



参考指南

# AWS 账户管理



# AWS 账户管理: 参考指南

Copyright © 2026 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。

# Table of Contents

什么是 AWS 账户？ .....	1
的特点 AWS 账户 .....	2
你是首次 AWS 使用吗？ .....	3
相关 AWS 服务 .....	3
使用根用户 .....	4
支持和反馈 .....	4
其他 AWS 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 .....	9
相关主题 .....	9
访问您的 账户 .....	9
规划您的 治理结构 .....	11
使用多个 AWS 账户的好处 .....	11
管理多个 AWS 账户 .....	12
何时使用 AWS Organizations .....	12
启用信任访问权限 .....	13
启用委托管理员账户 .....	14
使用限制访问权限 SCPs .....	16
何时使用 AWS Control Tower .....	17
了解 API 的操作模式 .....	18
授予更新账户属性的权限 .....	18
配置您的账户 .....	21
创建或更新您的账户别名 .....	21
AWS 区域 在您的账户中启用或禁用 .....	21
区域可用性参考 .....	23
启用和禁用区域之前的注意事项 .....	26
处理时间和请求限制 .....	26
为独立账户启用或禁用区域 .....	27
在组织中启用或禁用区域 .....	29
更新您的账单 AWS 账户 .....	31
更新根用户电子邮件 .....	31

为独立 AWS 账户更新根用户电子邮件 .....	32
为组织中的任何 AWS 账户 更新根用户电子邮件 .....	33
更新根用户密码 .....	35
更新你的 AWS 账户 名字 .....	36
更新独立版的账户名 AWS 账户 .....	37
为您组织内的任何 AWS 账户 更新账户名 .....	38
更新您的备用联系人 AWS 账户 .....	40
电话号码和电子邮件地址要求 .....	40
更新独立版的备用联系人 AWS 账户 .....	41
更新组织中任何 AWS 账户 成员的备用联系人 .....	44
账户 : AlternateContactTypes上下文密钥 .....	47
更新 AWS 账户的主要联系人 .....	47
电话号码和电子邮件地址要求 .....	48
更新独立账户 AWS 账户 或管理账户的主要联系人 .....	48
更新组织中任何 AWS 成员账户的主要联系人 .....	51
查看账户标识符 .....	53
找到你的 AWS 账户 身份证 .....	54
查找 AWS 账户的规范用户 ID .....	56
保护您的账户 .....	59
数据保护 .....	59
AWS PrivateLink .....	60
创建端点 .....	60
Amazon VPC 端点策略 .....	61
端点策略 .....	61
身份和访问管理 .....	62
受众 .....	62
使用身份进行身份验证 .....	62
使用策略管理访问 .....	64
AWS 账户管理和 IAM .....	65
基于身份的策略示例 .....	72
使用基于身份的策略 .....	74
问题排查 .....	76
AWS 托管策略 .....	78
AWSAccountManagementReadOnlyAccess .....	78
AWSAccountManagementFullAccess .....	79
策略更新 .....	80

合规性验证 .....	81
恢复能力 .....	81
基础结构安全性 .....	82
监控您的账户 .....	83
CloudTrail 日志 .....	83
中的账户管理信息 CloudTrail .....	83
了解账户管理日志条目 .....	84
使用监控账户管理事件 EventBridge .....	88
账户管理事件 .....	88
排查账户故障 .....	90
账户创建问题 .....	90
账户关闭问题 .....	91
我不知道如何删除或取消我的账户 .....	91
我在“账户”页面上看不到“关闭账户”按钮 .....	91
我关闭了账户，但仍未收到确认电子邮件 .....	91
我在尝试关闭账户时收到 ConstraintViolationException “” 错误 .....	92
我在尝试关闭成员账户时收到一条“CLOSE_ACCOUT_QUOTA_UCKEDED”错误 .....	92
在关闭管理账户之前，我需要删除我的 AWS 组织吗？ .....	92
其它问题 .....	92
我需要更换我的信用卡 AWS 账户 .....	92
我需要举报欺诈 AWS 账户 活动 .....	92
我需要关闭我的 AWS 账户 .....	93
关闭您的账户 .....	94
关闭账户前的注意事项 .....	94
如何关闭您的账户 .....	95
账户关闭后会发生什么 .....	98
后关闭期 .....	98
重新打开你的 AWS 账户 .....	98
API 参考 .....	100
操作 .....	101
AcceptPrimaryEmailUpdate .....	103
DeleteAlternateContact .....	108
DisableRegion .....	113
EnableRegion .....	117
GetAccountInformation .....	121
GetAlternateContact .....	127

GetContactInformation .....	133
GetGovCloudAccountInformation .....	137
GetPrimaryEmail .....	143
GetRegionOptStatus .....	147
ListRegions .....	151
PutAccountName .....	156
PutAlternateContact .....	161
PutContactInformation .....	167
StartPrimaryEmailUpdate .....	171
相关操作 .....	174
CreateAccount .....	175
CreateGovCloudAccount .....	175
DescribeAccount .....	175
数据类型 .....	175
AlternateContact .....	176
ContactInformation .....	178
Region .....	182
ValidationExceptionField .....	183
常见参数 .....	183
常见错误 .....	185
发出 HTTP 查询请求 .....	187
端点 .....	188
必须使用 HTTPS .....	188
签署 AWS 账户管理 API 请求 .....	188
配额 .....	189
管理印度地区的账户 .....	191
AWS 账户与 AWS 印度一起创作 .....	191
管理您的客户验证信息 .....	193
查看客户验证状态 .....	193
创建您的客户验证信息 .....	193
编辑您的客户验证信息 .....	194
接受的用于客户验证的印度证件 .....	195
管理您的 AWS 印度账户 .....	195
文档历史记录 .....	197
.....	cxcix

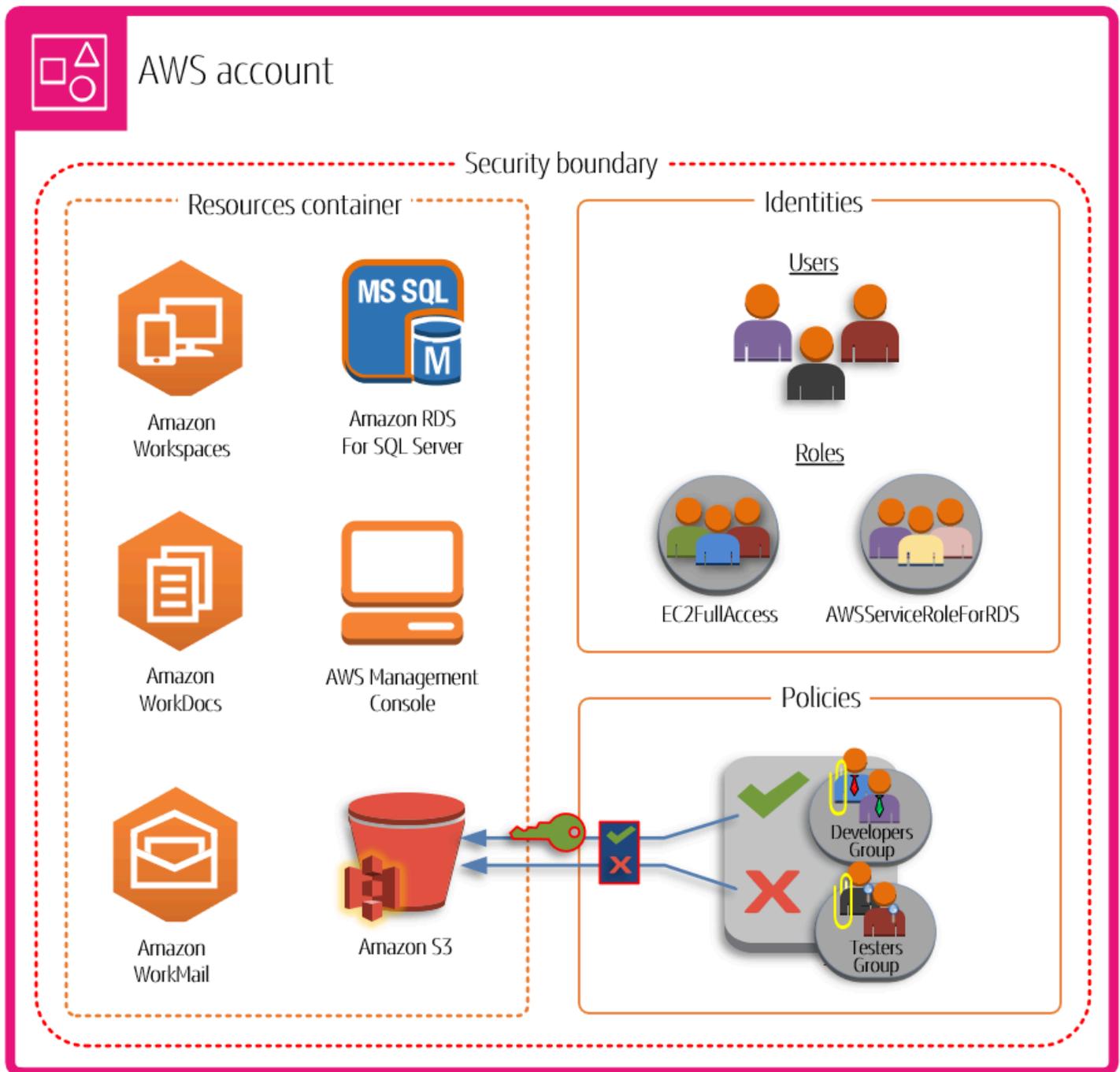
# 什么是 AWS 账户？

AWS 账户 代表您与之建立的正式业务关系 AWS。您可以在中创建和管理您的 AWS 资源 AWS 账户，您的账户提供访问和计费的身份管理功能。每个都 AWS 账户 有一个唯一的 ID，可以将其与其他 AWS 账户人区分开来。

您的云资源和数据包含在 AWS 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。

AWS 账户 也是访问 AWS 服务的基本组成部分。如下图所示，具有 AWS 账户 两个主要功能：

- **资源容器** — AWS 账户 是您作为 AWS 客户创建的所有 AWS 资源的基本容器。例如，亚马逊简单存储服务 (Amazon S3) 存储桶、亚马逊关系数据库服务 (Amazon RDS) 数据库和亚马逊弹性计算云 (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** — AWS 账户 也是您 AWS 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 AWS (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 AWS 账户 是扩展环境的最佳实践，因为它可以为成本提供自然的计费边界，隔离安全资源，为个人和团队提供灵活性，此外还可以适应新的业务流程。有关更多信息，请参阅 [使用多个 AWS 账户的好处](#)。

## 的特点 AWS 账户

AWS 账户 包括以下核心功能：

- **监控和控制成本**-账户是分配 AWS 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。除了账户级别的成本报告外，AWS 还提供内置支持，如果您选择在某个 AWS Organizations 时候使用，可以整合和报告整个账户集的成本。您还可以使用 AWS 服务配额来帮助防止意外的过度配置 AWS 资源和恶意行为，这些可能会严重影响您的 AWS 成本。
- **隔离单元** — 可以为您的 AWS 资源 AWS 账户 提供安全性、访问权限和计费边界，从而帮助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在逻辑上都与其他账户中配置的资源隔离，即使在您自己的 AWS 环境中也是如此。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。

## 你是首次 AWS 使用吗？

如果您是首次使用 AWS，则第一步是注册。AWS 账户注册时，使用您提供的详细信息 AWS 创建一个帐户，并将该帐户分配给您。创建后 AWS 账户，以 root 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 step-by-step 说明，请参阅[开始使用 AWS 账户](#)。

## 相关 AWS 服务

AWS 账户 与以下服务无缝协作：

- IAM

您的 AWS 账户 与 AWS 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。您还可以使用 IAM 来控制对所有 AWS 资源的访问权限，而不仅仅是账户的特定信息。在您着手设置 AWS 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。

- AWS Organizations

如果您的公司规模庞大或可能增长，则可能需要设置多个反映公司特定结构的 AWS 账户。AWS Organizations 提供底层基础设施和功能，供您构建和管理多账户环境。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 AWS Organizations](#)。

- AWS Control Tower

AWS Control Tower 提供了一种设置和管理安全的多账户 AWS 环境的简化方法。AWS Control Tower 使用实例化一组初始账户以及一些 AWS Organizations 针对该环境的默认防护栏和配置，自动创建您的多账户环境。只需几个步骤 AWS Control Tower 即可使用配置新 AWS 账户，同时确保账户符合您的组织政策。有关更多信息，请参阅 [何时使用 AWS Control Tower](#)。

## 使用 AWS 账户根用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务和资源。我们强烈建议不要使用根用户进行日常任务。有关要求根用户凭证的任务，请参阅《IAM 用户指南》中的 [需要根用户凭证的任务](#)。

要避免使用根用户处理日常任务，请了解 [如何在 AWS IAM Identity Center 中设置管理用户](#)。有关其他根用户安全建议，请参阅 [您的 AWS 账户的根用户最佳实践](#)。

### Important

任何 AWS 账户 拥有您的根用户凭证的人都可以不受限制地访问您账户中的所有资源，包括账单信息。

您可以 [更改或重置 root 用户密码](#)，以及 [创建或删除 root 用户的访问密钥](#)（访问密钥 IDs 和私有访问密钥）。有关使用 root 用户登录的帮助，请参阅 [《AWS 管理控制台 登录用户指南》中的以 root 用户身份 AWS 登录](#)。

## Support 对 AWS 账户管理的支持

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

如果您找不到想要的答案 AWS re:Post，则可以使用创建与账户或账单相关的支持案例 AWS 管理控制台。有关更多信息，请参阅[示例：创建账户和账单支持工单](#)。

## 其他 AWS 资源

- [AWS 培训和课程](#) — 指向基于角色的课程和专业课程以及自定进度的实验室的链接，可帮助您提高 AWS 技能并获得实践经验。
- [AWS 开发者工具](#) — 指向开发者工具和资源的链接，这些工具和资源提供文档、代码示例、发行说明和其他信息，可帮助您构建创新应用程序 AWS。
- [AWS 支持中心](#) — 用于创建和管理 Support AWS 案例的中心。还包括指向其他有用资源的链接，例如论坛、技术 FAQs、服务运行状况和 T AWS rusted Advisor。
- [AWS Support](#) — AWS 提供有关 Support 信息的主要网页 [one-on-one](#)，这是一个快速响应的支持渠道，可帮助您在云中构建和运行应用程序。
- [联系我们](#) — 查询 AWS 账单、账户、事件、滥用行为和其他问题的中央联络点。
- [AWS 网站条款](#) — 有关我们的版权和商标、您的帐户、许可证和网站访问权限以及其他主题的详细信息。

# 开始使用 AWS 账户

如果您不熟悉 AWS，第一步是注册 AWS 账户。当您这样做时，AWS 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学习和设置新的 AWS 账户。

## 主题

- [创建新 AWS 账户的先决条件](#)
- [创建一个 AWS 账户](#)
- [为您的根用户激活 MFA](#)
- [创建管理员用户](#)
- [访问你的 AWS 账户](#)

## 创建新 AWS 账户的先决条件

要注册 AWS 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。
- AWS 账户名 — 账户名称显示在多个位置，例如发票上，以及控制台（例如 Billing and Cost Management 控制面板和 AWS Organizations 控制台）中。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，可以考虑使用命名标准，例如组织-目的-环境（例如，AnyCompany-审计-生产）。对于个人账户，可以考虑使用命名标准，例如名字-姓氏-用途（例如 paulo-santos-testaccount）。
- 地址 — 如果您的联系地址和账单地址在印度，则您的账户的用户协议是与印度本地 AWS 卖家 Amazon Web Services India 私人有限公司（AWS 印度）签订的。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。AWS 在验证过程中，印度会向您收取 2 印度卢比的付款方式。AWS 验证完成后，印度将退还 2 印度卢比。
- 电话号码 - 此号码用于身份验证及确认您的账户所有权。您必须能够通过此号码接收来电和短信。

**⚠ Important**

如果此账户是为企业开设的，请使用公司电话号码，这样 AWS 账户 即使员工变更职位或离开公司，您的公司也可以保留访问权限。

## 创建一个 AWS 账户

这些说明用于在印度 AWS 账户 境外创建。有关在印度创建账户的信息，请参阅[AWS 账户与 AWS 印度一起创作](#)。要创建属于由管理的组织的账户 AWS Organizations，请参阅《AWS Organizations 用户指南》中的[在组织中创建成员账户](#)。

### AWS 管理控制台

#### 要创建 AWS 账户

1. 打开[注册 AWS](#) 页面。
2. 输入 root 用户的电子邮件地址和 AWS 账户 姓名，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**

如果此帐户适用于企业，请使用安全的公司通讯组列表（例如 `it.admins@example.com`），这样 AWS 账户 即使员工变更职位或离开公司，您的公司也可以保留访问该列表的权限。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。

3. 输入您的验证码，然后选择验证。
4. 为 root 用户输入一个强密码，进行确认，然后选择“继续”。AWS 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。
  - 它不得与您的 AWS 账户 姓名或电子邮件地址相同。
5. 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。

## 6. 输入您的公司或个人信息。

### Important

对于企业而言 AWS 账户，最佳做法是输入公司电话号码，而不是个人电话号码。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。

7. 阅读并接受 [AWS 客户协议](#)。请务必阅读并理解 AWS 客户协议的条款。
8. 选择继续。此时，您将收到一封电子邮件，确认您的设备 AWS 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，在完成激活帐户之前，您无法使用任何 AWS 服务。
9. 输入有关付款方式的信息，然后选择验证并继续。如果您想使用不同的账单地址作为账 AWS 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。

10. 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。
11. 输入验证码中显示的代码，然后提交。
12. 当自动系统与您联系时，请输入收到的 PIN，然后提交。
13. 选择一个可用 AWS 支持计划。有关可用支持计划的描述，请参阅[比较支持计划](#)。
14. 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。
15. 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。
16. 收到激活消息后，您可以登录[AWS 管理控制台](#)开始使用 AWS 服务。有关如何管理账户设置的一般信息，请参阅[配置你的 AWS 账户](#)。

## AWS CLI & SDKs

您可以在组织中创建成员帐户，该组织 AWS Organizations 通过在登录组织的管理账户时运行 [CreateAccount](#) 操作进行管理。

您不能使用 AWS Command Line Interface (AWS CLI) 或 AWS API 操作在组织 AWS 账户 之外创建独立服务器。

## 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未经授权的情况下访问您账户的风险。

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。[AWS 管理控制台](#)在下一页上，输入您的密码。

有关使用 root 用户登录的帮助，请参阅 [《AWS 管理控制台 登录用户指南》](#) 中的 [以 root 用户身份 AWS 登录](#)。

2. 为根用户启用 MFA。

有关说明，请参阅 [IAM 用户指南中的为 AWS 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 身份中心用户指南中的为 IAM 身份中心管理员用户设置 AWS 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](#)。

## 访问你的 AWS 账户

您可以通过以下任何一种 AWS 账户 方式访问您的：

### AWS 管理控制台

[AWS 管理控制台是一个基于浏览器的界面，可用于管理您的 AWS 账户 设置和资源。](#) AWS

## AWS 命令行工具

使用 AWS 命令行工具，您可以在系统的命令行中发出命令来执行 AWS 账户和执行 AWS 任务。与使用控制台相比，使用命令行处理更快、更方便。如果要生成执行 AWS 任务的脚本，命令行工具也很有用。AWS 提供了两组命令行工具：

- [AWS Command Line Interface\(AWS CLI\)](#)。有关安装和使用的信息 AWS CLI，请参阅《[AWS Command Line Interface 用户指南](#)》。
- [AWS Tools for Windows PowerShell](#)。有关安装和使用适用于 Windows 的工具的信息 PowerShell，请参阅《[AWS Tools for PowerShell 用户指南](#)》。

## AWS SDKs

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

## AWS 账户管理 HTTPS 查询 API

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

# 规划您的 AWS 账户 治理结构

尽管您可能从一个账户开始您的 AWS 旅程，但 AWS 建议您随着工作负载规模和复杂性的增加而设置多个帐户。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。

本节介绍可用的好处和治理服务 AWS ，以帮助实现多账户治理结构。

## 主题

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

## 使用多个 AWS 账户的好处

AWS 账户 构成了基础安全边界。AWS Cloud 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 AWS 账户？](#)。

将资源分成不同的资源 AWS 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，与审计师交谈并能够指向一个 AWS 账户 受 [支付卡行业 \(PCI\) 安全标准](#) 约束的工作负载的所有要素的审计员要容易得多。
- 隔离 — An AWS 账户 是安全保护的单位。应在 AWS 账户 不影响他人的情况下控制潜在的风险和安全威胁。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。您可以通过将团队移至分开 AWS 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。使用多个 AWS 账户 ，您可以支持业务部门的特定需求。

- 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一个付款人（使用 AWS Organizations 和整合账单），同时将各行项目分 AWS 账户开。
- 配额分配 — AWS 服务配额是分别为每个配额强制执行的 AWS 账户。将工作负载分成不同的 AWS 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 [AWS 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 AWS 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 [AWS Organizations](#)，这是一项免费 AWS 服务，用于管理组织 AWS 账户 中的所有内容。

AWS 还提供了 AWS Control Tower，它为 Organizations 增加了多层 AWS 托管自动化，并自动将其与其他 AWS 服务（如 AWS CloudTrail、AWS Config CloudWatch AWS Service Catalog、Amazon 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[AWS Control Tower 定价](#)。

另请参阅

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

## 何时使用 AWS Organizations

AWS Organizations 是一项可用于 AWS 账户 作为一个小组进行管理的 AWS 服务。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。有关的更多信息 AWS Organizations，请参阅《[AWS Organizations 用户指南](#)》。

可信访问权限

当您 AWS Organizations 使用群组管理账户时，组织的大多数管理任务只能由该组织的管理帐户执行。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 与该 AWS 服务之间的可信访问来将此附加功能扩展到其他服务。Trusted access to AWS services 向指定服务授予访问有关组织及其所含账户信息的权限。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[为 AWS 账户管理启用可信访问权限](#)。

## 委托管理员

启用可信访问权限后，您还可以选择将您的一个成员账户指定为账户管理的委托管理员 AWS 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 AWS 账户管理功能启用委托管理员账户](#)。

## 服务控制策略

如果您属于 AWS 账户 由管理的组织 AWS Organizations，则该组织的管理员可以应用[服务控制策略 \(SCPs\)](#)，[该策略](#)可以限制成员账户中的委托人可以执行的操作。SCP 从不授予权限；相反，它是一个限制成员账户可使用权限的过滤器。成员账户中的用户或角色（委托人）只能执行那些与适用于 SCPs 该账户的允许的操作和附加到委托人的 IAM 权限策略交叉的操作。例如，您可以使用 SCPs 防止账户中的任何委托人修改自己账户的备用联系人。

有关适用于 SCPs 的示例 AWS 账户，请参阅[使用 AWS Organizations 服务控制策略限制访问](#)。

## 为 AWS 账户管理启用可信访问权限

为 AWS 账户管理启用可信访问权限允许管理账户的管理员修改中每个成员账户的特定信息和元数据（例如，主要或备用联系方式）AWS Organizations。有关更多信息，请参阅《AWS Organizations 用户指南》中的[AWS 账户管理 AWS Organizations](#)。有关可信访问工作原理的一般信息，请参阅[与其他 AWS 服务 AWS Organizations 一起使用](#)。

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 AWS 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](#)。

## AWS 管理控制台

为 AWS 账户管理启用可信访问权限

1. 登录 [AWS Organizations 控制台](#)。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择AWS 账户管理。
4. 选择 Enable trusted access (启用可信访问)。
5. 在“为 AWS 账户管理启用可信访问”对话框中，键入 enable 进行确认，然后选择“启用可信访问”。

## AWS CLI & SDKs

为 AWS 账户管理启用可信访问权限

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。

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

以下示例为主叫账户的组织中的 AWS 账户管理启用可信访问权限。

```
$ 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 AWS 账户管理功能启用委托管理员账户

您可以启用委托管理员账户，以便可以在中为其他成员 AWS 账户调用账户管理 API 操作 AWS Organizations。为组织注册委托管理员账户后，该账户中的用户和角色可以通过支持可选 `AccountId` 参数在 `account` 命名空间中调用 AWS CLI 和 AWS SDK 操作，这些操作可以在组织模式下运行。

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。

## AWS 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
```

- AWS 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，您可以使用账户 123456789012 中的凭据调用账户管理 AWS 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。

## AWS 管理控制台

AWS 账户管理管理控制台不支持此任务。您只能通过使用其中一个中的 AWS CLI 或 API 操作来执行此任务 AWS SDKs。

## 使用 AWS Organizations 服务控制策略限制访问

本主题提供的示例说明了如何使用中的服务控制策略 (SCPs) AWS Organizations 来限制组织中账户中的用户和角色可以执行的操作。有关服务控制策略的更多信息，请参阅《AWS Organizations 用户指南》中的以下主题：

- [正在创建 SCPs](#)
- [附加 SCPs 到 OUs和账户](#)
- [的策略 SCPs](#)
- [SCP 策略语法](#)

Example 示例 1：阻止账户修改其备用联系人

以下示例拒绝任何成员账户在[独立账户模式](#)下调用 PutAlternateContact 和 DeleteAlternateContact API 操作。这可以防止受影响账户中的任何主体更改其备用联系人。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "account:PutAlternateContact",
        "account>DeleteAlternateContact"
      ],
      "Resource": [ "arn:aws:account::*:account" ]
    }
  ]
}
```

Example 示例 2：阻止任何成员账户修改组织中其他任何成员账户的备用联系人

以下示例以“\*”概括 Resource 元素，这意味着该元素同时适用于[独立模式请求](#)和[组织模式请求](#)。这意味着，即使是账户管理的委托管理员账户（如果 SCP 适用于此账户），也无法更改组织中任何账户的任何备用联系人。

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "account:PutAlternateContact",
        "account>DeleteAlternateContact"
      ],
      "Resource": [ "*" ]
    }
  ]
}
```

Example 示例 3：阻止 OU 中的成员账户修改其备用联系人

以下示例 SCP 包含一个条件，用于将账户的组织路径与两个 OUs 组织路径进行比较。这会导致禁止指定 OUs 账户中任何账户的委托人修改自己的备用联系人。

## 何时使用 AWS Control Tower

AWS Organizations 是一项基础服务，使您能够集中管理和保护整个 AWS 环境。这种以人 AWS Organizations 为中心的方法的一个关键组成部分是 AWS Control Tower。AWS Control Tower 充当 Organizations 中的管理控制台，通过应用规范性最佳实践，为设置和管理安全的多账户 AWS 环境提供了一种简化的方法。

提供的这种安全最佳实践方法 AWS Control Tower 扩展了的核心功能 AWS Organizations。AWS Control Tower 应用一套预防和侦查护栏，以帮助确保您的组织和账户与建议的安全和合规标准保持一致。

通过使用建立架构良好的 AWS Organizations 结构 AWS Control Tower，您可以快速部署可扩展、安全且合规 AWS 的环境。这种集中的云管理和治理方法对于希望在保持最高安全性和合规性标准的 AWS Cloud 同时充分利用云计算的力量至关重要。

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

## 了解 API 的操作模式

与的属性配合使用 AWS 账户的 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。如果您在调用账户管理 AWS CLI 或 AWS SDK 操作时不包含该 `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。当您调用账户管理 AWS CLI 或 AWS SDK 操作时，如果确实包含了该 `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。

AWS CLI 和 S AWS DK 操作既可以在独立环境中运行，也可以在组织环境中运行。

- 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 AWS 操作一样，您可以使用 [IAM 权限策略授予添加、更新或删除账户属性的权限](#)。AWS 账户在向 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。

## 的 Amazon 资源名称格式 AWS 账户

- 根据您要引用的账户是独立账户还是组织中的账户，您可以包含在政策声明 resource 元素中的 [亚马逊资源名称 \(ARN\)](#) 的结构会有所不同。AWS 账户 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。以下示例片段将该政策限制为仅适用于两个指定账户中的任意一个。OUs

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。另外，请注意，条件键的前缀是 `account`，即使您引用的是组织 OUs 中的路径。

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

## account:AccountResourceOrgTags

上下文键 `account:AccountResourceOrgTags` 允许您引用可以附加到组织账户的标签。标签是一对 `key/value` 字符串，可用于对账户中的资源进行分类和标签。有关更多信息，请参阅《AWS 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 AWS 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:AccountResourceOrgTags` 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:AccountResourceOrgTags/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版 AWS 账户。

# 配置你的 AWS 账户

本节包含的主题描述了如何管理您的 AWS 账户。

## Note

如果您 AWS 账户是在印度使用亚马逊 Web Services 印度私人有限公司 (AWS 印度) 创建的，则还有其他注意事项。有关更多信息，请参阅 [管理印度地区的账户](#)。

## 主题

- [创建 AWS 账户 别名](#)
- [AWS 区域 在您的账户中启用或禁用](#)
- [更新您的账单 AWS 账户](#)
- [更新根用户电子邮件地址](#)
- [更新根用户密码](#)
- [更新你的 AWS 账户 名字](#)
- [更新您的备用联系人 AWS 账户](#)
- [更新 AWS 账户的主要联系人](#)
- [查看 AWS 账户 标识符](#)

## 创建 AWS 账户 别名

如果您希望 IAM 用户的 URL 包含您的公司名称 (或其他 easy-to-remember 标识符) 而不是 AWS 账户 ID，则可以创建账户别名。

要了解如何创建或更新账户别名，请参阅 IAM 用户指南中的 [使用别名作为您的 AWS 账户 ID](#)。

## AWS 区域 在您的账户中启用或禁用

AWS 区域是世界上 AWS 有多个可用区的物理位置。可用区由一个或多个离散 AWS 的数据中心组成，每个数据中心都具有冗余电源、网络和连接，位于不同的设施中。这意味着每个区域在物理上 AWS 区域 都是孤立的，并且独立于其他区域。区域提供容错能力、稳定性和弹性，还可以减少延迟。在离最终用户 AWS 区域 更近的地方运行工作负载可以提高性能并降低延迟。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](#)。要详细了解您的工作负载 AWS 区域的弹性架构，请访问 [AWS 多区域](#) 基础知识。

AWS 区域 账户可用性大致分为两类：

- 默认区域 - 2019 年 3 月 20 日之前推出的区域默认处于启用状态。账户激活后，您可立即在这些默认区域中创建和管理资源。无法启用或禁用默认区域。
- 选择加入区域 - 2019 年 3 月 20 日后推出的区域默认处于禁用状态，称为选择加入区域。禁用的选择加入区域不会显示在控制台导航栏中，在启用前无法使用这些区域创建工作负载。要使用这些可选区域，您必须先要在您的 AWS 账户区域中启用它们。启用选择加入区域后，您可以在导航栏中选择该区域，并在该区域内创建和管理资源。要为您的独立账户启用选择加入区域，请参阅 [为独立账户启用或禁用区域](#)，要为您的成员账户启用选择加入区域，请参阅 [在组织中启用或禁用区域](#)。

当您注册时 AWS 账户，会根据您的联系地址所在的国家/地区为您 AWS 推荐一个可选区域。拥有 AWS 选择加入区域的国家/地区的买家会在“联系信息”页面上看到一条建议，要求在该国家/地区启用选择加入区域。在同时设有选择加入区域和默认区域的国家/地区（如印度、澳大利亚或加拿大），若选择加入区域距离客户更近，则会显示选择加入区域的推荐提示。账户激活后，您可以在账户中启用其他 AWS 选择加入区域，也可以选择禁用在注册期间启用的选择加入区域。

创建时 AWS 账户，系统会自动将您的 IAM 数据和证书配置为适用于所有默认区域，从而允许具有适当权限的根用户和 IAM 身份使用其现有证书访问这些区域中的 AWS 服务。AWS 默认情况下，选择加入区域处于禁用状态，而且 IAM 数据和证书最初在这些区域不可用，这会阻止访问该区域中的 AWS 服务。当您选择启用选择加入区域时，AWS 会将您的 IAM 数据和凭证传播到该区域。传播完成并启用可选区域后，根用户和 IAM 身份即可使用他们在默认区域中使用的相同 IAM 凭证访问新启用的选择加入区域中的 AWS 服务。

当您禁用某个选择加入区域时，您的 IAM 凭证将失效，且您将失去对该区域内资源的 IAM 访问权限。禁用选择加入区域不会删除该区域内的资源，且被禁用的选择加入区域内的资源（如有）的费用仍按标准费率持续计费。

#### Important

禁用某个区域会禁用 IAM 对该区域资源的访问权限。这不会删除相关资源，这些资源会继续产生费用。在禁用区域之前，请移除所有剩余资源。

AWS 将区域分组为 [分区](#)。每个区域仅属于一个分区，而每个分区包含一个或多个区域。分区具有独立的 AWS Identity and Access Management (IAM) 实例，在不同分区中的区域之间提供了硬边界。

AWS 商业区域位于aws分区中，中国的区域位于分区aws-cn中 AWS GovCloud (US) ，区域位于分区aws-us-gov中。根据您创建的分区 AWS 账户，可以在该分区 AWS 区域 中使用。

- aws分区中的账户可让您访问商业分区中的多个区域，这样您就可以在满足您要求的位置启动 AWS 资源。例如，您可能希望在欧洲启动 Amazon EC2 实例，以便更接近欧洲客户或满足法律要求。
- aws-us-gov分区中的账户为您提供访问 AWS GovCloud（美国西部）地区和 AWS GovCloud（美国东部）地区的权限。有关更多信息，请参阅 [AWS GovCloud \(US\)](#)。
- aws-cn 分区中的账户只能让您访问北京和宁夏区域。有关更多信息，请参阅 [中国的 Amazon Web Services](#)。

## 主题

- [区域可用性参考](#)
- [启用和禁用区域之前的注意事项](#)
- [处理时间和请求限制](#)
- [为独立账户启用或禁用区域](#)
- [在组织中启用或禁用区域](#)

## 区域可用性参考

下表 AWS 区域 按可用性类型列出。默认区域会自动启用且无法禁用，而选择性加入域必须手动启用后才能使用：

### Opt-in Regions

以下区域为选择加入区域，必须先启用才能使用：

Name	代码	Status
非洲（开普敦）	af-south-1	GA
亚太地区（香港）	ap-east-1	GA
亚太地区（台北）	ap-east-2	GA
亚太地区（海得拉巴）	ap-south-2	GA
亚太地区（雅加达）	ap-southeast-3	GA

Name	代码	Status
亚太地区 ( 墨尔本 )	ap-southeast-4	GA
亚太地区 ( 马来西亚 )	ap-southeast-5	GA
亚太地区 ( 新西兰 )	ap-southeast-6	GA
亚太地区 ( 泰国 )	ap-southeast-7	GA
加拿大西部 ( 卡尔加里 )	ca-west-1	GA
欧洲 ( 苏黎世 )	eu-central-2	GA
欧洲地区 ( 米兰 )	eu-south-1	GA
欧洲 ( 西班牙 )	eu-south-2	GA
以色列 ( 特拉维夫 )	il-central-1	GA
中东 ( 阿联酋 ) :	me-central-1	GA
中东 ( 巴林 )	me-south-1	GA
墨西哥 ( 中部 )	mx-central-1	GA

## Default Regions

以下区域默认启用且不可禁用：

Name	代码
亚太地区 ( 东京 )	ap-northeast-1
亚太地区 ( 首尔 )	ap-northeast-2
亚太地区 ( 大阪 )	ap-northeast-3
亚太地区 ( 孟买 )	ap-south-1

Name	代码
亚太地区 ( 新加坡 )	ap-southeast-1
亚太地区 ( 悉尼 )	ap-southeast-2
加拿大 ( 中部 )	ca-central-1
欧洲地区 ( 法兰克福 )	eu-central-1
欧洲地区 ( 斯德哥尔摩 )	eu-north-1
欧洲地区 ( 爱尔兰 )	eu-west-1
欧洲地区 ( 伦敦 )	eu-west-2
欧洲 ( 巴黎 )	eu-west-3
南美洲 ( 圣保罗 )	sa-east-1
美国东部 ( 弗吉尼亚州北部 )	us-east-1
美国东部 ( 俄亥俄州 )	us-east-2
美国西部 ( 北加利福尼亚 )	us-west-1
美国西部 ( 俄勒冈州 )	us-west-2

有关区域名称及其相应代码的列表，请参阅《AWS 一般参考指南》中的[区域端点](#)。有关每个区域 ( 不含终端节点 ) 支持的 AWS 服务列表，请参阅[AWS 区域服务列表](#)。

#### Important

AWS 建议您使用区域 AWS Security Token Service (AWS STS) 终端节点而不是全球终端节点来减少延迟。来自区域 AWS STS 终端节点的会话令牌在所有 AWS 区域都有效。如果您使用区域 AWS STS 终端节点，则无需进行任何更改。但是，来自全局 AWS STS 终端节点 (<https://sts.amazonaws.com>) 的会话令牌仅在 AWS 区域 您启用或默认启用的情况下才有效。如果您打算为账户启用新的区域，则可以使用来自区域 AWS STS 终端节点的会话令牌，也可以激活全球 AWS STS 终端节点来发放全部有效的会话令牌 AWS 区域。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 AWS STS 终端节点如何与 AWS 区域配合使用的更多信息，请参阅[AWS STS 在 AWS 区域中管理](#)。

## 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：

- 无论区域@@ 选择状态如何，您都可以使用跨区域推理地理位置中的所有目标区域 — 某些 AWS 生成式 AI 服务，包括 Amazon Bedrock ( 参见[通过跨区域推理提高吞吐量](#) ) 和 Amazon Q Developer ( 参见 [Amazon Q Developer 中的跨区域处理](#) ) 使用[跨区域推理](#)。如果您使用这些服务，它们会自动在您选定的地理区域内选择最优 AWS 区域——包括您尚未为资源和 IAM 数据启用的区域。这会最大限度地提高计算资源和模型的可用性，进而改善客户体验。
- 您可以使用 IAM 权限来控制对区域的访问权限 — AWS Identity and Access Management (IAM) 包括四种权限，允许您控制哪些用户可以启用、禁用、获取和列出区域。有关更多信息，请参阅《IAM 用户指南》中的 [AWS：允许启用和禁用 AWS 区域](#)。您也可以使用[aws:RequestedRegion](#)条件键来控制对 AWS 服务 中的访问权限 AWS 区域。
- 启用和禁用区域是免费的 - 启用或禁用区域均不收取任何费用。您只需为在新区域中创建的资源付费。
- Amazon EventBridge 集成 — 您可以在中订阅区域选项状态更新通知。EventBridge EventBridge 系统将为每次状态更改创建通知，允许客户自动执行工作流程。
- Expressive Region-Opt 状态 — 由于选择加入区域的 enabling/disabling 异步性质，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。AWS 尽管状态为，但有些 AWS 服务可能无法立即使用ENABLED。

## 处理时间和请求限制

启用或禁用区域时，请注意以下时间限制和请求限制：

- 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，AWS 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。
- 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。
- 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。
- Organizations 可以在给定时间在整个 AWS 组织中打开 50 个区域选择请求 — 管理账户在任何时候都可能有 50 个待处理的请求等待其组织完成。一个请求等于为一个账户启用或禁用一个特定区域。

## 为独立账户启用或禁用区域

要更新您 AWS 账户 有权访问的区域，请执行以下过程中的步骤。以下 AWS 管理控制台 过程始终仅在独立环境中起作用。您只能使用 AWS 管理控制台 查看或更新用于调用该操作的账户中的可用区域。

### AWS 管理控制台

#### 为独立版启用或禁用区域 AWS 账户

##### 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` ( 需要查看列表 AWS 区域 以及它们当前处于启用还是禁用状态 )。
- `account:EnableRegion`
- `account:DisableRegion`

1. 以 AWS 账户根用户 或的 [AWS 管理控制台](#) 身份登录，以具有最低权限的 IAM 用户或角色的身份登录。
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 AWS 区域 部分。
4. 选择要启用或禁用的区域，然后选择所需操作：启用或禁用。您将看到确认提示。

5. 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。

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。

启用选择加入区域后，您可以从区域导航栏中选择该区域。有关选择区域的步骤，请参阅[从 AWS 管理控制台的导航栏中选择区域](#)；有关账户中特定区域的控制台设置，请参阅[在 AWS 管理控制台中设置默认区域](#)。

## AWS CLI & SDKs

您可以使用以下 AWS CLI 命令或其 AWS 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

要更新您的成员账户的启用区域 AWS Organizations，请执行以下过程中的步骤。

### Note

#### AWS Organizations 托管策略

策略 `AWSOrganizationsReadOnlyAccess` 或 `AWSOrganizationsFullAccess` 已更新，提供访问 AWS 账户管理的权限，APIs 以便您可以从 AWS Organizations 控制台访问账户数据。要查看更新的托管策略，请参阅 [Organizations AWS 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以之前，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](#)。
- 为 AWS 账户管理服务启用可信访问权限。要进行设置，请参阅 [为 AWS 账户管理启用可信访问权限](#)。

## AWS 管理控制台

### 在组织中启用或禁用区域

1. 使用贵组织的管理账户凭据登录 AWS Organizations 控制台。

2. 在 AWS 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”。

## AWS CLI & SDKs

您可以使用以下 AWS CLI 命令或其 AWS SDK 等效操作启用、禁用、读取和列出组织成员账户的区域选择状态：

- `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"
}
```

## 更新您的账单 AWS 账户

您可以使用 AWS Billing 和成本管理控制台更新所有 AWS 账户 账单偏好。要了解如何更新账户的账单相关设置，请参阅 [《AWS 账单与成本管理 用户指南》](#)：

## 更新根用户电子邮件地址

出于各种业务原因，您可能需要更新您 AWS 账户的根用户电子邮件地址。例如，出于安全性和管理弹性考虑。本主题将引导您完成更新独立账户和成员账户的根用户电子邮件地址的过程。

#### Note

对的更改 AWS 账户 最多可能需要四个小时才能传播到任何地方。

您可以根据账户是独立账户还是组织账户的不同，分别更新根用户电子邮件：

- 独立 AWS 账户 — 对于与组织 AWS 账户 无关的用户，您可以使用 AWS 管理控制台更新根用户电子邮件。要了解如何执行此操作，请参阅 [为独立 AWS 账户更新根用户电子邮件](#)。

- AWS 账户 组织@@ 内部 — 对于属于组织的成员账户，管理账户或委托管理员账户中的用户可以从 AWS Organizations 控制台集中更新成员账户的根用户电子邮件，也可以通过 AWS CLI & SDKs 以编程方式更新该成员账户的 Amazon Web Services 电子邮件。AWS 要了解如何执行此操作，请参阅[更新组织中任何成员的根用户电子邮件](#)。

## 主题

- [为独立 AWS 账户更新根用户电子邮件](#)
- [为组织中的任何 AWS 账户更新根用户电子邮件](#)

## 为独立 AWS 账户更新根用户电子邮件

要编辑独立版的根用户电子邮件地址 AWS 账户，请执行以下过程中的步骤。

### AWS 管理控制台

#### Note

您必须以身份登录 AWS 账户根用户，这不需要其他 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 AWS 账户电子邮件地址和密码以您的[AWS 管理控制台](#)身份登录 AWS 账户根用户。
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](#)，点击账户详情旁边的操作按钮，然后选择更新电子邮件地址和密码。
4. 在账户详情页面，点击电子邮件地址旁边的编辑按钮。
5. 在编辑账户电子邮件页面，填写新电子邮件地址和确认新电子邮件地址字段，并确认您当前的密码。然后，选择保存并继续。no-reply@verify.signin.aws 将向新的电子邮件地址发送验证码。
6. 在编辑账户电子邮件页面，于验证码栏输入您通过电子邮件收到的验证码，然后选择确认更新。

#### 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。

## AWS CLI & SDKs

AWS CLI 或其中一个 API 操作不支持此任务 AWS SDKs。只有使用才能执行此任务 AWS 管理控制台。

## 为组织中的任何 AWS 账户 更新根用户电子邮件

要使用 AWS Organizations 控制台编辑组织中任何成员账户的根用户电子邮件地址，请执行以下过程中的步骤。

### Note

在更新成员账户的根用户电子邮件地址之前，我们建议您了解此操作的影响。有关更多信息，请参阅《AWS Organizations 用户指南》中的[通过 AWS Organizations 为成员账户更新根用户电子邮件地址](#)。

以根用户身份登录 AWS 管理控制台 后，您也可以直接从账户[页面](#)更新成员账户的根用户电子邮件地址。有关 step-by-step 说明，请按照中提供的步骤操作[为独立 AWS 账户更新根用户电子邮件](#)。

## AWS Management Console

### 注意

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

要通过 AWS Organizations 控制台来更新成员账户的根用户电子邮件地址

1. 登录 [AWS Organizations 控制台](#)。您必须以 IAM 用户身份登录，或在组织的管理账户中以根用户身份登录（[不推荐](#)）。
2. 在 AWS 账户 页面上，选择要为其更新根用户电子邮件地址的成员账户。
3. 在账户详细信息部分中选择操作按钮，然后选择更新电子邮件地址。
4. 在电子邮件下，输入根用户的新电子邮件地址，然后选择保存。此操作将向新的电子邮件地址发送一次性密码（OTP）。

**Note**

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

5. 在验证码下，输入在上一步中发送到新电子邮件地址的验证码，然后选择确认。此操作将更新该账户的根用户。

## AWS CLI & SDKs

您可以使用以下 AWS CLI 命令或其 AWS SDK 等效操作来检索或更新根用户的电子邮件地址（也称为主电子邮件地址）：

- [GetPrimaryEmail](#)
- [StartPrimaryEmailUpdate](#)
- [AcceptPrimaryEmailUpdate](#)

**注意**

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

**最小权限**

对于各个操作，您必须具有映射到此操作的权限：

- `account:GetPrimaryEmail`
- `account:StartPrimaryEmailUpdate`
- `account:AcceptPrimaryEmailUpdate`

如果使用这些单独权限，就可以向某些用户授予仅读取根用户电子邮件地址信息的权限，而向其他用户同时授予读取和写入的权限。

要完成根用户电子邮件地址 流程，您必须按照以下示例中显示的顺序 APIs 一起使用主电子邮件。

### Example `GetPrimaryEmail`

以下示例将检索组织中指定成员账户的根用户电子邮件地址。所用凭证必须来自组织管理账户或账户管理委托管理员账户。

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

### Example `StartPrimaryEmailUpdate`

以下示例将启动根用户电子邮件地址更新过程，识别新的电子邮件地址，并向组织中指定成员账户的新电子邮件地址发送一次性密码 (OTP)。所用凭证必须来自组织的管理账户或账户管理服务的委派管理员账户。

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

### Example `AcceptPrimaryEmailUpdate`

以下示例会接受 OTP 代码并将该新电子邮件地址设置到组织中的指定成员账户。所用凭证必须来自组织的管理账户或账户管理服务的委派管理员账户。

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

## 更新根用户密码

要编辑您 AWS 账户的 root 用户密码，请执行以下过程中的步骤。

## AWS 管理控制台

### 要编辑您的根用户密码

#### Note

您必须以身份登录 AWS 账户根用户，这不需要其他 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 AWS 账户电子邮件地址和密码以您的[AWS 管理控制台](#)身份登录 AWS 账户根用户。
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](#)，点击账户详情旁边的操作按钮，然后选择更新电子邮件地址和密码。
4. 在账户详情页面，点击密码旁边的编辑按钮。
5. 在编辑密码页面上，填写当前密码、新密码和确认新密码字段。然后，选择更新密码。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 AWS 账户根用户的密码](#)。

## AWS CLI & SDKs

AWS CLI 或其中一个 API 操作不支持此任务 AWS SDKs。您只能使用来执行此任务 AWS 管理控制台。

## 更新你的 AWS 账户 名字

管理多个名称时 AWS 账户，请使用与业务部门和应用程序一致的清晰命名惯例进行识别和组织。在重组、合并、收购或更新命名规范期间，您可能需要重命名账户，以维持一致的识别和管理标准。

账户名称会显示在多个位置，例如发票上以及账单和成本管理 (Billing and Cost Management) 控制面板和控制台等 AWS Organizations 控制台中。我们建议您使用标准方法来命名账户，以便您的账户名称易于识别。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，sales-catalog-prod）。出于隐私和安全考虑，请避免使用包含个人身份信息 (PII) 的账户名称。

- 独立 AWS 账户 — 对于 AWS 账户 未与组织关联的组织，您可以使用 AWS 管理控制台、或 AWS CLI 和更新您的账户名称 SDKs。若要了解如何执行此操作，请参阅[更新独立版的账户名 AWS 账户](#)。

- AWS 账户 在@@ 组织内部 — 对于属于组织的成员账户 AWS Organizations，管理账户或委托管理员账户中的用户可以从 AWS Organizations 控制台集中更新组织中任何成员账户的账户名，也可以通过 AWS CLI 和 SDKs 以编程方式更新组织中任何成员账户的账户名。若要了解如何执行此操作，请参阅[为您组织内的任何 AWS 账户 更新账户名](#)。

### Note

对的更改 AWS 账户 最多可能需要四个小时才能传播到任何地方。

## 主题

- [更新独立版的账户名 AWS 账户](#)
- [为您组织内的任何 AWS 账户 更新账户名](#)

## 更新独立版的账户名 AWS 账户

要更改独立版的帐户名 AWS 账户，请执行以下过程中的步骤。

### AWS 管理控制台

#### 最小权限

您可以使用根用户、IAM 用户或 IAM 角色来更新您的账户名称。如果您使用的是根用户，则无需其他 IAM 权限即可更新账户名称。使用 IAM 用户或 IAM 角色时，您必须至少具有以下 IAM 权限：

- `account:GetAccountInformation`
- `account:PutAccountName`

### 要更新独立账户的账户名

1. 使用您的 AWS 账户电子邮件地址和密码以您的[AWS 管理控制台](#)身份登录 AWS 账户根用户。
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](#)，点击账户详情旁边的操作按钮，然后选择更新账户名。
4. 在名称栏，输入您要更新的新账户名称，然后选择保存。

## AWS CLI & SDKs

### 最小权限

您可以使用根用户、IAM 用户或 IAM 角色来更新您的账户名称。要执行下列步骤，您的 IAM 用户或 IAM 角色必须至少具有以下 IAM 权限：

- `account:GetAccountInformation`
- `account:PutAccountName`

要更新独立账户的账户名

您还可以使用以下操作之一：

- AWS CLI: [put-account-name](#)

```
$ C:\> aws account put-account-name \  
    --account-name "New-Account-Name"
```

- AWS SDKs: [PutAccountName](#)

## 为您组织内的任何 AWS 账户 更新账户名

在 AWS Organizations 使用所有功能模式下，管理账户和委托管理员账户中的授权的 IAM 用户或 IAM 角色可以集中管理账户名称。

要为组织中的任何成员账户更改账户名，请执行以下流程中的步骤。

### 要求

要使用 AWS Organizations 控制台更新账户名，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[为组织启用所有功能](#)。
- 您需要为 AWS 账户管理服务启用可信访问权限。要进行设置，请参阅[为 AWS 账户管理启用可信访问权限](#)。

## AWS 管理控制台

### 最小权限

要更新成员账户的账户名称，您的 IAM 用户或 IAM 角色必须拥有以下权限：

- `organizations:DescribeOrganization` ( 仅限控制台 )
- `account:PutAccountName`

要更新成员账户的账户名称

1. 打开“组织”控制台，网址为 <https://console.aws.amazon.com/organizations/>。
2. 在左侧导航窗格中，选择 AWS 账户。
3. 在 AWS 账户 页面上，选择要更新的成员账户，选择操作下拉菜单，然后选择更新账户名。
4. 在名称栏中，输入更新的名称，然后选择保存。

## AWS CLI & SDKs

### 最小权限

要更新成员账户的账户名称，您的 IAM 用户或 IAM 角色必须拥有以下权限：

- `organizations:DescribeOrganization` ( 仅限控制台 )
- `account:PutAccountName`

要更新成员账户的账户名称

您还可以使用以下操作之一：

- AWS CLI: [put-account-name](#)

```
$ C:\> aws account put-account-name \  
    --account-id 111111111111 \  
    --account-name "New-Account-Name"
```

- AWS SDKs: [PutAccountName](#)

## 更新您的备用联系人 AWS 账户

备用联系人 AWS 最多可以联系三个与该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 AWS 账户 — 对于 AWS 账户 未与组织关联的组织，您可以使用 AWS 管理控制台或 AWS CLI & 更新自己的备用联系人 SDKs。要了解如何执行此操作，请参阅[为独立 AWS 账户更新备用联系人](#)。
- AWS 账户 组织内部 — 对于属于 AWS 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 AWS Organizations 控制台集中更新组织中的任何成员账户，也可以通过 AWS CLI & SDKs 以编程方式更新组织中的任何成员账户。要了解如何执行此操作，请参阅[更新组织 AWS 账户 中任何成员的备用联系人](#)。

### 主题

- [电话号码和电子邮件地址要求](#)
- [更新独立版的备用联系人 AWS 账户](#)
- [更新组织中任何 AWS 账户 成员的备用联系人](#)
- [账户 : AlternateContactTypes 上下文密钥](#)

## 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：“+ = . # | ! & - \_”。

## 更新独立版的备用联系人 AWS 账户

要添加或编辑独立版的备用联系人 AWS 账户，请执行以下步骤中的步骤。以下 AWS 管理控制台 过程始终仅在独立环境中起作用。您只能使用 AWS 管理控制台 访问或更改用于呼叫操作的账户中的备用联系人。

### AWS 管理控制台

为独立 AWS 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 [AWS 管理控制台](#)。
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**

对于企业而言 AWS 账户，最佳做法是输入公司的电话号码和电子邮件地址，而不是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。

## AWS CLI & SDKs

您可以使用以下 AWS CLI 命令或其 AWS SDK 等效操作来检索、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

如果您对相同 AWS 账户 和相同的联系人类型执行多项PutAlternateContact操作，则第一个操作会添加新联系人，而所有连续呼叫相同的联系 AWS 账户 人和联系人类型都会更新现有联系人。

## 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。

## 更新组织中任何 AWS 账户 成员的备用联系人

要添加或编辑组织 AWS 账户 中任何成员的备用联系人详细信息，请执行以下过程中的步骤。

### 要求

要使用 AWS 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[为组织启用所有功能](#)。
- 您需要为 AWS 账户管理服务启用可信访问权限。要进行设置，请参阅[为 AWS 账户管理启用可信访问权限](#)。

#### Note

AWS Organizations 托管策

略AWSOrganizationsReadOnlyAccess或AWSOrganizationsFullAccess已更新，提供访问 AWS 账户管理的权限，APIs 以便您可以从 AWS Organizations 控制台访问账户数据。要查看更新的托管策略，请参阅 [Organizations AWS 托管策略的更新](#)。

### AWS 管理控制台

为组织 AWS 账户 中的任何成员添加或编辑备用联系人

1. 使用组织的管理账户凭证登录 [AWS Organizations 控制台](#)。

2. 从 AWS 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

对于企业而言 AWS 账户，最佳做法是输入公司的电话号码和电子邮件地址，而不是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。

## AWS CLI & SDKs

您可以使用以下 AWS CLI 命令或其 AWS SDK 等效操作来检索、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。

 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**

如果您对相同 AWS 账户 和相同的联系人类型执行多项PutAlternateContact操作，则第一个操作会添加新联系人，而所有连续呼叫相同的联系 AWS 账户 人和联系人类型都会更新现有联系人。

**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。

## 账户：AlternateContactTypes上下文密钥

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。

## 更新 AWS 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 AWS 账户 — 对于 AWS 账户 未与组织关联的组织，您可以使用 AWS 管理控制台或 AWS CLI & 更新自己的主要账户联系人 SDKs。要了解如何执行此操作，请参阅[更新独立 AWS 账户 主要联系人](#)。
- AWS 账户 组织内部 — 对于属于 AWS 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 AWS Organizations 控制台集中更新组织中的任何成员账户，也可以通过 AWS CLI & SDKs 以编程方式更新组织中的任何成员账户。要了解如何执行此操作，请参阅[更新组织中的 AWS 账户 主要联系人](#)。

## 主题

- [电话号码和电子邮件地址要求](#)
- [更新独立账户 AWS 账户 或管理账户的主要联系人](#)
- [更新组织中任何 AWS 成员账户的主要联系人](#)

## 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 AWS 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。
- 对于企业而言 AWS 账户，最佳做法是输入公司的电话号码和电子邮件地址，而不是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。

## 更新独立账户 AWS 账户 或管理账户的主要联系人

要编辑独立版的主要联系人详细信息 AWS 账户，请执行以下步骤中的步骤。以下 AWS 管理控制台 过程始终仅在独立环境中起作用。您只能使用 AWS 管理控制台 访问或更改用于调用该操作的账户的主要联系人信息。

## AWS 管理控制台

为独立 AWS 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 [AWS 管理控制台](#)。
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。

## AWS CLI & SDKs

您可以使用以下 AWS CLI 命令或其 AWS SDK 等效操作来检索、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。

## 更新组织中任何 AWS 成员账户的主要联系人

要编辑组织中任何 AWS 成员账户中的主要联系人详细信息，请执行以下过程中的步骤。

### 其他要求

要使用 AWS 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[为组织启用所有功能](#)。
- 您需要为 AWS 账户管理服务启用可信访问权限。要进行设置，请参阅[为 AWS 账户管理服务启用可信访问权限](#)。

### AWS 管理控制台

编辑组织 AWS 账户中任何人的主要联系人

1. 使用组织的管理账户凭证登录 [AWS Organizations 控制台](#)。
2. 从 AWS 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。

### AWS CLI & SDKs

您可以使用以下 AWS CLI 命令或其 AWS SDK 等效操作来检索、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 AWS 账户 标识符

AWS 为每 AWS 账户人分配以下唯一标识符：

### [AWS 账户 ID](#)

一个 12 位数字（如 012345678901）用于唯一标识 AWS 账户。许多 AWS 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 AWS Identity and Access Management (IAM) 用户，则可以使用账户 ID 或账户别名登录。AWS 管理控制台 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。AWS 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 AWS 账户 时，您可以使用此 ID 来识别。您可以按 [根用户](#) 或 IAM 用户的身份检索 AWS 账户 的规范用户 ID。

您必须通过身份验证 AWS 才能查看这些标识符。

#### Warning

请勿将您的 AWS 凭证（包括密码和访问密钥）提供给需要您的 AWS 账户 标识符才能与您共享 AWS 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。AWS 账户

## 找到你的 AWS 账户 身份证

您可以使用 AWS 管理控制台 或 AWS Command Line Interface (AWS CLI) 来查找 AWS 账户 ID。在控制台中，账户 ID 的位置取决于您是以根用户还是以 IAM 用户身份登录。无论您以根用户还是以 IAM 用户身份登录，账户 ID 都是相同的。

### 以根用户身份查找您的账户 ID

#### AWS 管理控制台

在以 root 用户 AWS 账户 身份登录时查找你的 ID

#### 最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当以根用户身份登录时，您不需要任何 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

如果您没有看到安全凭证页面，您可以用 IAM 角色的联合用户身份登录，而非 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 AWS 账户 ID 旁边。

#### AWS CLI & SDKs

要查找您的 AWS 账户 身份证，请使用 AWS CLI

#### 最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当以根用户身份运行命令时，您不需要任何 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 用户身份查找账户 ID

### AWS 管理控制台

以 IAM 用户 AWS 账户 身份登录时查找您的 ID

#### 最小权限

要执行下列步骤，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

如果您没有看到安全凭证页面，您可以用 IAM 角色的联合用户身份登录，而非 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 AWS 账户 ID 旁边。

### AWS CLI & SDKs

要查找您的 AWS 账户 身份证，请使用 AWS CLI

#### 最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当以 IAM 用户或角色的身份运行命令时，您必须具有：
  - `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 AWS 账户的规范用户 ID

您可以使用 AWS 管理控制台 或找到适合您的 AWS 账户 规范用户 ID。AWS CLI 的规范用户 ID AWS 账户 是该账户所特有的。您可以以根用户、联合用户或 IAM 用户的 AWS 账户 身份检索规范用户 ID。

### 以根用户或 IAM 用户的身份查找规范 ID

#### AWS 管理控制台

在您以根用户或 IAM 用户身份登录控制台时查找您的账户的规范用户 ID

#### 最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当以根用户身份运行命令时，您不需要任何 IAM 权限。
- 当以 IAM 用户身份登录时，您必须具有：
  - `account:GetAccountInformation`

1. 以根用户或 IAM 用户身份登录。AWS 管理控制台
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

如果您没有看到安全凭证页面，您可以用 IAM 角色的联合用户身份登录，而非 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)。

## AWS CLI & SDKs

要查找规范用户 ID，请使用 AWS CLI

同样的 AWS CLI，API 命令适用于 AWS 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 IAM 角色的联合用户身份查找规范 ID

### AWS 管理控制台

在以具有 IAM 角色的联合用户身份登录控制台时查找账户的规范用户 ID

#### 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 角色的联合用户身份登录。AWS 管理控制台
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 AWS 账户 的规范 ID。

## AWS CLI & SDKs

要查找规范用户 ID，请使用 AWS CLI

同样的 AWS CLI，API 命令适用于 AWS 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
```

# AWS 账户管理中的安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。[责任共担模式](#)将此描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。AWS 还为您提供可以安全使用的服务。作为[AWS 合规计划](#)的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于账户管理的合规计划，请参阅[按合规计划划分 AWS 服务的范围和按合规计划 AWS 服务](#)。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您的公司的要求以及适用的法律法规。

本文档可帮助您了解在使用 AWS 账户管理时如何应用分担责任模型。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。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的账户管理资源。

## 主题

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

# AWS 账户管理中的数据保护

分 AWS [担责任模型](#)适用于 AWS 账户管理中的数据保护。如本模型所述 AWS，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 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](#)。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 [AWS Shared Responsibility Model and GDPR](#) 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。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 )。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的[使用跟 CloudTrail 踪](#)。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 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。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 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 ) 第 140-3 版》<https://aws.amazon.com/compliance/fips/>。

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）。这包括您 AWS 服务使用控制台、AWS CLI API 或进行账户管理或其他操作时 AWS SDKs。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 URL，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。

## AWS PrivateLink 用于 AWS 账户管理

如果您使用 Amazon Virtual Private Cloud ( 亚马逊 VPC ) 托管 AWS 资源，则无需通过公共互联网即可从 VPC 内部访问 AWS 账户管理服务。

Amazon VPC 允许您在自定义虚拟网络中启动 AWS 资源。可以使用 VPC 控制您的网络设置，例如 IP 地址范围、子网、路由表和网络网关。有关更多信息 VPCs，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 AWS 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 \(AWS PrivateLink\)](#)。

### 创建端点

您可以使用、AWS Command Line Interface (AWS CLI)、AWS 软件开发工具包 AWS 管理控制台、AWS 账户管理 API 或在 VPC 中创建 AWS 账户管理终端节点 CloudFormation。

有关使用 Amazon VPC 控制台或创建和配置终端节点的信息 AWS CLI，请参阅 Amazon VPC 用户指南中的[创建接口终端节点](#)。

### 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：

```
com.amazonaws.us-east-1.account
```

您必须完全按照说明使用字符串，并指定 us-east-1 区域。作为一项全球服务，账户管理仅在该 AWS 区域托管。

有关使用创建和配置终端节点的信息 CloudFormation，请参阅 CloudFormation 用户指南中的[AWSEC2::: 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](#)
- 《AWS 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 Amazon VPC 终端节点策略，该策略允许账户 123456789012 中的一个名为 Alice 的 IAM 用户检索和更改任何用户的备用联系信息 AWS 账户，但拒绝所有 IAM 用户删除任何账户中任何备用联系信息的权限。

如果要属于 AWS 组织一部分的账户的访问权限授予该组织成员账户中的委托人，则该 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《AWS PrivateLink 指南》中的[使用 VPC 端点控制对服务的访问](#)。

## 用于 AWS 账户管理的 Identity and Access Management

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和被授权（获得权限）使用账户管理资源。您可以使用 IAM AWS 服务，无需支付额外费用。

### 主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [AWS 账户管理如何与 IAM 配合使用](#)
- [账户管理的基于身份的 AWS 策略示例](#)
- [使用基于身份的策略 \( IAM 策略 \) 进行 AWS 账户管理](#)
- [AWS 账户管理身份和访问权限疑难解答](#)

## 受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅[AWS 账户管理身份和访问权限疑难解答](#)）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅[AWS 账户管理如何与 IAM 配合使用](#)）
- IAM 管理员：编写用于管理访问权限的策略（请参阅[账户管理的基于身份的 AWS 策略示例](#)）

## 使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center（例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录用户指南》中的[如何登录您的 AWS 账户](#)。

对于编程访问，AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的[适用于 API 请求的 AWS 签名版本 4](#)。

## AWS 账户 root 用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，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，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service，或者 AWS 服务使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。AWS IAM Identity Center 有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的[什么是 IAM Identity Center？](#)。

## IAM 用户和群组

[IAM 用户](#)是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的[要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问](#)。

[IAM 组](#)指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的[IAM 用户使用案例](#)。

## IAM 角色

[IAM 角色](#)是具有特定权限的身份，可提供临时凭证。您可以通过[从用户切换到 IAM 角色（控制台）](#)或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的[担任角色的方法](#)。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon 上运行的应用程序非常有用。EC2 有关更多信息，请参阅《IAM 用户指南》中的[IAM 中的跨账户资源访问](#)。

## 使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 [JSON 策略概述](#)。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

### 基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的 [使用客户管理型策略定义自定义 IAM 权限](#)。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的 [在托管策略与内联策略之间进行选择](#)。

### 基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中 [指定主体](#)。

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

### 其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，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)-在中指定组织或组织单位的最大权限 AWS Organizations。有关更多信息，请参阅《AWS Organizations 用户指南》中的 [服务控制策略](#)。

- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的[资源控制策略 \(RCPs\)](#)。
- 会话策略 – 在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。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 AWS 确定是否允许请求，请参阅 IAM 用户指南中的[策略评估逻辑](#)。

## AWS 账户管理如何与 IAM 配合使用

在使用 IAM 管理对账户管理的访问之前，您应该了解哪些 IAM 功能可用于账户管理。

您可以在 AWS 账户管理中使用的 IAM 功能

IAM 功能	账户管理支持
<a href="#">基于身份的策略</a>	是
<a href="#">基于资源的策略</a>	否
<a href="#">策略操作</a>	是
<a href="#">策略资源</a>	是
<a href="#">策略条件键</a>	是
<a href="#">ACLs</a>	否
<a href="#">ABAC (策略中的标签)</a>	否
<a href="#">临时凭证</a>	是
<a href="#">主体权限</a>	是
<a href="#">服务角色</a>	否
<a href="#">服务关联角色</a>	否

要全面了解账户管理和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM [配合使用的AWS 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附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[使用客户管理型策略定义自定义 IAM 权限](#)。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的[IAM JSON 策略元素引用](#)。

### 适用于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[账户管理的基于身份的 AWS 策略示例](#)。

## 账户管理内基于资源的策略

支持基于资源的策略：否

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

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的[IAM 中的跨账户资源访问](#)。

## 账户管理的策略操作

支持策略操作：是

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

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。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[AWS 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。AWS 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[账户管理的基于身份的 AWS 策略示例](#)。

## 账户管理的策略资源

支持策略资源：是

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

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 [Amazon 资源名称 \( ARN \)](#) 指定资源。对于不支持资源级权限的操作，请使用通配符 ( \* ) 指示语句应用于所有资源。

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

账户管理服务在 IAM 策略的 Resources 元素中支持以下特定资源类型，以帮助您筛选策略并区分以下类型 AWS 账户：

- account

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

- accountInOrganization

此resource类型仅匹配由 AWS 账户 该 AWS 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[AWS 账户管理定义的资源](#)。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅[AWS 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[账户管理的基于身份的 AWS 策略示例](#)。

## 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 AWS 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。

Condition 元素根据定义的条件指定语句何时执行。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。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的[AWS 全局条件上下文密钥](#)。

账户管理服务支持以下条件键，您可以使用这些键来为 IAM 策略提供精细筛选：

- 账户:TargetRegion

此条件键的参数由一系列 [AWS 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

此条件键的参数由通过组织层次结构通往特定组织单元（OU）的路径的列表组成。它让您筛选策略，使其仅影响匹配 OU 中的目标账户。

```
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账户。

- 账户:EmailTargetDomain

此条件键的参数由电子邮件域的列表组成。它让您可以筛选策略，使其仅影响与指定电子邮件域匹配的操作。此条件键不区分大小写。您应在策略条件块中使用 `StringEqualsIgnoreCase` 而非 `StringEquals`，以便根据目标电子邮件地址域来控制操作。以下是一个示例策略，它让您可以在电子邮件域名包含 `example.com`、`company.org` 或任何大小写组合（如 `EXAMPLE.COM`）时完成 `account:StartPrimaryEmailUpdate` 操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowConditionKey",
      "Effect": "Allow",
      "Action": [
        "account:StartPrimaryEmailUpdate"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "account:EmailTargetDomain": [
            "example.com",
            "company.org"
          ]
        }
      }
    }
  ]
}
```

要查看账户管理条件密钥列表，请参阅服务授权参考中的[AWS 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[AWS 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[账户管理的基于身份的 AWS 策略示例](#)。

## 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 ( 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。

## 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 ) : 否

基于属性的访问权限控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体 ( 用户或角色 ) 和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

对于 AWS 账户管理，仅通过 `account:AccountResourceOrgTags/key-name` 条件键支持基于标签的访问控制。账户命名空间 APIs 中不支持标准 `aws:ResourceTag/key-name` 条件密钥。

使用受支持条件密钥的示例 JSON 策略

以下示例策略允许访问您的组织中使用密钥 "" 和值 "12345CostCenter" 或 "67890" 标记的帐户的联系信息。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "account:GetContactInformation",
        "account:GetAlternateContact"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "account:AccountResourceOrgTags/CostCenter": [
            "12345",
            "67890"
          ]
        }
      }
    }
  ]
}
```

```
}  
  }  
] }  
}
```

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的[基于属性定义权限和 IAM 教程：根据标签定义访问 AWS 资源的权限](#)。

## 将临时凭证用于账户管理

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的[IAM 中的临时安全凭证](#)和[使用 IAM 的 AWS 服务](#)。

## 账户管理的跨服务主体权限

支持转发访问会话 ( FAS )：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，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担任、代表您执行操作的 [IAM 角色](#)。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的[创建向 AWS 服务委派权限的角色](#)。

## 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与服务相关联的 AWS 服务角色。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 AWS 账户，并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

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

## 账户管理的基于身份的 AWS 策略示例

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。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。

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

有关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[“AWS 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 AWS 管理控制台](#)
- [提供对“账户”页面的只读访问权限 AWS 管理控制台](#)
- [提供对“账户”页面的完全访问权限 AWS 管理控制台](#)

### 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 AWS 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 AWS 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 AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 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[AWS 托管策略](#)或[工作职能的 AWS 托管策略](#)。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的[IAM 中的策略和权限](#)。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的[IAM JSON 策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的[使用 IAM Access Analyzer 验证策略](#)。

- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的[使用 MFA 保护 API 访问](#)。

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

## 使用中的“账户”页面 AWS 管理控制台

要访问中的[账户页面](#) AWS 管理控制台，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 AWS 账户。如果您创建的基于身份的策略比所需的最低权限更严格，则无法为具有该策略的实体 (IAM 用户或角色) 正常运行控制台。

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` AWS 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](#)。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，在很多情况下，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 AWS 管理控制台

在以下示例中，您想要为 AWS 账户中的 IAM 用户授予对 AWS 管理控制台中“账户”页面的只读访问权限。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 AWS 区域，还必须包括 `account:ListRegions` 操作。

### JSON

```
{
  "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 AWS 管理控制台

在以下示例中，您想要为 AWS 账户中的 IAM 用户授予对 AWS 管理控制台中“账户”页面的完全访问权限。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。

### JSON

```

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

```

## 使用基于身份的策略（IAM 策略）进行 AWS 账户管理

有关 AWS 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。

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

## AWS 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[账户管理的基于身份的 AWS 策略示例](#)。

### Note

要向 IAM 用户授予对账户页面中特定[账户](#)设置的写入 GetAccountInformation 权限 AWS 管理控制台，除了要用于修改该设置的权限（或许可）之外，您还必须允许该权限。

权限名称	访问级别	说明
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:GetPrimaryEmail	读取	授予权限以检索账户的主电子邮件地址。
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 AWS 组织中成员账户主电子邮件地址更新的权限。
account:CloseAccount	写入	授予关闭账户的权限。

权限名称	访问级别	说明
		 <b>Note</b> 此权限仅适用于控制台。此权限不支持 API 访问。
account:DeleteAlternateContact	写入	授予权限以删除账户的备用联系人。
account:DisableRegion	写入	授予权限以禁用使用区域。
account:EnableRegion	写入	授予权限以启用使用区域。
account:PutAccountName	写入	授予权限以更新账户的名称。
account:PutAlternateContact	写入	授予权限以修改账户的备用联系人。
account:PutContactInformation	写入	授予权限以更新账户的主要联系人信息。
account:StartPrimaryEmailUpdate	写入	授予启动 AWS 组织中成员账户主电子邮件地址更新的权限。

## AWS 账户管理身份和访问权限疑难解答

使用以下信息可帮助您诊断和修复在使用账户管理和 IAM 时可能遇到的常见问题。

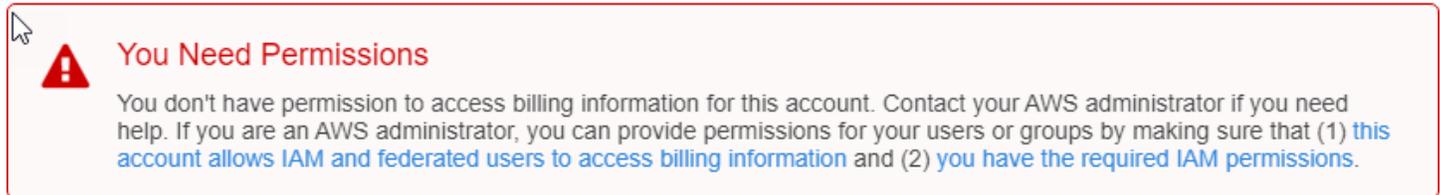
### 主题

- [我没有在“账户”页面中执行操作的权限](#)
- [我无权执行 iam:PassRole](#)
- [我想允许我以外的其他人 AWS 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 AWS 管理控制台 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 mateojackson IAM 用户尝试使用控制台在的“账户”页面 AWS 账户 中查看其详细信息 AWS 管理控制台 但没有 `account:GetAccountInformation` 权限时，就会出现以下示例错误。



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

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

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

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

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

## 我想允许我以外的其他人 AWS 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[AWS 账户管理如何与 IAM 配合使用](#)。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户，请参阅 [IAM 用户指南中的向您拥有 AWS 账户的另一个 IAM 用户提供访问权限](#)。
- 要了解如何向第三方提供对您的资源的访问[权限 AWS 账户](#)，请参阅 [IAM 用户指南中的向第三方提供访问权限](#)。AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的[为经过外部身份验证的用户（身份联合验证）提供访问权限](#)。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 [IAM 中的跨账户资源访问](#)。

## AWS AWS 账户管理的托管策略

AWS 账户管理目前提供两种可供您使用的 AWS 托管策略：

- [AWS 托管策略：AWSAccountManagementReadOnlyAccess](#)
- [AWS 托管策略：AWSAccountManagementFullAccess](#)
- [账户管理对 AWS 托管政策的更新](#)

AWS 托管策略是由创建和管理的独立策略 AWS。AWS 托管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，AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于使用案例的[客户管理型策略](#)来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 [AWS 托管策略](#)。

### AWS 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：

- 关于你的元数据 AWS 账户
- 已启用或禁用的 AWS 账户（您只能使用 AWS 控制台查看账户中区域的状态）AWS 区域

方法为：授予运行任何 Get\* 或 List\* 操作的权限。它不提供修改账户元数据或启用或禁 AWS 区域用账户的任何功能。

### 权限详细信息

该策略包含以下权限。

- `account`— 允许委托人检索相关的元数据信息 AWS 账户。它还允许主体列出为 AWS 管理控制台中的账户启用的 AWS 区域。

### JSON

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

## AWS 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：

- 关于你的元数据 AWS 账户
- 启用或禁用 AWS 区域的 AWS 账户（只有使用 AWS 控制台，您才能查看账户的状态或启用或禁用区域）

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**— 允许委托人查看或修改相关的元数据信息 AWS 账户。它还允许主体列出为账户启用的 AWS 区域 以及在 AWS 管理控制台中启用或禁用。

### JSON

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

## 账户管理对 AWS 托管政策的更新

查看自该服务开始跟踪这些变更以来账户管理 AWS 托管政策更新的详细信息。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
AWS 账户管理已推出新的 AWS 托管政策，并开始跟踪变更	账户管理最初使用以下 AWS 托管政策启动： <ul style="list-style-type: none"><li>• <a href="#">AWSAccountManagemementReadOnlyAccess</a></li><li>• <a href="#">AWSAccountManagemementFullAccess</a></li></ul>	2021 年 9 月 30 日

## AWS 账户管理的合规性验证

第三方审计师评估可 AWS 账户 作为多个合规计划的一部分在您中运行的 AWS 服务的安全 AWS 性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规计划范围内的 AWS 服务列表，请参阅“按合规计划划分 [AWS 服务的范围](#)”和“[按合规计划 AWS 服务](#)”。有关一般信息，请参阅 [AWS 合规计划 AWS](#)。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅《AWS Artifact 用户指南》中的“AWS Artifact “下载报告”。

您在使用服务时的合规责任取决于您的 AWS 账户 数据的敏感性、贵公司的合规目标以及适用的法律和法规。AWS 提供了以下资源来帮助实现合规性：

- [安全与合规性快速入门指南](#) — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 [Amazon Web Services 上构建 HIPAA 安全与合规性](#) — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

### Note

并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅 [符合 HIPAA 要求的服务参考](#)。

- [AWS 合规资源 AWS](#) — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- [使用 AWS Config 开发人员指南中的规则评估资源](#) — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- [AWS Security Hub CSPM](#) — 这 AWS 服务 可以全面了解您的安全状态 AWS ，帮助您检查自己是否符合安全行业标准和最佳实践。
- [AWS Audit Manager](#) — 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

## AWS 账户管理的弹性

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。各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、容错能力和可扩展性。

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

## 基础设施安全 AWS 账户管理

作为托管 AWS 服务，在您 AWS 账户 中运行的服务受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅[AWS 云安全](#)。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS security Pillar Well-Architected Framework 中的[基础设施保护](#)。

您可以使用 AWS 已发布的 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[AWS Security Token Service](#) ( AWS STS ) 生成临时安全凭证来对请求进行签名。

# 监控你的 AWS 账户

监控是维护 AWS 账户管理和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。AWS 提供以下监控工具，用于监视账户管理，在出现问题时进行报告，并在适当时自动采取措施：

- AWS CloudTrail 捕获（记录）由您或代表您进行的 API 调用 AWS 账户 和相关事件，并将日志文件写入您指定的亚马逊简单存储服务 (Amazon S3) 存储桶。这可以让您标识哪些用户和账户调用了 AWS、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 [AWS CloudTrail 《用户指南》](#)。
- Amazon EventBridge 通过自动响应系统事件（例如应用程序可用性问题和资源更改）来提高您的 AWS 服务的自动化程度。来自 AWS 服务的事件几乎实时地传送到 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 AWS 账户管理 API 调用 AWS CloudTrail

AWS 账户管理 APIs 与一项服务集成 AWS CloudTrail，该服务提供用户、角色或调用账户管理操作的 AWS 服务所采取的操作的记录。CloudTrail 将所有账户管理 API 调用捕获为事件。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 [《AWS CloudTrail 用户指南》](#)。

## 中的账户管理信息 CloudTrail

CloudTrail 在您创建账户 AWS 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，会将该活动与其他 AWS 服务 CloudTrail 事件一起 CloudTrail 记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 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 AWS 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，当您在中创建跟踪时 AWS 管理控制台，该跟踪将应用于所有跟踪 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。您可以配置其他 AWS 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](#)
- [配置 Amazon SNS 通知 CloudTrail](#)
- [接收来自多个区域的 CloudTrail 日志文件](#)
- [接收来自多个账户的 CloudTrail 日志文件](#)

AWS CloudTrail 记录本指南的“[API 参考](#)”部分中找到的所有[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：

- 请求是使用根用户还是 AWS Identity and Access Management (IAM) 用户证书发出
- 请求是使用 IAM 角色还是联合用户的临时安全凭证发出的
- 请求是否由其他 AWS 服务发出

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

## 了解账户管理日志条目

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": "AR0A1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```

"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "AR0A1234567890EXAMPLE",
    "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": "AR0A1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",

```

```

"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "AROAI1234567890EXAMPLE",
    "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
    "accountId": "123456789012",
    "userName": "ServiceTestRole"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-04-30T18:33:00Z"
  }
},
"eventTime": "2021-04-30T18:33:08Z",
"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": "ARO1234567890EXAMPLE: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": "2021-04-30T18:33:00Z"
    }
  }
},
"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"
}
```

## 使用监控账户管理事件 EventBridge

Amazon EventBridge (前身为 CloudWatch 事件) 可帮助您监控特定于事件的事件并启动使用其他事件的目标操作 AWS 服务。来自 AWS 服务的事件以近乎实时 EventBridge 的方式传送到。

使用 EventBridge，您可以创建匹配传入事件的规则，并将它们路由到目标进行处理。

有关更多信息，请参阅《[亚马逊 EventBridge 用户指南](#)》EventBridge 中的“[亚马逊入门](#)”。

### 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，只有特定于通过 CloudTrail 启用和禁用区域和 API 调用的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 事件记录在目标账户中。此外，当启用或禁用过程开始时，将向调用者账户发送一个 EventBridge 事件，并在任一过程完成后再次发送一个事件。

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和返回的状态相匹配：GetRegionOptStatusListRegions APIs

- 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"
    ]
  }
}
```

## 为您排查问题 AWS 账户

使用以下主题中的信息帮助诊断和解决 AWS 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《AWS 登录用户指南》中的[排查 AWS 账户登录问题](#)。

### 故障排除主题

- [排查 AWS 账户 创建问题](#)
- [排查 AWS 账户 关闭的问题](#)
- [排查其他 AWS 账户问题](#)

## 排查 AWS 账户 创建问题

使用下表中的参考链接来帮助您诊断和修复创建新内容时遇到的问题 AWS 账户。

问题	参考链接	来源
我不知道如何注册或创建账户	<a href="#">创建一个 AWS 账户</a>	本指南
如果我没有接 AWS 到验证新账户的电话或者我输入的 PIN 不起作用，我该怎么办？	<a href="https://repost.aws/knowledge-center/phone-verify-no-call">https://repost.aws/knowledge-center/phone-verify-no-call</a>	AWS re:Post
当我尝试 AWS 账户 通过电话验证时，如何解决“最大失败尝试次数”错误？	<a href="https://repost.aws/knowledge-center/maximum-failed-attempts">https://repost.aws/knowledge-center/maximum-failed-attempts</a>	AWS re:Post
已经过去 24 小时，但我的账户还没有激活	<a href="https://repost.aws/knowledge-center/create-and-activate-aws-account">https://repost.aws/knowledge-center/create-and-activate-aws-account</a>	AWS re:Post
我创建了新账户后无法登录	<a href="https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html">https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html</a>	AWS 登录用户指南

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

## 排查 AWS 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 AWS 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 ConstraintViolationException “” 错误](#)
- [我在尝试关闭成员账户时收到一条“CLOSE\\_ACCOUNT\\_QUOTA\\_LOCKED”错误](#)
- [在关闭管理账户之前，我需要删除我的 AWS 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 AWS 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 [root 用户身份登录](#) 才能关闭您的账户。AWS 管理控制台 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

该确认邮件仅发送至 AWS 账户的根用户电子邮件地址。如果您在几个小时内没有收到此电子邮件，则可以以 [root 用户 AWS 管理控制台 身份登录](#)，以检查您的账户是否已关闭。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。如果您关闭的账户是成员账户，则可以通过检查已关闭的账户是否在 AWS Organizations 控制台 CLOSED 中标记为来验证成功关闭。有关更多信息，请参阅《AWS 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员账户。只有当组织没有任何活跃的成员账户时，您才能关闭管理账户。要验证您的组织中是否没有活跃的成员账户，请转到 AWS Organizations 控制台，并确保所有成员账户都显示在其账户名称 Closed 旁边。然后就可以关闭管理账户。

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

您正在尝试使用 AWS Organizations 控制台关闭管理账户，但这是不可能的。要关闭管理账户，您需要以管理账户的 [root 用户身份登录](#)，然后从“账户”页面将其关闭。AWS 管理控制台 有关更多信息，请参阅《AWS 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 配额的更多信息，请参阅《AWS Organizations 用户指南》中的 [AWS Organizations 配额](#)。

## 在关闭管理账户之前，我需要删除我的 AWS 组织吗？

不，在关闭管理账户之前，您无需删除您的 AWS 组织。但是只有当组织没有任何活跃的成员账户时，您才能关闭管理账户。要验证您的组织中是否没有活跃的成员账户，请转到 AWS Organizations 控制台，并确保所有成员账户都显示在其账户名称 Closed 旁边。然后就可以关闭管理账户。

## 排查其他 AWS 账户问题

使用此处的信息有助于排查与 AWS 账户相关的问题。

### 问题

- [我需要更换我的信用卡 AWS 账户](#)
- [我需要举报欺诈 AWS 账户 活动](#)
- [我需要关闭我的 AWS 账户](#)

## 我需要更换我的信用卡 AWS 账户

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

## 我需要举报欺诈 AWS 账户 活动

如果您怀疑使用了您的欺诈活动 AWS 账户 并想举报，请参阅[如何举报滥用 AWS 资源](#)。

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 AWS 账户

有关解决关闭时遇到的问题帮助 AWS 账户，请参阅 [关闭一个 AWS 账户](#)。

# 关闭一个 AWS 账户

如果您不再需要您的 AWS 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 AWS 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 AWS 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 AWS 客户协议。
- 在关闭资源 AWS 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[AWS 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，您将在下个月收到账 AWS 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 AWS 服务。您可以在[后关闭期](#)登录和访问已关闭的 AWS 账户，但只能查看账单信息、访问账户设置或联系[AWS 支持](#)。
- 您不能在关闭时将注册到 AWS 账户的电子邮件地址用作其他 AWS 账户的主要电子邮件。如果想在不同的 AWS 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。有关更多信息，请参阅[更新根用户电子邮件地址](#)。
- 如果已经针对 AWS 账户根用户启用[多重身份验证 \(MFA\)](#)，或者已配置[IAM 用户上的 MFA 设备](#)，则在关闭账户时不会自动删除 MFA。如果您选择在[后关闭期](#) 90 天内保持 MFA 开启状态，请让 MFA 设备保持活动状态直到后关闭期到期，以防需要在此期间访问该账户。请注意，账户永久关闭后，硬件 TOTP 令牌设备无法与其他用户关联。如果随后想将硬件 TOTP 令牌用于其他用户，可以选择在关闭账户之前[停用硬件 MFA 设备](#)。适用于[IAM 用户](#)的 MFA 设备必须由账户管理员删除。

### 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 [AWS Organizations 的限额](#)。
- 如果您使用 Cont AWS 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《AWS 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

- AWS 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 AWS 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 AWS 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 AWS 账户 已关闭或永久关闭](#)”，以及[我的域名已在 Route 53 中注册](#)。
- AWS 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 AWS 账户 之前明确删除了其中的跟踪。AWS 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[AWS 账户 闭包和跟踪](#)。AWS 账户

## 如何关闭您的账户

您可以使用以下步骤关闭您 AWS 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 AWS 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 AWS 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 AWS Organizations。

从“账户”页面关闭独立账户

1. [在要关闭 AWS 管理控制台 的中，以 root 用户身份登录](#)。AWS 账户 您以 IAM 用户身份或角色登录时无法关闭账户。
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**

AWS CLI 或其中一个 API 操作不支持此任务 AWS SDKs。您只能使用来执行此任务 AWS 管理控制台。

## Member account

成员帐户是 AWS 账户 其中的一部分 AWS Organizations。

通过 AWS Organizations 控制台关闭成员账户

1. 登录 [AWS Organizations 控制台](#)。
2. 在 AWS 账户 页面上，找到并选择您想要关闭的成员账户的名称。您可以导航 OU 层次结构，或查看没有 OU 结构的账户的平面列表。
3. 选择页面顶部的账户名称旁边的 Close ( 关闭 )。仅当 AWS 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，请以根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**

您关闭的任何成员账户将在 AWS Organizations 控制台中的账户名称旁边显示一个 CLOSED 标签，并自原始关闭日期后持续最长 90 天。90 天后，AWS Organizations 控制台中将不再显示此成员账户。

从“账户”页面关闭成员账户

或者，您可以直接从中的[账户页面](#)关闭 AWS 成员账户 AWS 管理控制台。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 AWS CLI 和关闭成员账户 SDKs

有关如何使用 AWS CLI 和关闭成员账户的说明 SDKs，请参阅《AWS 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 AWS 账户 其父账户或主账号的账户 AWS Organizations。

### Note

您无法直接从 AWS Organizations 控制台关闭管理账户。

### 从“账户”页面关闭管理账户

1. [以您要关闭 AWS 管理控制台 的管理账户的 root 用户身份登录](#)。您以 IAM 用户身份或角色登录时将无法注销账户。
2. 确认组织中没有剩余的活跃成员账户。为此，请前往 [AWS Organizations 控制台](#)，确保所有成员账户在其账户名称旁边显示 Closed。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

AWS CLI 或其中一个 API 操作不支持此任务 AWS SDKs。您只能使用来执行此任务 AWS 管理控制台。

## AWS GovCloud (US) account

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

## 关闭 AWS GovCloud (US) 账户

如果您有与账户关联 AWS 账户的 AWS GovCloud (US) 账户，则需要先关闭标准账户，然后再关闭该 AWS 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 AWS GovCloud (US) 收费，请参阅 AWS GovCloud (US) 用户指南中的[关闭 AWS 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 AWS 账户 关闭的问题](#)。
- 您关闭的任何成员账户都将在 AWS Organizations 控制台中账户名称旁边显示一个CLOSED标签，有效期最长为原始关闭日期后的 90 天。90 天后，该成员账户将不再显示在 AWS Organizations 控制台中。
- 如果您已 AWS 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 AWS 账户，如果您向其他人授予了必要的权限，则他们 AWS 账户 可以再次访问您账户的 AWS 服务和资源。

并非所有地区和服务都会立即关闭账户，可能需要几个小时才能完成。

## 后关闭期

关闭后期是指从您关闭账户之日到 AWS 永久关闭账户 AWS 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 AWS 服务。关闭后期限过后，将 AWS 永久关闭您的 AWS 账户，您将无法再重新开放。AWS 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[AWS 账户 ID](#)将永远无法重复使用。

## 重新打开你的 AWS 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，AWS 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[AWS 支持](#)；(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

账户管理 (account) 命名空间中的 API 操作允许您修改自己的 AWS 账户。

每个 AWS 账户 支持包含账户信息的元数据，包括最多三个与该账户关联的备用联系人的信息。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，您可以从 AWS Organizations 管理账户中的身份调用这些 API 操作 AWS 账户，并为任何组织成员指定账户 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，它包含适用于各种编程语言和平台（Java AWS SDKs、Ruby、.NET、iOS、Android 等）的库和示例代码。它们 SDKs 提供了一种便捷的方式来创建对 Organizations 的编程 AWS 访问权限。例如，负责对请求 SDKs 进行加密签名、管理错误和自动重试请求。有关（包括如何下载和安装它们）的更多信息 AWS SDKs，请[参阅适用于 Amazon Web Services 的工具](#)。

我们建议您使用 AWS SDKs 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

向发送 HTTP 请求时 AWS，必须对请求进行签名，这样 AWS 才能识别谁发送了这些请求。您可以使用访问密钥（由 AWS 访问密钥 ID 和私有访问密钥组成）签署请求。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。另一种选择是，使用 AWS 安全令牌服务生成临时安全证书，然后使用这些证书签署请求。

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 AWS API 请求](#)。

当您使用 AWS 命令行界面 (AWS CLI) 或其中一个 AWS SDKs 向其发出请求时 AWS，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](mailto: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 AWS 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

账户管理支持一项服务 CloudTrail，用于记录您 AWS 的 API 调用 AWS 账户并将日志文件传输到 Amazon S3 存储桶。通过使用收集的信息 CloudTrail，您可以确定哪些请求已成功向账户管理部门发出、谁发出了请求、何时发出等。有关账户管理及其支持的更多信息 CloudTrail，请参阅[使用记录 AWS 账户管理 API 调用 AWS CloudTrail](#)。要了解更多信息 CloudTrail，包括如何将其开启和查找日志文件，请参阅[AWS CloudTrail 用户指南](#)。

# 操作

支持以下操作：

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

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

## AcceptPrimaryEmailUpdate

接受来自 [StartPrimaryEmailUpdate](#) 的要求为指定账户更新主要电子邮件地址 ( 也称为根用户电子邮件地址 ) 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。

### 请求正文

请求接受采用 JSON 格式的以下数据。

#### [AccountId](#)

指定您要通过此操作访问或修改 AWS 账户的 12 位帐户 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}`

是否必需：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}

是否必需：是

### PrimaryEmail

与指定账户一起使用的新的主要电子邮件地址。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。

是否必需：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

检索已接受的主要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。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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，或者尝试将账户的根用户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。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：409

### InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：500

### ResourceNotFoundException

操作失败，找不到指定的资源。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：429

## ValidationException

操作失败，其中一个输入参数无效。

fieldList

检测到无效条目的字段。

message

通知您该请求中无效内容的消息。

reason

验证失败的原因。

HTTP 状态代码：400

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 SDK](#)



## DeleteAlternateContact

从中删除指定的备用联系人 AWS 账户。

关于如何使用备用联系人操作的完整详细信息，请参阅[为您的 AWS 账户更新备用联系人](#)。

### Note

在更新由 AWS Organizations 管理的备用联系人信息之前 AWS 账户，必须先启用 AWS 账户管理与 Organizations 之间的集成。有关更多信息，请参阅[对 AWS 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。

## 请求正文

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 AWS 账户的 12 位数账户 ID 号。

如果未指定此参数，则默认为用于调用操作的身份的 AWS 帐户。

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

是否必需：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。

### errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：403

### InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

### errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：500

### ResourceNotFoundException

操作失败，找不到指定的资源。

### errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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。

### errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：429

### ValidationException

操作失败，其中一个输入参数无效。

### fieldList

检测到无效条目的字段。

### message

通知您该请求中无效内容的消息。

### reason

验证失败的原因。

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

{
  "AccountName": "MyAccount"
}
```

#### 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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 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。

## 请求正文

请求接受采用 JSON 格式的以下数据。

### AccountId

指定您要通过此操作访问或修改 AWS 账户的 12 位帐户 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`）。当您禁用某个区域时，AWS 会执行操作以在您的账户中停用该区域，例如销毁该区域中的 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：最小长度为 1。最大长度为 50。

是否必需：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。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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，或者尝试将账户的根用户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。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

HTTP 状态代码：409

## InternalServerErrorException

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

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。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

HTTP 状态代码：429

## ValidationException

操作失败，其中一个输入参数无效。

fieldList

检测到无效条目的字段。

message

通知您该请求中无效内容的消息。

reason

验证失败的原因。

HTTP 状态代码：400

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 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。

## 请求正文

请求接受采用 JSON 格式的以下数据。

### AccountId

指定您要通过此操作访问或修改 AWS 账户的 12 位帐户 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。指定帐户 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，AWS 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：最小长度为 1。最大长度为 50。

是否必需：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。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

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，或者尝试将账户的根用户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。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：409

## InternalServerErrorException

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：429

## ValidationException

操作失败，其中一个输入参数无效。

## fieldList

检测到无效条目的字段。

## message

通知您该请求中无效内容的消息。

## reason

验证失败的原因。

HTTP 状态代码：400

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

## GetAccountInformation

检索有关指定账户的信息，包括其账户名称、账户 ID 以及账户创建日期和时间。要使用此 API，IAM 用户必须拥有 `account:GetAccountInformation` IAM 权限。

### 请求语法

```
POST /getAccountInformation 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。

### 请求正文

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 AWS 账户的 12 位数账户 ID 号。

如果未指定此参数，则默认为用于调用操作的身份的 AWS 帐户。

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

## 响应语法

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

{
  "AccountCreatedDate": "string",
  "AccountId": "string",
  "AccountName": "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。

### AccountCreatedDate

创建账户的日期和时间。

类型：时间戳

### AccountId

指定您要通过此操作访问或修改 AWS 账户的 12 位帐户 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}`

### AccountName

账户的名称。

类型：字符串

长度限制：最小长度为 1。最大长度为 50。

模式：`[ -;=?-~ ]+`

## 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。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：403

### InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码 : 429

### ValidationException

操作失败，其中一个输入参数无效。

fieldList

检测到无效条目的字段。

message

通知您该请求中无效内容的消息。

reason

验证失败的原因。

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账户信息。

### 示例请求

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

{}
```

### 示例响应

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

{
  "AccountId": "123456789012",
  "AccountName": "MyAccount",
  "AccountCreatedDate": "2020-11-30T17:44:37Z"
}
```

## 示例 2

以下示例检索了组织中指定成员账户的账户信息。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.GetAccountInformation

{
  "AccountId": "123456789012"
}
```

### 示例响应

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

{
  "AccountId": "123456789012",
  "AccountName": "MyMemberAccount",
  "AccountCreatedDate": "2020-11-30T17:44:37Z"
}
```

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)

- [AWS 适用于 Ruby V3 的 SDK](#)

## GetAlternateContact

检索附加到的指定备用联系人。AWS 账户

关于如何使用备用联系人操作的完整详细信息，请参阅[为您的 AWS 账户更新备用联系人](#)。

### Note

在更新由 AWS Organizations 管理的备用联系人信息之前 AWS 账户，必须先启用 AWS 账户管理与 Organizations 之间的集成。有关更多信息，请参阅[对 AWS 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。

## 请求正文

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 AWS 账户的 12 位数账户 ID 号。

如果未指定此参数，则默认为用于调用操作的身份的 AWS 帐户。

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

是否必需：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。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

HTTP 状态代码：403

### InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

HTTP 状态代码：500

### ResourceNotFoundException

操作失败，找不到指定的资源。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

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。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：429

## ValidationException

操作失败，其中一个输入参数无效。

### fieldList

检测到无效条目的字段。

### message

通知您该请求中无效内容的消息。

### reason

验证失败的原因。

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

## GetContactInformation

检索 AWS 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[为您的 AWS 账户更新主要联系人](#)。

### 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。

### 请求正文

请求接受采用 JSON 格式的以下数据。

#### [AccountId](#)

指定您要通过此操作访问或修改 AWS 账户的 12 位帐户 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。指定帐户 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 AWS 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。

`errorType`

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：403

## InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

`errorType`

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：500

## ResourceNotFoundException

操作失败，找不到指定的资源。

`errorType`

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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。

`errorType`

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：429

## ValidationException

操作失败，其中一个输入参数无效。

`fieldList`

检测到无效条目的字段。

`message`

通知您该请求中无效内容的消息。

reason

验证失败的原因。

HTTP 状态代码：400

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

## GetGovCloudAccountInformation

检索与指定标准 GovCloud 账户 ( 如果存在 ) 关联的账户的相关信息，包括 GovCloud 账户 ID 和状态。要使用此 API，IAM 用户必须拥有 `account:GetGovCloudAccountInformation` IAM 权限。

### 请求语法

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

{
  "StandardAccountId": "string"
}
```

### URI 请求参数

该请求不使用任何 URI 参数。

### 请求正文

请求接受采用 JSON 格式的以下数据。

#### StandardAccountId

指定要通过此操作访问或修改的 AWS 账户的 12 位数账户 ID 号。

如果未指定此参数，则默认为用于调用操作的身份的 AWS 帐户。

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

## 响应语法

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

{
  "AccountState": "string",
  "GovCloudAccountId": "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。

### AccountState

关联账户的 GovCloud 账户状态。

类型：字符串

有效值：PENDING\_ACTIVATION | ACTIVE | SUSPENDED | CLOSED

### GovCloudAccountId

关联账户的 12 位数账户 ID GovCloud 号。

类型：字符串

模式：\d{12}

## 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。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：403

## InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：500

## ResourceNotFoundException

操作失败，找不到指定的资源。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：404

## ResourceUnavailableException

操作失败，因为它指定的资源当前不可用。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：424

## TooManyRequestsException

操作失败，调用频率过高且超过了节流限制。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码 : 429

### ValidationException

操作失败，其中一个输入参数无效。

fieldList

检测到无效条目的字段。

message

通知您该请求中无效内容的消息。

reason

验证失败的原因。

HTTP 状态代码 : 400

## 示例

### 示例 1

以下示例检索使用其凭证调用操作的账户的关联 GovCloud 账户信息。

### 示例请求

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

{}
```

### 示例响应

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

{
  "GovCloudAccountId": "123456789012",
  "AccountState": "ACTIVE"
}
```

## 示例 2

以下示例检索组织中指定成员 GovCloud 账户的关联账户信息。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.GetGovCloudAccountInformation

{
  "StandardAccountId": "111111111111"
}
```

### 示例响应

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

{
  "GovCloudAccountId": "123456789012",
  "AccountState": "ACTIVE"
}
```

## 示例 3

以下示例尝试检索未关联 GovCloud 账户的标准账户的关联 GovCloud 账户信息。

### 示例请求

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

{
  "StandardAccountId": "222222222222"
}
```

### 示例响应

```
HTTP/1.1 404
Content-Type: application/json
```

```
{  
  "message": "GovCloud Account ID not found for Standard Account - 222222222222."  
}
```

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

# GetPrimaryEmail

检索指定账户的主要电子邮件地址。

## 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。

## 请求正文

请求接受采用 JSON 格式的以下数据。

### [AccountId](#)

指定您要通过此操作访问或修改 AWS 账户的 12 位帐户 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主要电子邮件地址。

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。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

HTTP 状态代码：403

### InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

HTTP 状态代码：500

ResourceNotFoundException

操作失败，找不到指定的资源。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

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。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

fieldList

检测到无效条目的字段。

message

通知您该请求中无效内容的消息。

reason

验证失败的原因。

HTTP 状态代码：400

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于.NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)

- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 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。

## 请求正文

请求接受采用 JSON 格式的以下数据。

### AccountId

指定您要通过此操作访问或修改 AWS 账户的 12 位帐户 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。指定帐户 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：最小长度为 1。最大长度为 50。

是否必需：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：最小长度为 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。

`errorType`

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：403

### InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

`errorType`

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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。

`errorType`

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：429

### ValidationException

操作失败，其中一个输入参数无效。

`fieldList`

检测到无效条目的字段。

`message`

通知您该请求中无效内容的消息。

`reason`

验证失败的原因。

HTTP 状态代码：400

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 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。

### 请求正文

请求接受采用 JSON 格式的以下数据。

#### AccountId

指定您要通过此操作访问或修改 AWS 账户的 12 位帐户 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。指定帐户 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。请勿直接在 AWS CLI 之外使用 NextToken 响应元素。有关用法示例，请参阅《AWS 命令行界面用户指南》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《AWS 命令行界面用户指南》中的[分页](#)。

类型：字符串

长度限制：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。

`errorType`

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：403

InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

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。

errorType

API Gateway 填充到 x-amzn-ErrorType 响应标头的值。

HTTP 状态代码：429

ValidationException

操作失败，其中一个输入参数无效。

fieldList

检测到无效条目的字段。

message

通知您该请求中无效内容的消息。

reason

验证失败的原因。

HTTP 状态代码：400

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)

- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

## PutAccountName

更新指定账户的账户名称。要使用此 API，IAM 主体必须拥有 `account:PutAccountName` IAM 权限。

### 请求语法

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

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

### URI 请求参数

该请求不使用任何 URI 参数。

### 请求正文

请求接受采用 JSON 格式的以下数据。

#### AccountId

指定您要通过此操作访问或修改的 AWS 账户的 12 位数账户 ID 号。

如果未指定此参数，则默认为用于调用操作的身份的 AWS 帐户。

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

### AccountName

账户的名称。

类型：字符串

长度限制：最小长度为 1。最大长度为 50。

模式：`[ -;=?-~]+`

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。

errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：403

### InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

### errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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。

### errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：429

### ValidationException

操作失败，其中一个输入参数无效。

### fieldList

检测到无效条目的字段。

### message

通知您该请求中无效内容的消息。

### reason

验证失败的原因。

HTTP 状态代码：400

## 示例

### 示例 1

以下示例为用于调用该操作的凭证所属账户更新名称。

### 示例请求

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

{
  "AccountName": "MyAccount"
```

```
}
```

## 示例响应

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

## 示例 2

以下示例为组织中的指定成员账户更新账户名称。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.PutAccountName  
  
{  
  "AccountId": "123456789012",  
  "AccountName": "MyMemberAccount"  
}
```

## 示例响应

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

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)

- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

## PutAlternateContact

修改附加到的指定备用联系人。AWS 账户

关于如何使用备用联系人操作的完整详细信息，请参阅[为您的 AWS 账户更新备用联系人](#)。

### Note

在更新由 AWS Organizations 管理的备用联系人信息之前 AWS 账户，必须先启用 AWS 账户管理与 Organizations 之间的集成。有关更多信息，请参阅[对 AWS 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。

## 请求正文

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 AWS 账户的 12 位数账户 ID 号。

如果未指定此参数，则默认为用于调用操作的身份的 AWS 帐户。

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

是否必需：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：最小长度为 1。最大长度为 254。

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

是否必需：是

### [Name](#)

为备用联系人指定姓名。

类型：字符串

长度限制：最小长度为 1。长度上限为 64。

是否必需：是

### PhoneNumber

为备用联系人指定电话号码。

类型：字符串

长度限制：最小长度为 1。最大长度为 25。

模式：`[\s0-9()+-]+`

是否必需：是

### Title

为备用联系人指定职务。

类型：字符串

长度限制：最小长度为 1。最大长度为 50。

是否必需：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。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：403

## InternalServerError

由于内部错误，操作失败 AWS。请稍后重新尝试操作。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：429

## ValidationException

操作失败，其中一个输入参数无效。

## fieldList

检测到无效条目的字段。

## message

通知您该请求中无效内容的消息。

## reason

验证失败的原因。

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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

## PutContactInformation

更新 AWS 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[为您的 AWS 账户更新主要联系人](#)。

### 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。

### 请求正文

请求接受采用 JSON 格式的以下数据。

#### AccountId

指定您要通过此操作访问或修改 AWS 账户的 12 位帐户 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

### [ContactInformation](#)

包含与 AWS 账户相关的主要联系人信息的详细信息。

类型：[ContactInformation](#) 对象

是否必需：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。

### errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：403

### InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

### errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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。

### errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：429

### ValidationException

操作失败，其中一个输入参数无效。

### fieldList

检测到无效条目的字段。

### message

通知您该请求中无效内容的消息。

### reason

验证失败的原因。

HTTP 状态代码：400

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

# StartPrimaryEmailUpdate

启动为指定账户更新主要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。

## 请求正文

请求接受采用 JSON 格式的以下数据。

### AccountId

指定您要通过此操作访问或修改 AWS 账户的 12 位帐户 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}`

是否必需：是

## PrimaryEmail

在指定账户中使用的新的主要电子邮件地址（也称为根用户电子邮件地址）。

类型：字符串

长度限制：最小长度为 5。长度上限为 64。

是否必需：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

主要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。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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，或者尝试将账户的根用户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。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：409

## InternalServerError

由于内部存在错误，操作失败 AWS。请稍后重新尝试操作。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：500

## ResourceNotFoundException

操作失败，找不到指定的资源。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

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。

## errorType

API Gateway 填充到 `x-amzn-ErrorType` 响应标头的值。

HTTP 状态代码：429

## ValidationException

操作失败，其中一个输入参数无效。

fieldList

检测到无效条目的字段。

message

通知您该请求中无效内容的消息。

reason

验证失败的原因。

HTTP 状态代码：400

## 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 命令行界面 V2](#)
- [AWS 适用于 .NET 的 SDK V4](#)
- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Go v2 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS JavaScript V3 版软件开发工具包](#)
- [AWS 适用于 Kotlin 的 SDK](#)
- [AWS 适用于 PHP 的 SDK V3](#)
- [AWS Python 软件开发工具包](#)
- [AWS 适用于 Ruby V3 的 SDK](#)

## 其他 AWS 服务中的相关操作

以下操作与命名空间相关 AWS 账户管理 但属于 AWS Organizations 命名空间的一部分：

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

- [DescribeAccount](#)

## CreateAccount

CreateAccountAPI 操作只能在由 AWS 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《AWS Organizations API Reference》中的 [CreateAccount](#)。

## CreateGovCloudAccount

CreateGovCloudAccountAPI 操作只能在由 AWS 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《AWS Organizations API Reference》中的 [CreateGovCloudAccount](#)。

## DescribeAccount

DescribeAccountAPI 操作只能在由 AWS 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《AWS Organizations API Reference》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 AWS 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：最小长度为 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：最小长度为 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：最小长度为 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：最小长度为 1。最大长度为 50。

必需：否

#### 另请参阅

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

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

## ContactInformation

包含与 AWS 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：最小长度为 1。最大长度为 60。

是否必需：是

#### City

主要联系人地址中的城市。

类型：字符串

长度限制：最小长度为 1。最大长度为 50。

是否必需：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。

是否必需：是

#### FullName

主要联系人地址中的全名。

类型：字符串

长度限制：最小长度为 1。最大长度为 50。

是否必需：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：最小长度为 1。最大长度为 20。

模式：[+][\s0-9()-]+

是否必需：是

## PostalCode

主要联系人地址中的邮政编码。

类型：字符串

长度限制：最小长度为 1。最大长度为 20。

是否必需：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：最小长度为 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：最小长度为 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：最小长度为 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：最小长度为 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：最小长度为 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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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：最小长度为 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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

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

## ValidationExceptionField

输入未能满足 AWS 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

是否必需：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

有关以特定语言之一使用此 API 的更多信息 AWS SDKs，请参阅以下内容：

- [AWS 适用于 C++ 的 SDK](#)
- [AWS 适用于 Java 的 SDK V2](#)
- [AWS 适用于 Ruby V3 的 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。有关签名版本 4 的更多信息，请参阅 IAM 用户指南中的[签署 AWS API 请求](#)。

#### Action

要执行的操作。

类型：字符串。

是否必需：是

## Version

请求所针对的 API 版本，以格式表示 YYYY-MM-DD。

类型：字符串。

是否必需：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 AWS 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 X-Amz-Date 值：20120325T120000Z。

条件：X-Amz-Date 对所有请求而言是可选的；它可以用于覆盖对请求签名所使用的日期。如果日期标题以 ISO 8601 基本格式指定，则 X-Amz-Date 不是必填项。使用 X-Amz-Date 时，它总是会覆盖 Date 标题的值。有关更多信息，请参阅 IAM 用户指南中的[AWS API 请求签名要素](#)。

类型：字符串

必需：条件

### X-Amz-Security-Token

通过调用 AWS Security Token Service (AWS STS) 获得的临时安全令牌。有关支持来自 AWS 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 AWS 服务](#)。

条件：如果您使用的是中的临时安全证书 AWS STS，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 AWS 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

本节列出了所有 AWS 服务的 API 操作中常见的错误。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 AWS 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

我们的记录中不存在提供的 X.509 证书或 AWS 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

AWS 访问密钥 ID 需要订阅该服务。

HTTP 状态代码：403

#### RequestExpired

请求在请求的日期戳后超过 15 分钟或请求到期日期（例如预签名 URLs）超过 15 分钟到达服务，或者请求上的日期戳超过未来 15 分钟。

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

输入无法满足 AWS 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

本节包含有关使用 AWS 账户管理查询 API 的一般信息。有关 API 操作和错误的详细信息，请参阅[API 参考](#)。

### Note

您可以使用其中一个，而不是直接调用 AWS 账户管理查询 API AWS SDKs。AWS SDKs 由适用于各种编程语言和平台（Java、Ruby、.NET、iOS、Android 等）的库和示例代码组成。SDKs 提供了一种便捷的方法来创建对 AWS 账户管理的编程访问权限，以及 AWS。例如，负责处理诸如对请求 SDKs 进行加密签名、管理错误和自动重试请求之类的任务。有关信息 AWS SDKs，包括如何下载和安装它们，请参阅[适用于 Amazon Web Services 的工具](#)。

使用 AWS 账户管理查询 API，您可以调用服务操作。查询 API 请求是 HTTPS 请求，必须包含用于指示要执行的操作的 Action 参数。AWS 账户管理支持 GET 并 POST 请求所有操作。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 AWS 账户管理 API 请求](#)

## 端点

AWS 账户管理有一个托管在美国东部（弗吉尼亚北部）的全球 API 终端节点 AWS 区域。

有关所有服务的 AWS 终端节点和区域的更多信息，请参阅中的[区域和终端节点AWS 一般参考](#)。

## 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 AWS 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将 AWS 根账户凭据用于 AWS 账户管理的日常工作。您可以将证书用于 AWS Identity and Access Management (IAM) 用户，也可以使用临时证书，例如用于 IAM 角色。

要签署您的 API 请求，必须使用 AWS 签名版本 4。有关使用签名版本 4 的信息，请参阅 IAM 用户指南中的[签署 AWS API 请求](#)。

有关更多信息，请参阅下列内容：

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

## 的配额 AWS 账户管理

您的每项 AWS 服务 AWS 账户 都有默认配额，以前称为限制。除非另有说明，否则每个配额都是 AWS 区域特定的。

每个 AWS 账户 都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
一个中的备用联系人数量 AWS 账户	3 - BILLING、SECURITY 和 OPERATIONS 各一个
每个账户的并发区域选择请求数	6
每个组织的并发区域选择请求数	50
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 DisableRegion 请求速率	每秒 1 个，突增到每秒 1 个
每个账户的 EnableRegion 请求速率	每秒 1 个，突增到每秒 1 个
每个调用方账户的 GetAccountInformation 请求速率	每秒 3 个，突增到每秒 3 个
每个账户的 GetAlternateContact 请求速率	每秒 10 个，突增到每秒 15 个
每个账户的 GetContactInformation 请求速率	每秒 10 个，突增到每秒 15 个

资源	限额
每个账户的 GetGovCloudAccount Information 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 GetRegionOptStatus 请求速率	每秒 5 个，突增到每秒 5 个
每个账户的 ListRegions 请求速率	每秒 5 个，突增到每秒 5 个
每个调用方账户的 PutAccountName 请求速率	每秒 1 个，突增到每秒 1 个
每个账户的 PutAlternateContact 请求速率	每秒 5 个，突增到每秒 8 个
每个账户的 PutContactInformation 请求速率	每秒 5 个，突增到每秒 8 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

如果您注册了新的，AWS 账户 并选择印度作为联系方式和账单地址，则您的用户协议是与印度本地 AWS 卖家亚马逊网络服务印度私人有限公司 ( AWS 印度 ) 签订的。AWS 印度管理您的账单，您的发票总额以印度卢比 (INR) 而不是美元 (USD) 列出。有关管理的信息 AWS 账户，请参阅[配置你的 AWS 账户](#)。

如果您的账户位于 AWS 印度，请按照本主题中的步骤管理您的账户。本主题介绍如何注册 AWS 印度账户、编辑印度账户信息、管理客户验证以及添加或编辑您的永久账号 (PAN)。AWS

在注册时进行信用卡验证时，AWS 印度会向您的信用卡收取 2 印度卢比的费用。AWS 验证完成后，印度将退还2印度卢比。在验证过程中，您可能会重定向至您的银行。

## 主题

- [AWS 账户 与 AWS 印度一起创作](#)
- [管理您的客户验证信息](#)

## AWS 账户 与 AWS 印度一起创作

AWS 印度是印度 AWS 的本地销售商。如果您的联系地址和账单地址在印度，并且您想创建一个账户，请使用以下步骤注册 AWS 印度账户。

### 注册 AWS 印度账户

1. 打开[亚马逊云科技主页](#)。
2. 选择“创建”AWS 账户。

#### Note

如果您 AWS 最近登录过，则该选项可能不存在。请改为选择登录控制台。如果创建新 AWS 账户选项仍不可见，请选择登录其他账户，然后选择创建新 AWS 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位于印度，则根据印度计算机应急响应小组 (CERT-in) 的规定，AWS 在授予您使用 AWS 服务的权限之前，必须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。AWS 在验证过程中，印度会向您的信用卡收取 2 印度卢比的费用。AWS 验证完成后，印度将退还 2 印度卢比。
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。您还可以在账户设置中的客户验证页面或稍后在 Health AWS h Dashboard 中查看状态。您必须通过客户验证才能访问 AWS 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响应小组 (CERT-in) 的规定，AWS 在授予您新的或持续的 AWS 服务访问权限之前，必须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，AWS 将检查证件编号是否有效，以及您提供的姓名是否与您用于客户验证的文件关联的姓名相符。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 AWS 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 [AWS 管理控制台](#)。
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 Health AWS h Dashboard 收到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 [AWS 管理控制台](#)。
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 Health AWS h Dashboard 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 号码由十个字符组成，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。
- 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 和驾驶执照。
- 适用于企业账户 - PAN 卡和公司注册证书。

## 管理您的 AWS 印度账户

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 AWS 管理控制台 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号 \(GSTs\)](#)
- [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 AWS 账户管理的文档版本。

变更	说明	日期
<a href="#">新账户名 APIs</a>	Support for <a href="#">PutAccountName</a> APIs and new <a href="#">GetAccountInformation</a> 、查看或修改账户名。	2025 年 4 月 22 日
<a href="#">停止支持安全问题的编辑</a>	由于支持已终止，因此已从指南中删除了编辑您的安全问题主题。	2025 年 1 月 6 日
<a href="#">新的主邮箱 APIs</a>	支持新增 <a href="#">GetPrimaryEmail</a> 和 <a href="#">AcceptPrimaryEmailUpdate</a> APIs 集中更新中任何成员账户的根用户电子邮件地址 AWS Organizations。 <a href="#">StartPrimaryEmailUpdate</a> 有关更多信息，请参阅《AWS Organizations 用户指南》中的 <a href="#">为成员账户更新根用户电子邮件地址</a> 。	2024 年 6 月 6 日
<a href="#">重写“关闭账户”主题</a>	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
<a href="#">不再支持添加新的安全问题</a>	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
<a href="#">不再支持 <code>aws-portal</code> 命名空间</a>	AWS Identity and Access Management 之前用于管理您的账户的 (IAM) 操作 (例	2024 年 1 月 1 日

	如aws-portal:ModifyAccount 和aws-portal:ViewAccount ) 已终止标准支持。	
<a href="#">重写“区域”主题</a>	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
<a href="#">将根用户主题迁移到 IAM 用户指南中</a>	将有关根用户的讨论整合到一个主题中，并添加了已迁移至 IAM 用户指南的根用户主题交叉引用链接。	2023 年 9 月 18 日
<a href="#">主账户联系人主题中添加了新的部分</a>	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
<a href="#">新的联系信息 APIs</a>	Support 支持新的GetContactInformation 和 PutContactInformation APIs.	2022 年 7 月 22 日
<a href="#">AWS 账户管理现在支持通过 AWS Organizations 控制台更新备用联系人。</a>	现在，您可以使用更新的 AWS Organizations 托管政策提供的账户 API 权限，通过 AWS Organizations 控制台更新组织的备用联系人。	2022 年 2 月 8 日
<a href="#">初始版本</a>	《AWS 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。