚马逊云科技电子邮件更改为已在使用的电子邮件地址，就会发生这种情况。

HTTP 状态代码：409

InternalServerErrorException

操作失败，Amazon 内部存在错误。请稍后重新尝试操作。

HTTP 状态代码：500

ResourceNotFoundException

操作失败，找不到指定的资源。

HTTP 状态代码：404

TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

HTTP 状态代码：400

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [Amazon 命令行界面](#)
- [适用于 .NET 的 Amazon SDK](#)
- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Go v2 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [Amazon 适用于 JavaScript 的开发工具包 V3](#)

- [适用于 PHP V3 的 Amazon SDK](#)
- [适用于 Python 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

其他 Amazon 服务中的相关操作

以下操作与 Amazon Account Management 相关但属于 Amazon Organizations 命名空间的一部分：

- [CreateAccount](#)
- [CreateGovCloudAccount](#)
- [DescribeAccount](#)

CreateAccount

CreateAccount API 操作只能在 Amazon Organizations 服务管理的组织环境中使用。API 操作的定义见该服务的命名空间。

有关更多信息，请参阅《Amazon Organizations API 参考》中的 [CreateAccount](#)。

CreateGovCloudAccount

CreateGovCloudAccount API 操作只能在 Amazon Organizations 服务管理的组织环境中使用。API 操作的定义见该服务的命名空间。

有关更多信息，请参阅《Amazon Organizations API 参考》中的 [CreateGovCloudAccount](#)。

DescribeAccount

DescribeAccount API 操作只能在 Amazon Organizations 服务管理的组织环境中使用。API 操作的定义见该服务的命名空间。

有关更多信息，请参阅《Amazon Organizations API 参考》中的 [DescribeAccount](#)。

数据类型

支持以下数据类型：

- [AlternateContact](#)

- [ContactInformation](#)
- [Region](#)
- [ValidationExceptionField](#)

AlternateContact

此结构包含与 Amazon 账户关联的备用联系人的详细信息

内容

AlternateContactType

备用联系人的类型。

类型：字符串

有效值：BILLING | OPERATIONS | SECURITY

必需：否

EmailAddress

与此备用联系人关联的电子邮件地址。

类型：字符串

长度限制：长度下限为 1。最大长度为 254。

模式：`^[\\s]*[\\w+=.#!&-]+@[\\w.-]+\\. [\\w]+[\\s]*$`

必需：否

Name

与此备用联系人关联的姓名。

类型：字符串

长度限制：长度下限为 1。长度上限为 64。

必需：否

PhoneNumber

与此备用联系人关联的电话号码。

类型：字符串

长度限制：长度下限为 1。最大长度为 25。

模式：`^[\\s0-9()+-]+$`

必需：否

Title

与此备用联系人关联的头衔。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：否

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

ContactInformation

包含与 Amazon Web Services 账户 关联的主要联系人信息的详细信息。

内容

AddressLine1

主要联系人地址中的第一行。

类型：字符串

长度限制：长度下限为 1。最大长度为 60。

必需：是

City

主要联系人地址中的城市。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：是

CountryCode

主要联系人地址中的 ISO-3166 双字母国家/地区代码。

类型：字符串

长度限制：固定长度为 2。

必需：是

FullName

主要联系人地址中的全名。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：是

PhoneNumber

主要联系人信息中的电话号码。该号码将经过验证，在某些国家/地区将检查是否激活。

类型：字符串

长度限制：长度下限为 1。最大长度为 20。

模式：`^[+][\s0-9()-]+`

必需：是

PostalCode

主要联系人地址中的邮政编码。

类型：字符串

长度限制：长度下限为 1。最大长度为 20。

必需：是

AddressLine2

主要联系人地址中的第二行（如有）。

类型：字符串

长度限制：长度下限为 1。最大长度为 60。

必需：否

AddressLine3

主要联系人地址中的第三行（如有）。

类型：字符串

长度限制：长度下限为 1。最大长度为 60。

必需：否

CompanyName

与主要联系人信息关联的公司的名称（如有）。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：否

DistrictOrCounty

主要联系人地址中的地区或县（如有）。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：否

StateOrRegion

主要联系人地址中的州或地区。如果邮寄地址位于美国 (US) 境内，则此字段中的值可以是双字符州代码（例如 NJ），也可以是州的全名（例如 New Jersey）。以下国家/地区需填写此字段：US、CA、GB、DE、JP、IN 和 BR。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：否

WebsiteUrl

与主要联系人信息关联的网站的 URL（如有）。

类型：字符串

长度限制：最小长度为 1。最大长度为 256。

必需：否

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

Region

这是一种表示给定账户的地区的结构，其中包括一个名称和选择加入状态。

内容

RegionName

给定地区的区域代码（例如 `us-east-1`）。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：否

RegionOptStatus

区域可能处于以下潜在状态之一（已启用、启用、已禁用、禁用、默认已启用）。

类型：字符串

有效值：ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT

必需：否

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

ValidationExceptionField

输入不满足 Amazon 服务在指定字段中指定的限制。

内容

message

验证异常的相关消息。

类型：字符串

必需：是

name

检测到无效条目的字段名称。

类型：字符串

必需：是

另请参阅

有关在特定语言的 Amazon SDK 中使用此 API 的更多信息，请参阅以下内容：

- [适用于 C++ 的 Amazon SDK](#)
- [适用于 Java V2 的 Amazon SDK](#)
- [适用于 Ruby V3 的 Amazon SDK](#)

常见参数

以下列表包含所有操作用于使用查询字符串对 Signature Version 4 请求进行签名的参数。任何特定于操作的参数都列在该操作的主题中。有关 Signature Version 4 的更多信息，请参阅《IAM 用户指南》中的[签署 Amazon API 请求](#)。

Action

要执行的操作。

类型：字符串。

必需：是

Version

编写请求所针对的 API 版本，格式为 YYYY-MM-DD。

类型：字符串。

必需：是

X-Amz-Algorithm

您用于创建请求签名的哈希算法。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

有效值：AWS4-HMAC-SHA256

必需：条件

X-Amz-Credential

凭证范围值，该值是一个字符串，其中包含您的访问密钥、日期、您要定位的区域、您请求的服务以及终止字符串（“aws4_request”）。值采用以下格式表示：access_key/YYYYMMDD/region/service/aws4_request。

有关更多信息，请参阅《IAM 用户指南》中的[创建已签名的 Amazon API 请求](#)。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

必需：条件

X-Amz-Date

用于创建签名的日期。格式必须为 ISO 8601 基本格式 (YYYYMMDD'T'HHMMSS'Z')。例如，以下日期时间是有效的 X-Amz-Date 值：20120325T120000Z。

条件：X-Amz-Date 对于所有请求都是可选的；它可以用于覆盖对请求签名所使用的日期。如果以 ISO 8601 基本格式指定 Date 标头，则不需要 X-Amz-Date。使用 X-Amz-Date 时，它始终会覆盖 Date 标头的值。有关更多信息，请参阅《IAM 用户指南》中的[Amazon API 请求签名的元素](#)。

类型：字符串

必需：条件

X-Amz-Security-Token

通过调用 Amazon Security Token Service (Amazon STS) 获得的临时安全令牌。有关支持来自 Amazon STS 的临时安全凭证的服务列表，请参阅《IAM 用户指南》中的[使用 IAM 的 Amazon Web Services 服务](#)。

条件：如果您使用来自 Amazon STS 的临时安全凭证，则必须包含安全令牌。

类型：字符串

必需：条件

X-Amz-Signature

指定从要签名的字符串和派生的签名密钥计算的十六进制编码签名。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

必需：条件

X-Amz-SignedHeaders

指定作为规范请求的一部分包含的所有 HTTP 标头。有关指定已签名标头的更多信息，请参阅《IAM 用户指南》中的[创建已签名的 Amazon API 请求](#)。

条件：当您在查询字符串中而不是 HTTP 授权标头中包括身份验证信息时，请指定此参数。

类型：字符串

必需：条件

常见错误

本部分列出了所有 Amazon 服务的常见 API 操作错误。对于特定于此服务的 API 操作的错误，请参阅该 API 操作的主题。

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：400

IncompleteSignature

请求签名不符合 Amazon 标准。

HTTP 状态代码：400

InternalFailure

由于未知错误、异常或故障，请求处理失败。

HTTP 状态代码：500

InvalidAction

所请求的操作无效。确认正确键入了操作。

HTTP 状态代码：400

InvalidClientTokenId

在我们的记录中没有所提供的 X.509 证书或 Amazon 访问密钥 ID。

HTTP 状态代码：403

NotAuthorized

您无权执行此操作。

HTTP 状态代码：400

OptInRequired

Amazon 访问密钥 ID 需要订阅服务。

HTTP 状态代码：403

RequestExpired

请求到达服务的时间超过请求上的日期戳 15 分钟或超过请求到期日期 15 分钟（例如，对于预签名 URL），或者请求上的日期戳比当前时间晚了 15 分钟以上。

HTTP 状态代码：400

ServiceUnavailable

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：503

ThrottlingException

由于请求限制而导致请求被拒绝。

HTTP 状态代码：400

ValidationError

输入未能满足 Amazon 服务指定的约束。

HTTP 状态代码：400

通过提出 HTTP 查询请求来调用 API

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

Note

您可以使用 Amazon 开发工具包之一，代替对 Amazon 账户管理查询 API 进行直接调用。Amazon 开发工具包中包含适用于各种编程语言和平台（Java、Ruby、.NET、iOS、Android 等）的库和示例代码。这些开发工具包提供了一种简便方法，以使用编程方式访问 Amazon 账户管理和 Amazon。例如，软件开发工具包执行以下类似任务：加密签署请求、管理错误以及自动重试请求。有关 Amazon 开发工具包的信息（包括如何下载及安装），请参阅[适用于 Amazon Web Services 的工具](#)。

使用 Amazon 账户管理查询 API，您可以调用服务操作。查询 API 请求是必须包含参数 Action 以指示要执行的操作的 HTTPS 请求。Amazon 账户管理支持所有操作的 GET 和 POST 请求。也就是说，API 不要求您对某些操作使用 GET，而对其他一些操作使用 POST。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 [API 参考](#) 中的各个操作页面。

主题

- [端点](#)
- [必须使用 HTTPS](#)

- [签署 Amazon 账户管理 API 请求](#)

端点

Amazon 账户管理有一个在美国东部 (弗吉尼亚州北部) Amazon Web Services 区域 托管的全局 API 端点。

有关所有服务的 Amazon 端点和区域的更多信息，请参阅 Amazon Web Services 一般参考 中的 [区域和端点](#)。

必须使用 HTTPS

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

签署 Amazon 账户管理 API 请求

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

要对您的 API 请求进行签名，您必须使用 Amazon 签名版本 4。有关 Signature Version 4 的信息，请参阅《IAM 用户指南》中的 [签署 Amazon API 请求](#)。

有关更多信息，请参阅下列内容：

- [Amazon 安全凭证](#)：提供有关可用于访问 Amazon 的凭证类型的一般信息。
- [IAM 中的安全最佳实践](#)：提供有关使用 IAM 服务的建议，以帮助您保护您的 Amazon 资源，包括 Amazon 账户管理中的资源。
- [IAM 中的临时安全凭证](#)：说明如何创建和使用临时安全凭证。

Amazon Account Management 的配额

对于每项 Amazon 服务，您的 Amazon Web Services 账户都具有默认配额（以前称为限制）。除非另有说明，否则每个配额都针对的是特定的 Amazon Web Services 区域。

每个 Amazon Web Services 账户都具有以下与账户管理相关的配额：

资源	限额
每个目标账户的最大 StartPrimaryEmailUpdate 请求数	每 30 秒 3 个
一个 Amazon Web Services 账户 中的备用联系人	3 - BILLING、SECURITY 和 OPERATIONS 各一个
每个调用方账户的 AcceptPrimaryEmailUpdate 请求速率	每秒 1 个，突增到每秒 1 个
每个账户的 DeleteAlternateContact 请求速率	每秒 1 个，突增到每秒 6 个
每个账户的 GetAlternateContact 请求速率	每秒 3 个，突增到每秒 5 个
每个账户的 GetContactInformation 请求速率	每秒 3 个，突增到每秒 5 个
每个调用方账户的 GetPrimaryEmail 请求速率	每秒 3 个，突增到每秒 3 个
每个账户的 PutAlternateContact 请求速率	每秒 1 个，突增到每秒 6 个
每个账户的 PutContactInformation 请求速率	每秒 1 个，突增到每秒 2 个
每个调用方账户的 StartPrimaryEmailUpdate 请求速率	每秒 1 个，突增到每秒 1 个

管理印度地区的账户

如果您注册一个新的 Amazon Web Services 账户 并选择印度作为您的联系地址，则您将与 Amazon Web Services India Private Limited (Amazon India) (印度当地的一家 Amazon 销售商) 签订您的用户协议。AmazonIndia 管理您的账单，您的发票总额将以印度卢比 (而非美元 (USD)) 列出。创建 Amazon India 账户之后，无法更改联系信息中的国家/地区。有关管理 Amazon Web Services 账户 的信息，请参阅 [配置你的 Amazon Web Services 账户](#)。

如果您的账户是 Amazon India 账户，请执行本主题中的步骤来管理您的账户。本主题介绍如何注册 Amazon India 账户、编辑有关您的 Amazon India 账户的信息、管理客户验证以及添加或编辑您的永久账号 (PAN)。

在注册期间进行的信用卡验证过程中，Amazon India 将对您的信用卡收取 2 INR。AmazonIndia 将在验证完成后退回 2 INR。在验证过程中，您可能会重定向至您的银行。

主题

- [通过 Amazon 印度创建 Amazon Web Services 账户](#)
- [管理您的客户验证信息](#)

通过 Amazon 印度创建 Amazon Web Services 账户

Amazon India 是印度的一家当地 Amazon 销售商。如果您的联系地址在印度，而您想要创建账户，请使用以下步骤注册一个 Amazon India 账户。

注册 Amazon India 账户

1. 打开[亚马逊云科技主页](#)。
2. 选择创建 Amazon Web Services 账户。

Note


如果您最近登录过 Amazon，则此选项可能不存在。请改为选择登录控制台。如果创建新 Amazon Web Services 账户 选项仍不可见，请选择登录其他账户，然后选择创建新 Amazon Web Services 账户。

3. 输入您的账户信息，验证电子邮件地址，然后为账户选择一个强密码。
4. 选择企业或个人。个人账户和企业账户具有相同的特征和功能。

5. 输入您的公司或个人联系信息。如果您的联系地址或账单地址在印度，则根据《印度计算机应急团队》(CERT-IN) 的规定，Amazon 需要在授予您访问 Amazon 服务的权限之前收集和验证您的身份信息。

您从您的联系人或账单信息中选择的姓名必须与您计划用于客户验证的证件上显示的姓名一致。例如，如果计划使用公司注册证书验证企业账户，您必须提供证书上显示的公司名称。有关可接受的证件类型列表，请参阅 [the section called “接受的用于客户验证的印度证件”](#)。

6. 在您阅读客户协议后，请选中条款和条件复选框，然后选择继续。
7. 在账单信息页上，输入要使用的付款方式。您必须在验证过程中提供 CVV。
8. 在您有 PAN 吗？下，如果想在税务发票上显示永久账号 (PAN)，请选择是，然后输入您的 PAN。如果没有 PAN 或者想在注册后添加 PAN，请选择否。
9. 选择验证并继续。Amazon 在验证过程中，India 将对您的卡收取 2 INR。AmazonIndia 将在验证完成后退回 2 INR。
10. 在确认您的身份页面上，选择您注册账户的主要目的。
11. 选择最能代表账户所有者的所有权类型。如果您选择公司、组织或合作伙伴作为所有权类型，请输入主要管理人员的姓名。关键管理人员可以是董事、运营主管或负责公司运营的人。
12. 根据您选择的所有权类型，请选择一种可接受的印度证件类型进行验证，然后键入您的证件信息。

 Note

如果您拥有个人账户并计划使用非由印度联邦颁发的驾驶执照，我们建议使用不同的个人证件类型进行验证。

13. 选择要用于客户验证的姓名。

如果您的账单和联系信息中的姓名与印度地址相关联，则会显示这些姓名供您选择。确保您选择的姓名与计划用于客户验证的证件类型上的姓名一致。如果需要更改与您的账单或联系地址相关联的姓名，您可以在完成账户注册后进行更改。

14. 同意提交信息进行验证，然后选择继续。

完成账户注册后，您将收到有关客户验证结果的电子邮件通知。您还可以稍后在账户设置中的客户验证页面或 Amazon 运行状况控制面板中查看状态。您必须通过客户验证才能访问 Amazon 服务。

15. 选择是否要发短信 (SMS) 或拨打语音通话验证您的手机号码。
16. 选择您的国家或地区代码，然后输入您的手机号码。
17. 完成安全检查。

18. 选择发送短信或立即呼叫我。稍等片刻之后，您的手机将通过短信或自动通话收到四位数的 PIN 码。
19. 在确认您的身份页面上，输入您收到的 PIN，然后选择继续。
20. 在选择支持计划页面上，选择您的支持计划，然后选择完成注册。待您的付款方式和客户验证经过验证后，您的账户将被激活，您会收到一封确认激活账户的电子邮件。

Note

如果您完成了客户验证，并且编辑了之前用于验证身份的姓名、地址或证件，则可能需要再次更新并完成客户验证。有关更多信息，请参阅 [the section called “编辑您的客户验证信息”](#)。

管理您的客户验证信息

根据《印度计算机应急团队》(CERT-IN) 的规定，Amazon 需要在授予您首次或继续访问 Amazon 服务的权限之前收集和验证您的身份信息。您的身份必须使用您提供的印度账单或联系地址中的姓名进行验证。在验证过程中，Amazon 将检查证件编号是否有效，以及您提供的姓名是否与用户客户验证的证件关联的姓名相匹配。您从联系人或账单信息中选择的姓名必须与证件上显示的姓名完全一致。

要更新账单姓名和地址，请参阅 [付款偏好](#) 页面。要更新您的联系人姓名和地址，请参阅 [the section called “更新 Amazon Web Services 账户的主要联系人”](#)。如果编辑之前用于客户验证的任何信息，例如账单或联系信息中的姓名或印度地址，则可能需要更新并重新提交客户验证信息。

查看客户验证状态

您可以随时在客户验证页面上查看您的客户验证状态。如果验证状态为需要验证或验证失败，请编辑或更新您的客户验证信息并提交验证。

创建您的客户验证信息

要完成客户验证，您需要提供可接受的印度证件中的信息。有关可接受的证件类型列表，请参阅 [the section called “接受的用于客户验证的印度证件”](#)。

1. 登录到 [Amazon Web Services Management Console](#)。
2. 在右上角的导航栏中，选择账户名称（或别名），然后选择账户。
3. 在其他设置下，选择客户验证。

如果之前尚未提供客户验证信息，您会看到创建客户验证页面。

4. 选择与您计划用于客户验证的证件类型上的姓名完全一致的姓名。例如，如果计划使用公司注册证书验证企业账户，您必须提供证书上显示的公司名称。
5. 提供页面上要求的其余信息。根据选择的证件类型，您可能需要上传证件正面和背面的副本。如果上传了图像文件，请确保证件中的所有信息都清晰可见。
6. 选择提交。

您将通过电子邮件或在 Amazon 运行状况控制面板上接收客户验证结果和任何后续步骤的通知。

编辑您的客户验证信息

您可以编辑客户验证信息，例如您注册账户的主要目的、您的组织类型，以及您要用于验证的姓名、证件类型、证件上传或证件信息。

如果编辑用于客户验证的名称或证件类型，或者更新任何证件信息，则保存更改需要重新验证您的身份。

1. 登录到 [Amazon Web Services Management Console](#)。
2. 在右上角的导航栏中，选择账户名称（或别名），然后选择账户。
3. 在其他设置下，选择客户验证。
4. 选择编辑，然后更新要更改的信息。

更新信息时，请注意以下指南：

- 如果选择不同的姓名，则该姓名必须与您计划用于客户验证的证件上的姓名完全一致。例如，如果计划使用公司注册证书验证企业账户，您必须提供证书上显示的公司名称。
- 如果选择其他证件类型，您需要上传证件正面和背面（如果适用）的副本。证件上传中的所有信息都应清晰可见。
- 如果您拥有个人账户并计划使用非由印度联邦颁发的驾驶执照，我们建议使用不同的个人证件类型进行验证。

有关可接受的证件类型的列表，请参阅 [the section called “接受的用于客户验证的印度证件”](#)。

5. 选择提交。

如果由于保存的更改类型而必须再次验证您的身份，您将通过电子邮件接收客户验证结果和任何后续步骤的通知。您也可以返回客户验证页面或在 Amazon 运行状况控制面板中查看结果。

接受的用于客户验证的印度证件

接受印度政府签发的以下证件类型进行客户验证。

Note

政府可能会随时更改以下共享链接。

- PAN 卡 - 永久账号 (PAN) 卡有数字和实体卡两种格式，其中含有印度所得税部门向个人、公司和实体签发的唯一字母数字标识符。PAN 由十个字符组成，包括字母和数字，格式为 **AAAAA1111A**。要使用此证件进行验证，您还必须提供 PAN 证件上显示的出生日期（个人）或注册日期（企业），并上传卡片的正面。请访问[所得税部门的官方网站](#)，查看您的 PAN 的有效性。
- 选民身份证/EPIC - 选民身份证也称为选民带照片的身份证 (EPIC)，其中包含印度选举委员会向印度符合条件的选民签发的唯一识别码。选民 ID/EPIC 号码由 10 个字符组成，包括字母和数字。请访问[印度选举委员会](#)的官方网站，检查您的选民 ID 的有效性。要使用此证件进行验证，您必须上传卡片的正面和背面。
- 驾驶执照 - 如果您的驾驶执照不是由印度联邦颁发的，我们建议使用其他证件类型进行验证。驾驶执照号码由 12-16 个字符组成，包括字母、数字、空格和连字符。要使用此证件进行验证，您必须提供出生日期并上传卡片的正面和背面。您可以访问道路运输和公路部的 [Parivahan Sewa 网站](#)，检查您驾驶执照的有效性。
- 护照 - 印度护照是印度公民身份的证明，可用作国际旅行的身份证明。在由 Passport Seva Kendra (PSK) 签发的护照中，护照文档号是与个人护照相关联的唯一字母数字标识符。护照档案号由 15 个字符组成，包括字母和数字。与护照号码不同，护照档案号可以在您的印度护照的最后一页中找到。要使用此证件进行验证，您必须提供出生日期，并上传护照的第一页和最后一页（含有护照档案号）。您可以前往印度外交部的 [Passport Seva Kendra](#) 网站检查您的护照档案号是否有效。

Note

对于客户验证，只接受在印度签发的印度护照上的护照档案号。如果您的印度护照是在其他国家/地区签发的，则必须使用不同的印度证件进行客户验证。

- 公司注册证书 - 公司注册证书是由印度公司事务部 (MCA) 签发的证件，上面注明了企业注册为法人实体的日期。证书用于唯一标识和跟踪在印度注册的公司。每份证书都包含公司识别号 (CIN)，这是一个由 21 个字符（包括字母和数字）组成的唯一字母数字标识符。要使用此证件进行验证，您必须上传公司注册证书证件。您可以前往[印度公司事务部门门户网站](#)检查您的 CIN 是否有效。

个人和企业账户接受的印度证件类型不同：

- 适用于个人账户 - PAN 卡、选民身份证/EPIC、驾驶执照和护照。
- 适用于企业账户 - PAN 卡和公司注册证书。

管理您的 Amazon India 账户

除以下任务外，管理账户的程序与在印度境外创建的账户一致。有关管理账户的一般信息，请参阅 [配置您的账户](#)。

使用 Amazon Web Services Management Console 执行以下任务：

- [添加或编辑永久账号](#)
- [编辑多个永久账号](#)
- [the section called “管理您的客户验证信息”](#)
- [编辑多个商品和服务税识别号 \(GST\)](#)
- [查看税务发票](#)

《账户管理用户指南》的文档历史记录

下表描述了 Amazon 账户管理的文档版本。

变更	说明	日期
终止对编辑安全质疑问题的支持	由于支持已终止，因此已从指南中删除了“编辑您的安全挑战问题”主题。	2025年1月6日
重写“关闭账户”主题	全面修改了整个关闭账户主题，包括添加了如何关闭成员和管理账户的步骤。	2024 年 2 月 1 日
不再支持添加新的安全问题	添加了新内容，表示添加安全问题的选项已从账户页面中移除。	2024 年 1 月 5 日
不再支持 <code>aws-portal</code> 命名空间	Amazon Identity and Access Management (IAM) 之前用于管理您的账户的操作（例如 <code>aws-portal:ModifyAccount</code> 和 <code>aws-portal:ViewAccount</code> ）已终止标准支持。	2024 年 1 月 1 日
重写“区域”主题	全面修改了整个区域主题，包括添加了展开和折叠控件。	2023 年 10 月 8 日
已将 root 用户主题重新定位到《IAM用户指南》	将关于 root 用户的讨论整合到一个主题中，添加了移至《用户指南》的 root 用户主题的 IAM 交叉引用链接。	2023 年 9 月 18 日
主账户联系人主题中添加了新的部分	添加了新的电话号码和电子邮件地址要求部分。	2023 年 9 月 12 日

新的联系信息 APIs	对新的 Support GetContactInformation 和 PutContactInformation APIs.	2022 年 7 月 22 日
Amazon 账户管理现在支持通过 Amazon Organizations 控制台更新备用联系人。	现在，您可以使用更新的 Amazon Organizations 托管政策提供的账户API权限，通过 Amazon Organizations 控制台更新组织的备用联系人。	2022 年 2 月 22 日
初始版本	《Amazon 账户管理参考指南》的首次发布	2021 年 9 月 30 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。