

---

# Amazon 账户管理

参考指南

亚马逊云科技



## Amazon 账户管理: 参考指南

Copyright © 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 拥有的其它商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

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

## Table of Contents

欢迎使用 .....	1
什么是 Amazon Web Services 账户? .....	1
我需要多个吗Amazon Web Services 账户? .....	1
管理多个Amazon Web Services 账户 .....	2
入门：您是 Amazon 新用户吗? .....	2
开始使用 .....	3
管理Amazon Web Services 账户 .....	6
创建 账户 .....	6
查看账户标识符 .....	7
查找您的Amazon Web Services 账户ID .....	8
查找的规范用户 IDAmazon Web Services 账户 .....	9
更新根用户 .....	11
更新联系信息 .....	11
主账户联系人 .....	12
替代账户联系人 .....	12
设置或更改安全挑战问题 .....	18
指定哪个Amazon Web Services 区域你的账户可以使用 .....	18
设置或更改Amazon Web Services 账户alias .....	20
创建、删除和查看Amazon Web Services 账户alias .....	21
关闭您的 账户 .....	22
在您关闭 Amazon Web Services 账户 之前的注意事项 .....	23
排除关闭时的错误Amazon Web Services 账户 .....	24
关闭您的 Amazon Web Services 账户 .....	25
访问您的Amazon Web Services 账户关闭它之后 .....	25
后关闭期之后 .....	25
为您的账单Amazon Web Services 账户 .....	26
管理印度的账户 .....	26
确定您的账户所属的公司 .....	26
创建Amazon Web Services 账户使用 AISPL .....	27
管理您的 AISPL 账户 .....	27
使用根用户 .....	29
登录 .....	29
激活 MFA .....	30
更改密码 .....	30
创建访问密钥 .....	31
创建根用户的访问密钥 .....	31
删除根用户的访问密钥 .....	32
比较根用户和 IAM 用户 .....	33
需要 root 用户的任务 .....	34
账户管理 &Amazon Organizations .....	35
可信访问权限 .....	35
委托管理员账户 .....	36
示例 SCPs .....	37
最佳实践 .....	39
根用户 .....	39
限制你对 root 用户执行的任务 .....	39
锁定你的Amazon Web Services 账户root 用户访问密钥 .....	39
Amazon 访问密钥 .....	40
删除 (或不生成) 账户访问密钥 .....	40
使用临时安全凭证 (IAM 角色) 代替长期访问密钥 .....	40
正确管理 IAM 用户访问密钥 .....	41
使用 Amazon 访问密钥访问移动应用程序 .....	42
了解更多信息 .....	42
安全性 .....	43

数据保护 .....	43
Amazon PrivateLink .....	44
创建终端节点 .....	44
Amazon VPC 终端节点策略 .....	44
端节点策略 .....	44
Identity and Access Management .....	45
Audience .....	45
使用身份进行身份验证 .....	46
使用策略管理访问 .....	47
Amazon账户管理和 IAM .....	48
基于身份的策略示例 .....	53
问题排查 .....	55
Amazon托管式策略 .....	57
Amazon 账户管理只读访问 .....	57
Amazon 账户管理完全访问 .....	58
策略更新 .....	58
合规性验证 .....	59
故障恢复能力 .....	59
基础设施安全性 .....	59
监控 .....	60
CloudTrail 日志 .....	60
CloudTrail 中的账户管理信息 .....	60
了解账户管理日志条目 .....	61
API 参考 .....	64
Actions .....	65
DeleteAlternateContact .....	66
GetAlternateContact .....	69
PutAlternateContact .....	73
相关操作 .....	76
CreateAccount .....	76
创建 GovCloud账户 .....	76
DescribeAccount .....	76
数据类型 .....	77
AlternateContact .....	78
常见参数 .....	79
常见错误 .....	80
发出 HTTP 查询请求 .....	82
Endpoints .....	82
必须使用 HTTPS .....	82
SIGNAmazon账户管理 API 请求 .....	82
配额 .....	84
排除的故障Amazon Web Services 账户 .....	85
账户创建问题 .....	85
我没收到来自的电话Amazon验证我的新账户 .....	85
当我尝试验证我的时候，我收到有关“最大失败尝试次数”错误的错误Amazon Web Services 账户通过电话 .....	86
根用户问题 .....	86
root 用户受到限制 .....	86
我忘记账户根用户的密码 .....	86
我无权访问我的电子邮件Amazon Web Services 账户 .....	86
登录问题 .....	87
要获取我的Amazon Web Services 账户ID 或别名 .....	87
我忘记了 IAM 用户名或密码 .....	87
其他问题 .....	87
我需要为我的信用卡更改Amazon Web Services 账户 .....	88
我需要举报欺诈Amazon Web Services 账户活动 .....	88
我需要关闭我的Amazon Web Services 账户 .....	88

文档历史记录 .....	89
Amazon词汇表 .....	90
.....	xci

# 欢迎使用 Amazon 账户管理参考指南

## 什么是 Amazon Web Services 账户？

本指南包含以下信息：Amazon Web Services 账户. 如何创建它们、如何管理它们以及如何使用它们。

中的账户 Amazon 是访问的基本组成部分 Amazon 服务。它提供这两个基本功能：

- **容器**— 一个 Amazon Web Services 账户是所有的基本容器 Amazon 你可以创建的资源 Amazon 客户。当您创建 Amazon Simple Storage Service (Amazon S3) 存储桶或 Amazon Relational Database Service (Amazon RDS) 数据库以存储您的数据时，或创建 Amazon Elastic Compute Cloud (Amazon EC2) 实例以处理您的数据时，您正在自己的账户中创建资源。每个资源都由亚马逊资源名称 (ARN) 唯一标识，该名称包含或拥有该资源的账户的账户 ID。
- **安全边界**— 一个 Amazon Web Services 账户也是你的基本安全边界 Amazon 资源的费用。您在帐户中创建的资源仅适用于拥有同一账户凭据的用户。

您可以在账户中创建的主要资源包括：身份之外的压缩算法（例如 [IAM 用户](#) 和 [角色](#)。这些身份有人可以用来登录的凭据，或者 [authenticate](#) 到 Amazon。身份也有 [权限策略](#) 指定了登录的人有权处理账户中的资源。

您可以创建 Amazon Identity and Access Management (IAM) 用户授予贵公司人员的访问权限。该 IAM 用户可以拥有 [a password](#) 这允许该人访问 Amazon 控制台。用户也可以拥有一个 [访问密钥](#) 让人运行命令来自的 Amazon Command Line Interface (Amazon CLI) 或者从其中一个调用 API Amazon 开发工具包。

IAM 角色特别灵活，因为您可以通过使用 [联邦和身份提供商](#) 之外的压缩算法（例如 [Amazon Web Services Single Sign On \(Amazon Web Services SSO\)](#)）。如果您的公司已经在使用身份提供商，则可以将其与联合身份验证一起使用，以简化如何提供对中资源的访问权限 Amazon Web Services 账户。Amazon 支持符合行业标准的身份提供商 [OpenID Connect \(OIDC\)](#) 或者 [SAML 2.0 \(安全断言标记语言 2.0\)](#)。如果将任何 Active Directory 实施与 Microsoft Active Directory 联合身份验证服务结合使用，那么后者会将其变成源

## 我需要多个吗 Amazon Web Services 账户？

Amazon Web Services 账户作为基本安全边界 Amazon。它们充当资源容器，提供了有用的隔离级别。隔离资源和用户的能力是建立安全、良好管理的环境的关键要求。

将你的资源分成单独的 Amazon Web Services 账户有助于您在云环境中支持以下原则：

- **安全控制**— 不同的应用程序可以具有不同的安全配置文件，需要围绕它们不同的控制策略 例如，与审计师交谈要容易得多，而且能够指向一个审计员 Amazon Web Services 账户它承载受到影响的工作负载的所有元素 [支付卡行业 \(PCI\) 安全标准](#)。
- **隔离**— 一个 Amazon Web Services 账户是一个安全保护单位。应将潜在风险和安全隐患包含在 Amazon Web Services 账户而不影响他人。由于不同的团队或安全配置文件不同，可能会有不同的安全需求。
- **许多团队**— 不同的团队有不同的责任和资源需求。您可以通过将团队移动到分开来防止他们互相干扰 Amazon Web Services 账户。
- **数据隔离**— 除了隔离团队之外，还必须将数据存储隔离到帐户中。这有助于限制可以访问和管理该数据存储的人数。这有助于遏制对高度私密数据的暴露，因此可以帮助遵守 [欧盟通用数据保护条例 \(GDPR\)](#)。
- **业务流程**— 不同的业务单位或产品可能具有完全不同的目的和流程。有多个 Amazon Web Services 账户，您可以支持业务部门的特定需求。
- **Billing**— 账户是在账单级别分隔物品的唯一真实方法。多个账户有助于在不同业务单位、职能团队或个人用户之间分开账单级别的项目。您仍然可以将所有账单合并到单个付款人（使用 Amazon Organizations 和整合账单），同时将行项目分隔为 Amazon Web Services 账户。

- 配额分配—Amazon每个服务配额分别强制执行Amazon Web Services 账户. 将工作负载分为不同Amazon Web Services 账户阻止他们互相消耗配额。

本文中描述的所有建议和程序都符合[Amazon架构完善的框架](#). 此框架旨在帮助您设计灵活、有弹性且可扩展的云基础架构。即使你从小开始，我们建议你遵循框架中的这一指导方针。这样做可以帮助您安全地扩展环境，而不会影响随着增长的持续运营。

## 管理多个Amazon Web Services 账户

在开始添加多个账户之前，您需要制定管理它们的计划。为此，我们建议使用[Amazon Organizations](#)，这是一个免费的Amazon服务来管理所有Amazon Web Services 账户在组织中。

Amazon还优惠Amazon Control Tower，它添加了层Amazon管理 Organizations 的自动化并自动将其与其他组织集成Amazon类似服务Amazon CloudTrail、Amazon Config，Amazon CloudWatch，Amazon Service Catalog，以及其他。这些服务可能产生额外的费用。有关更多信息，请参阅 [Amazon Control Tower 定价](#)。

## 入门：您是 Amazon 新用户吗？

创建一个分步式的Amazon Web Services 账户，然后通过使用Amazon Identity and Access Management(IAM)，请参阅[the section called “开始使用” \(p. 3\)](#)。

如果您是的新用户Amazon，那么你的第一步就是注册Amazon Web Services 账户. 当您执行此操作的时候，Amazon创建新的Amazon Web Services 账户以及你提供的详细信息并将其分配给你。

全新Amazon Web Services 账户从内置的开始根用户，账户的内在管理员。您可以登录到Amazon Web Services Management Console将使用您在注册时提供的电子邮件地址和密码以根用户身份。

### Important

我们强烈建议您将根用户用于仅限执行以下任务：

- 在中创建第一个管理用户Amazon Identity and Access Management(IAM)。然后，您可以使用此IAM 管理员用户来执行管理任务，而不是根用户。这些区域有：[入门教程 \(p. 3\)](#)向您介绍如何创建这个第一个用户。
- 执行的任务仅限根用户可以执行。有关这些任务的列表，请参阅[需要根用户凭证的任务 \(p. 34\)](#)。
- 使用保护根用户凭证[推荐的最佳实践 \(p. 39\)](#)。

对于所有其他任务，请登录Amazon Web Services Management Console或者Amazon Command Line Interface(Amazon CLI) 使用以下用户之一的凭证：

- 网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的IAM 用户将附加到[权限策略](#)允许所需的任务。
- 网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的IAM 角色将附加到[权限策略](#)允许所需的任务。你可以使用某种形式的[联合身份验证](#)，例如通过使用Amazon Web Services Single Sign On(Amazon Web Services SSO) 或 SAML 2.0 提供商，例如微软 Active Directory 联合服务。

在您首次以根用户身份登录之后，我们建议您启用多重验证 (MFA) 以帮助确保此重用户的安全。

接下来，您可以在中创建具有管理员权限的 IAM 用户Amazon Web Services 账户. 除了少数情况外，该用户几乎可以在你的账户中执行任何操作[仅限于 root 用户的任务 \(p. 34\)](#)。

# 开始使用Amazon Web Services 账户

按照以下步骤创建您的 Amazon Web Services 账户。创建账户后，以根用户身份登录以创建 IAM 用户以执行日常管理任务。

## 步骤

- [Prerequisites \(p. 3\)](#)
- [第 1 步：创建您的Amazon Web Services 账户 \(p. 3\)](#)
- [第 2 步：登录到新账户的 root 用户 \(p. 5\)](#)
- [第 3 步：为您的根用户启用多重验证 \(p. 5\)](#)
- [第 4 步：创建 IAM 管理员用户 \(p. 5\)](#)

## Prerequisites

注册Amazon Web Services 账户，您需要提供以下信息：

- 账户名称— 账户名称显示在多个位置，例如发票上，以及 Billing and Cost Management 控制面板和 Amazon Organizations控制台。

我们建议您使用账户命名标准，以便可以轻松识别账户名称并与您可能拥有的其他账户区分开来。如果是公司账户，请考虑使用命名标准，例如组织-目的-环境（例如，AnyCompany-审核-Pad）。如果是个人账户，请考虑使用命名标准，例如名-姓-目的（例如，paulo-santos 测试账户）。

注册后，您可以在账户设置中更改账户名称。有关更多信息，请参阅 [如何更改我的名称Amazon Web Services 账户？](#)

- 电子邮件地址— 此电子邮件地址用作帐户 root 用户的登录名称，并且是恢复帐户所必需的，例如忘记密码的情况。您必须能够接收发送到此地址的电子邮件。在执行某些任务之前，必须验证自己有权访问发送到此地址的电子邮件。

### Important

如果此账户适用于企业，我们建议您使用公司通讯组列表（例如，it.admins@example.com）。避免使用个人的公司电子邮件地址（例如，paulo.santos@example.com）。这种方法有助于确保贵公司可以保留对Amazon Web Services 账户即使员工改变职位或离开公司也是如此。电子邮件地址可用于重置帐户的 root 用户凭据。请确保保护对此通讯组列表或地址的访问权限。

- 电话号码— 当需要确认账户所有权时，可以使用此号码。你必须能够通过此电话号码接听来电。

### Important

如果此帐户适用于企业，我们建议您使用公司电话号码而不是个人电话号码。这有助于确保您的公司可以保留对Amazon Web Services 账户即使员工改变职位或离开公司也是如此。

- 多重验证设备。— 为了保护你的Amazon资源，[在根账户上启用多重验证 \(MFA\)](#)。

## 第 1 步：创建您的Amazon Web Services 账户

1. 打开[Amazon主页](#)在您的浏览器中。
2. 选择创建Amazon Web Services 账户。

### Note

如果你登录Amazon最近，选择登录到控制台。如果选项创建新的Amazon Web Services 账户不可见，首先选择登录到其他账户，然后选择创建新的Amazon Web Services 账户。



3. 输入您的账户信息，然后选择Continue. 请确保正确输入帐户信息，尤其是电子邮件地址。如果您输入的电子邮件地址错误，则无法访问帐户。
4. 选择个人或者专业. 这些选项之间的区别仅在于我们要求您提供的信息。两种账户类型都具有相同的特性和功能。
5. 输入您的公司或个人信息。请参阅中的建议[先决条件 \(p. 3\)](#)有关电子邮件地址和电话号码的部分。
6. 阅读并接受[Amazon客户协议](#). 一定要阅读并理解Amazon客户协议。
7. 选择创建账户然后继续.

此时，您将收到一封电子邮件，确认Amazon Web Services 账户已准备好使用。您可以使用注册过程中提供的电子邮件地址和密码登录到您的新账户。但是，您无法使用任何Amazon服务直到你完成帐户激活为止。

8. 在存储库的付款信息页面中，输入有关付款方式的信息。如果您要将与您在中提供的其他地址用于账单目的[Step 3 \(p. 4\)](#)，选择使用新地址然后输入用于计费目的的地址。
9. 选择验证并添加.

#### Note

如果您的联系地址位于印度，则您的账户用户协议是与本地亚马逊互联网服务私人有限公司 (AISPL) 签订的。Amazon印度的卖家。您必须在验证过程中提供 CVV。您可能还必须输入一次性密码，具体取决于您的银行。AISPL 将在验证过程中将对您的付款方式收取 2 INR。AISPL 将在验证完成后退回 2 INR。

10. 接下来，您必须验证您的电话号码。从列表中选择您的国家或地区代码，然后输入可以在接下来的几分钟内拨打的电话号码。输入 CAPTCHA 代码，然后提交。
11. 这些区域有：Amazon自动验证系统致电您并提供 PIN 码。使用手机输入 PIN 码然后选择Continue.
12. 最后，您可以选择您的Amazon Web Services Support计划。选择一个可用计划。有关可用计划的说明，请参阅[Compare Amazon Web Services Support计划](#).

此时将显示一个确认页面，指示您的账户正在激活。这通常只需要几分钟时间，但有时可能需要长达 24 小时。在激活过程中，您可以登录新的Amazon Web Services 账户。在激活完成之前，你可能会看到完成注册按钮。您可以忽略它。

Amazon将在账户激活完成后发送确认电子邮件。检查您的电子邮件和垃圾邮件文件夹以获取确认电子邮件 在您收到此消息后，您可以完全访问所有消息Amazon服务。

## 解决账户激活延迟问题

帐户激活有时可能会延迟。如果该过程需要超过 24 小时，请检查以下内容：

- 完成账户激活过程。

在添加所有必要信息之前，您可能意外关闭了注册过程的窗口。要完成注册过程，请打开[注册](#)页。然后，选择登录到现有的Amazon Web Services 账户，然后使用您为帐户选择的电子邮件地址和密码登录。

- 查看与您的付款方式相关的信息。Check[付款方法](#)中的Amazon Billing and Cost Management控制台。修复信息中的任何错误。
- 联系你的金融机构。金融机构偶尔拒绝来自Amazon. 联系您的付款方式的发卡机构，并要求他们批准来自Amazon.

#### Note

Amazon一旦您的金融机构批准了授权请求，就会立即取消该请求。您无需为来自的授权请求付费 Amazon. 对于金融机构的报表，授权请求可能仍显示为少量费用（通常为 1 美元）。

- 查看您的电子邮件，了解是否要求您提供 检查你的电子邮件和垃圾邮件文件夹看看Amazon需要你提供任何信息才能完成激活过程。
- 尝试使用其他浏览器。

- 联系人Amazon Web Services Support. 联系人[Amazon Web Services Support](#)寻求帮助。一定要提及你已经尝试过的任何疑难解答步骤

#### Note

请勿在与之通信中提供敏感信息，例如信用卡号。Amazon.

## 第 2 步：登录到新账户的 root 用户

在您成功创建账户后，您可以登录并开始使用Amazon服务。

要以根用户身份登录到您的新账户，请参阅[以Amazon Web Services 账户根用户 \(p. 29\)](#)。

## 第 3 步：为您的根用户启用多重验证

我们强烈建议您为账户的根用户启用 MFA。这大大降低了某人在未经您授权的情况下访问您账户的风险。有关更多信息，请参阅[在上激活 MFAAmazon Web Services 账户根用户 \(p. 30\)](#)。

## 第 4 步：创建 IAM 管理员用户

由于您无法限制 root 用户可以执行的操作，因此我们强烈建议您不要将 root 用户用于任何不明确需要 root 用户的任务。相反，创建一个具有管理权限的 IAM 用户，然后以该 IAM 用户身份登录执行日常管理任务。

有关如何创建此类用户的说明，请参阅[创建您的第一个 IAM 管理员用户](#)中的IAM 用户指南。

# 管理 Amazon Web Services 账户

本节包含介绍如何管理 Amazon Web Services 账户。

## Note

如果您的 Amazon Web Services 账户是在印度使用 Amazon Internet Services Private Limited (AISPL) 创建的，还有其他注意事项。有关更多信息，请参阅[管理印度的账户](#) (p. 26)。

## 主题

- [创建 Amazon Web Services 账户](#) (p. 6)
- [查看账户标识符](#) (p. 7)
- [修改账户名称、电子邮件地址或密码 Amazon Web Services 账户根用户](#) (p. 11)
- [添加或更新主要和备用联系人信息](#) (p. 11)
- [设置或更改安全挑战问题](#) (p. 18)
- [指定哪个 Amazon Web Services 区域你的账户可以使用](#) (p. 18)
- [设置或更改 Amazon Web Services 账户 alias](#) (p. 20)
- [关闭您的 Amazon Web Services 账户](#) (p. 22)
- [为您的账单 Amazon Web Services 账户](#) (p. 26)
- [管理印度的账户](#) (p. 26)

## 创建 Amazon Web Services 账户

本主题介绍如何创建独立版本 Amazon Web Services 账户这不是由管理的 Amazon Organizations。如果你想创建一个帐户，该帐户属于由管理的组织 Amazon Organizations，请参阅[创建 Amazon Web Services 账户在组织中](#)。

这些说明用于创建 Amazon Web Services 账户在印度之外。要在印度创建账户，请参阅[创建 Amazon Web Services 账户使用 AISPL](#) (p. 27)。

Amazon Web Services Management Console

### 创建 Amazon Web Services 账户

#### 最小权限

要执行以下步骤，您必须至少具有以下 IAM 权限：

- 因为此操作发生在你有 Amazon Web Services 账户，此操作不需要 Amazon 权限。

1. 打开[Amazon Web Services 主页](#)。
2. 选择创建 Amazon Web Services 账户。

## Note

如果你登录 Amazon 最近，这种选择可能不存在。相反，选择登录到控制台。那么，如果创建新的 Amazon Web Services 账户还是不可见，首先选择登录到其他账户，然后选择创建新的 Amazon Web Services 账户。

3. 输入您的账户信息，然后选择 Continue。请确保正确输入帐户信息，尤其是电子邮件地址。如果您输入的电子邮件地址不正确，您将无法访问您的电子邮件地址，Amazon Web Services 账户。

### Important

由于Amazon Web Services 账户该帐户的 root 用户，我们强烈建议您使用可以由群组访问的电子邮件地址，而不是只能由个人访问。这样，如果注册了Amazon Web Services 账户离开公司，Amazon Web Services 账户仍然可以使用，因为电子邮件地址仍可访问。如果您无法访问与Amazon Web Services 账户，那么如果丢失了密码，则无法恢复对帐户的访问权限。

4. 选择个人或者专业。

### Note

个人账户和专业账户具有相同的特性和功能。

5. 输入您的公司或个人信息。

### Important

对于专业Amazon Web Services 账户，最佳做法是输入公司电话号码而不是个人电话号码。配置账户使用[Amazon Web Services 账户根用户 \(p. 29\)](#)使用个人电子邮件地址或个人电话号码可能会使您的帐户不安全。

6. 阅读并接受[Amazon客户协议](#)。

### Note

一定要阅读并理解Amazon客户协议。

7. 选择创建账户然后继续。
8. 在存储库的付款信息页面中，输入有关付款方式的信息，然后选择验证并添加。

### Note

如果您想为您的账单地址使用不同的账单地址Amazon选择账单信息使用新地址选择之前验证并添加。

在添加有效的付款方式之前，您无法继续注册过程。

9. 接下来，您必须验证您的电话号码。从列表中选择您的国家或地区代码，然后输入可在接下来几分钟内联系的电话号码。
10. 输入 CAPTCHA 中显示的代码，然后提交。
11. 当自动系统与您联系时，输入您收到的 PIN 码然后选择Continue。
12. 在存储库的选择 Support 计划页面上，选择一个可用的Amazon Web Services Support计划。有关可用 Support 计划及其优势的说明，请参阅[CompareAmazon Web Services Support计划](#)。
13. 最后，等待你的新帐户被激活。这通常需要几分钟，但可能需要长达 24 小时。

当您的账户完全激活后，您将收到一封确认电子邮件。检查您的电子邮件和垃圾邮件文件夹中的确认消息 收到此电子邮件后，您有权访问所有电子邮件后，您将拥有Amazon服务。

### Amazon CLI & SDKs

您可以在由管理的组织中创建成员账户。Amazon Organizations通过运行[CreateAccount](#)登录组织管理账户时操作。

您无法独立创建Amazon Web Services 账户在组织外部使用Amazon Command Line Interface(Amazon CLI) 或者AmazonAPI 操作。

## 查看账户标识符

Amazon将以下唯一标识符分配给每个Amazon Web Services 账户：

### Amazon Web Services 账户 (p. 8) ID

一个 12 位数字，如 123456789012，它唯一标识 Amazon Web Services 账户。许多 Amazon 资源在其 [Amazon Resource Name \(ARN\)](#) 中包含账户 ID。账户 ID 部分将一个账户中的资源与另一个账户中的资源区分开来。如果您是 Amazon Identity and Access Management (IAM) 用户，您可以登录 Amazon Web Services Management Console 使用账户 ID 或账户别名。

### 规范用户 ID (p. 9)

一个字母数字标识符，  
如 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be，这是一种混淆的形式 Amazon Web Services 账户 ID。您可以使用这个 ID 来识别 Amazon Web Services 账户使用 Amazon Simple Storage Service (Amazon S3) 授予对存储桶和对象的跨账户访问权限时。您可以检索的规范用户 ID Amazon Web Services 账户作为根用户或 IAM 用户。

您必须通过 Amazon 进行身份验证才能查看这些标识符。

#### Warning

不要提供您的 Amazon 证书（包括密码和访问密钥）发送给需要 Amazon Web Services 账户要共享的标识符 Amazon 资源与您一起。这样做将给予他们相同的访问权限 Amazon Web Services 账户您拥有的。

## 查找您的 Amazon Web Services 账户 ID

您可以找到 Amazon Web Services 账户 ID 使用 Amazon Web Services Management Console 或者 Amazon Command Line Interface (Amazon CLI)。在控制台中，账户 ID 的位置取决于您以根用户还是 IAM 用户身份登录。无论您是以根用户还是 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

#### Amazon Web Services Management Console

查找您的 Amazon Web Services 账户以根用户身份登录时的 ID

##### 最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当您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，选择您的账户名称或编号，然后选择 My Security Credentials (我的安全凭证)。
  2. 展开 Account identifiers (账户标识符) 部分。账号显示在标签旁边 Amazon Web Services 账户 ID。

#### Amazon CLI & SDKs

查找您的 Amazon Web Services 账户使用 ID Amazon CLI

##### 最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当您以 root 用户身份运行命令时，您不需要任何 IAM 权限。

使用 `get-caller-identity` 命令如下所示。

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

```
--output text  
123456789012
```

## 以 IAM 用户身份查找账户 ID

Amazon Web Services Management Console

查找您的 Amazon Web Services 账户作为 IAM 用户登录时的 ID

最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- `aws-portal:ViewAccount`

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

Tip

如果您没有看到我的安全凭证页面中，您可以以具有 IAM 角色的联合用户身份登录，而不是 IAM 用户身份登录。在这种情况下，查找条目我的账户以及旁边的账户 ID 号码。

2. 在页面顶部，下账户详细信息，账号显示在标签旁边 Amazon Web Services 账户 ID。

Amazon CLI & SDKs

查找您的 Amazon Web Services 账户使用 IDAmazon CLI

最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当您以 IAM 用户或角色身份运行命令时，您必须拥有：
  - `sts:GetCallerIdentity`

使用 `get-caller-identity` 命令如下所示。

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

## 查找的规范用户 IDAmazon Web Services 账户

您可以找到使用 Amazon Web Services Management Console 或 Amazon CLI 的 Amazon Web Services 账户的规范用户 ID。的规范用户 IDAmazon Web Services 账户特定于该账户。您可以检索的规范用户 IDAmazon Web Services 账户作为根用户、联合身份用户或 IAM 用户。

## 以根用户或 IAM 用户身份查找规范 ID

Amazon Web Services Management Console

在以根用户或 IAM 用户身份登录控制台时查找账户的规范用户 ID

最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当您以 root 用户身份运行命令时，您不需要任何 IAM 权限。
- 当您以 IAM 用户身份登录时，您必须具有：
  - `aws-portal:ViewAccount`

1. 登录到 Amazon Web Services Management Console 作为根用户或 IAM 用户。
2. 在右上角的导航栏中，选择您的账户名称或编号，然后选择 My Security Credentials (我的安全凭证)。
3. 如果您是根用户，请展开 Account identifiers (账户标识符)，并找到 Canonical User ID (规范用户 ID)。

您将会看到 Amazon 列出的账户 ID 和规范用户 ID 值。您可以使用规范用户 ID 来配置 Amazon S3 访问控制列表 (ACL)。

如果你是 IAM 用户，请在账户详细信息查找账户规范用户 ID。

### Amazon CLI & SDKs

使用查找规范用户 ID Amazon CLI

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

使用 [列出存储桶](#) 命令如下所示。

```
$ aws s3api list-buckets \  
  --query Owner.ID \  
  --output text  
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

## 以具有 IAM 角色的联合用户身份查找规范 ID

### Amazon Web Services Management Console

当以具有 IAM 角色的联合身份用户登录控制台时查找账户的规范用户 ID

最小权限

- 您必须有权列出和查看 Amazon S3 存储桶。

1. 登录到 Amazon Web Services Management Console 作为具有 IAM 角色的联合用户。
2. 在 Amazon S3 控制台中，选择存储桶名称以查看存储桶的详细信息。
3. 选择 Permissions (权限)，然后选择 Access Control List (访问控制列表)。

在页面顶部的 Access for bucket owner (存储桶拥有者的访问权限) 下，会显示 Amazon Web Services 账户的规范用户 ID。

### Amazon CLI & SDKs

使用查找规范用户 ID Amazon CLI

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

使用 [列出存储桶](#) 命令如下所示。

```
$ aws s3api list-buckets \  
  --query Owner.ID \  
  --output text
```



```
--query Owner.ID \  
--output text  
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

## 修改账户名称、电子邮件地址或密码 Amazon Web Services 账户根用户

编辑您的 Amazon Web Services 账户的名称，或者要更改根用户的密码或电子邮件地址，请执行以下过程中的步骤。使用电子邮件地址和密码以身份登录时使用 Amazon Web Services 账户根用户。

### Note

对的更改 Amazon Web Services 账户到处传播可能需要长达四个小时。

### Amazon Web Services Management Console

编辑您的 Amazon Web Services 账户名称、Root 用户密码或 Root 用户电子邮件地址

#### 最小权限

要执行以下步骤，您必须至少具有以下 IAM 权限：

- 您必须以 Amazon Web Services 账户 root 用户，不需要额外的 IAM 权限。您无法以 IAM 用户或角色身份执行这些步骤。

1. 使用您的 Amazon Web Services 账户登录的电子邮件地址和密码 [Amazon Web Services Management Console](#) 作为您的 Amazon Web Services 账户根用户。
2. 选择窗口右上角的账户名称，然后选择我的账户。
3. 在 Account Settings 页面上，选择 Account Settings 旁的 Edit。

### Note

系统可能会提示您批准访问此信息。Amazon 向与帐户关联的电子邮件地址和主要联系人电话号码发送请求。选择请求中的链接以在浏览器中打开它，然后批准访问权限。

4. 在要更新的字段的旁边，选择 Edit。
5. 输入您的更改后，选择 Save changes。
6. 完成您的所有更改后，选择完成。

### Amazon CLI & SDKs

中不支持此任务 Amazon CLI 或者通过来自其中一个的 API 操作 Amazon 开发工具包。您只能使用 Amazon Web Services Management Console。

## 添加或更新主要和备用联系人信息

您可以存储有关主账户联系人 (p. 12) 为您的 Amazon Web Services 账户。

您还可以为以下内容添加联系信息 [替代账户联系人 \(p. 12\)](#)：

- 计费
- 操作



- 安全性

## 访问或更新主账户联系人

编辑您的Amazon Web Services 账户的主要联系人详细信息，请执行以下程序中的步骤。

Amazon Web Services Management Console

编辑您的Amazon Web Services 账户的主要联系方式

### 最小权限

要执行以下步骤，您至少必须具有以下 IAM 权限：

- `aws-portal:ViewAccount` ( 要查看账户详情页面 )
- `aws-portal:ModifyAccount`

1. 登录到[Amazon Web Services Management Console](#)作为具有最低权限的 IAM 用户或角色。
2. 选择窗口右上角的账户名称，然后选择我的账户。
3. 向下滚动到部分联系信息，然后在旁边选择编辑。

### Note

系统可能会提示您批准访问此信息。Amazon向与帐户关联的电子邮件地址和主要联系人电话号码发送请求。选择请求中的链接以在浏览器中打开它，然后批准访问权限。

4. 更改任何可用字段中的值。

### Important

对于专业Amazon Web Services 账户，最佳做法是输入公司电话号码和电子邮件地址，而不是属于个人的电话号码和电子邮件地址。配置账户的[使用Amazon Web Services 账户根用户 \(p. 29\)](#)使用个人的电子邮件地址或电话号码可能会使该个人离开公司时你的帐户难以恢复。

5. 完成您的所有更改后，选择更新。

Amazon CLI & SDKs

您目前无法修改Primary使用联系信息Amazon CLI或者来自其中一个的 API 操作Amazon开发工具包。您只能通过使用Amazon Web Services Management Console。

## 访问或更新备用联系人

您可以添加和删除备用联系人Amazon Web Services 账户更新联系人的详细信息。

主题

- [操作模式 \(p. 12\)](#)
- [授予权限以更新替代联系人员 \(p. 13\)](#)
- [访问和更新账户的备用联系人详细信息 \(p. 15\)](#)

## 操作模式

使用的 API 操作Amazon Web Services 账户的备用联系人始终以两种操作模式之一工作：

- 独立上下文— 当帐户中的用户或角色访问或更改其他联系人时，使用此模式同一账户。当您会自动使用独立上下文模式不要包含AccountID当你调用账户管理之一的参数Amazon CLI或者AmazonSDK 操作。
- Organizations 上下文— 当组织中一个帐户中的用户或角色访问或更改同一组织中不同成员帐户中的备用联系人时，使用此模式。当您会自动使用组织上下文模式Do包含AccountID当你调用账户管理之一的参数Amazon CLI或者AmazonSDK 操作。在此模式下，您只能从组织的管理帐户或账户管理的委派管理帐户调用操作。

这些区域有：Amazon Web Services Management Console下面的过程总是有效仅限在独立上下文中。您可以使用Amazon Web Services Management Console要仅访问或更改您使用的帐户中的备用联系人，请调用该操作。

这些区域有：Amazon CLI和AmazonSDK 操作可以在任何一种情况下工作。

- 如果您不要包含AccountID参数，然后操作在独立上下文中运行，并自动将请求应用于您用于发出请求的帐户。无论账户是否为组织成员，都是如此。
- 如果你确实包含AccountID参数，然后该操作在 Organizations 上下文中运行，该操作在指定的组织帐户上运行。
  - 如果调用该操作的帐户是账户管理服务的管理帐户或委派管理员帐户，则可以在AccountID参数以更新指定的账户。
  - 组织中唯一可以调用其他联系人操作之一并在AccountID参数是指定为[委托管理员账户 \(p. 36\)](#)用于账户管理服务。包括管理账户在内的任何其他账户都会收到AccessDenied例外。
- 如果您在独立模式下运行操作，则必须允许您使用 IAM 策略运行该操作，该策略包括Resource任何一个元素"\*"允许所有资源，或者[使用独立账户语法的 ARN \(p. 13\)](#)。
- 如果您在组织模式下运行操作，则必须允许您使用 IAM 策略运行该操作，该策略包括Resource任何一个元素"\*"允许所有资源，或者[使用组织中成员账户语法的 ARN \(p. 13\)](#)。

## 授予权限以更新替代联系人员

和大多数人一样Amazon操作，您可以授予添加、更新或删除备用联系人的权限Amazon Web Services 账户使用IAM 权限策略。当您IAM 权限策略附加到IAM 委托人（用户或角色）时，您可以指定委托人可在哪些条件下对哪些资源执行哪些操作。

以下是创建权限策略的一些账户管理特定注意事项。

### 的 Amazon 资源名称格式Amazon Web Services 账户

- 这些区域有：[Amazon 资源名称 \(ARN\)](#)为了Amazon Web Services 账户你可以包含在resource根据您要引用的账户是独立账户还是组织中的账户，策略声明的元素的构造方式有所不同。请参阅上一部分[操作模式 \(p. 12\)](#)。

- 独立账户的账户 ARN：

```
arn:aws:account::{AccountID}:account
```

在独立模式下运行备用联系人操作时，必须使用此格式，方法是不包括AccountID参数。

- 组织中成员账户的账户 ARN：

```
arn:aws:account::{ManagementAccountID}:account/o-{OrganizationID}/{AccountID}
```

在组织模式下运行备用联系人操作时，必须使用此格式，方法是将AccountID参数。

## IAM 策略的上下文密钥

账户管理服务还提供了几个[特定于账户管理服务的条件键](#) (p. 51)这可以对您授予的权限进行精细控制。

### `account:AlternateContactTypes`

上下文键`account:AlternateContactTypes`允许您指定 IAM 策略允许 (或拒绝) 三种账单类型中的哪种。

例如, 以下示例 IAM 权限策略使用此条件密钥允许附加的委托人仅检索但不能修改BILLING组织中特定账户的备用联系人。

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "account:GetAlternateContact",
      "Resource": [
        "arn:aws:account::123456789012:account/o-aa111bb222/11111111111"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "account:AlternateContactTypes": [
            "BILLING"
          ]
        }
      }
    }
  ]
}
```

### `account:AccountResourceOrgPaths`

上下文键`account:AccountResourceOrgPaths`允许您指定通过组织层次结构到特定组织单位 (OU) 的路径。只有该 OU 包含的成员账户才符合条件。以下示例代码段将策略限制为仅应用于两个指定 OU 中的任何一个账户。

由于`account:AccountResourceOrgPaths`是多值字符串类型, 必须使用[ForAnyValue](#)或者[ForAllValues](#)多值字符串运算符。另外, 请注意, 条件键上的前缀是`account`, 尽管你正在引用组织中的 OU 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中账户的标签。标签是一个键/值字符串对, 您可以使用它对账户中的资源进行分类和标记。有关标记的更多信息, 请参阅[标签编辑器](#)中的 Amazon Resource Groups 用户指南。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[什么是适用于的 ABAC](#) Amazon 中的 IAM 用户指南。以下示例代码段将策略限制为仅应用于组织中具有带有密钥的标签的帐户 `project` 值为 `blue` 或者 `red`。

由于 `account:AccountResourceOrgTags` 是多值字符串类型，必须使用 [ForAnyValue](#) 或者 [ForAllValues](#) 多值字符串运算符。另外，请注意，条件键上的前缀是 `account`，尽管你在引用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。你不能将标签附加到独立的 Amazon Web Services 账户。

## 访问和更新账户的备用联系人详细信息

编辑您的 Amazon Web Services 账户的备用联系人详细信息，请执行以下程序中的步骤。

### Amazon Web Services Management Console

编辑您的 Amazon Web Services 账户的备用联系方式

#### 最小权限

要执行以下步骤，您至少必须具有以下 IAM 权限：

- `aws-portal:ViewAccount` ( 要查看账户详情页面 )

您还必须具有以下权限选项之一：

以下权限允许用户执行任何或全部备用联系人命令：

- `aws-portal:ModifyAccount`

1. 登录到 [Amazon Web Services Management Console](#) 作为具有最低权限的 IAM 用户或角色。
2. 选择窗口右上角的账户名称，然后选择我的账户。
3. 在存储库的账户设置页面，向下滚动到替代联系人，然后在标题的右侧，选择编辑。

#### Note

系统可能会提示您批准访问此信息。Amazon 向与帐户关联的电子邮件地址和主要联系人电话号码发送请求。选择请求中的链接以在浏览器中打开它，然后批准访问权限。

4. 更改任何可用字段中的值。

#### Important

对于专业 Amazon Web Services 账户，最佳做法是输入公司电话号码和电子邮件地址，而不是属于个人的电话号码和电子邮件地址。

5. 完成您的所有更改后，选择更新。

### Amazon CLI & SDKs

您可以检索、更新或删除替代联系信息可以通过使用以下方式 Amazon CLI 命令或他们的 Amazon SDK 等效操作：

- [获取替代联系人](#)
- [PutAlternateContact](#)
- [删除替代联系人](#)

### Notes

- 要从管理帐户或组织中的委托管理员帐户对成员账户执行这些操作，您必须为[账户服务启用可信访问](#)。
- 您无法访问与用于调用该操作的帐户不同的组织中的帐户。

### 最小权限

对于每个操作，您都必须具有映射到该操作的权限：

- `account:GetAlternateContact`
- `account:PutAlternateContact`
- `account>DeleteAlternateContact`

如果您使用这些个人权限，则可以授予某些用户只读取联系人信息的能力，并授予其他用户读取和写入的能力。

这些区域有：`aws-portal`权限仅适用于Amazon Web Services Management Console，且不能用于授予权限Amazon CLI或者AmazonSDK 操作。

### Example

以下示例检索来电者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

以下示例还检索当前账单备用联系人，但这次检索组织中指定的成员账户。使用的凭证必须来自组织的管理帐户，或者来自账户管理的委派管理员帐户。

```
$ 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

以下示例为呼叫者账户设置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

以下示例还设置了 Operations 备用联系人，但这次是为组织中指定的成员帐户设置的。使用的凭证必须来自组织的管理帐户，或者来自账户管理的委派管理员帐户。

```
$ 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

如果你执行多个PutAlternateContact同样的操作Amazon Web Services 账户和相同的联系人类型，第一个添加新的联系人，以及所有连续的呼叫都是相同的Amazon Web Services 账户然后联系人类型更新现有联系人。

### Example

以下示例删除呼叫者帐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

如果您尝试多次删除同一联系人，第一个联系人将以静默方式成功。以后的所有尝试都会生成ResourceNotFound例外。

### Example

以下示例还删除了 Security 备用联系人，但这次删除组织中指定的成员帐户。使用的凭证必须来自组织的管理帐户，或者来自账户管理的委派管理员帐户。

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

```
--alternate-contact-type=SECURITY
```

如果成功，此命令不会产生任何输出。

## 设置或更改安全挑战问题

您可以通过将安全质询问题及其答案添加到您的账户中来提高账户的安全性。Amazon Web Services 账户 .Amazon 当你需要联系时，可以使用信息来帮助验证你是账户所有者 Amazon Web Services Support 寻求帮助。

要选择安全质询问题并提供答案，请执行以下程序中的步骤。

Amazon Web Services Management Console

要添加或编辑您的安全质询问题 Amazon Web Services 账户

最小权限

要执行以下步骤，您必须至少具有以下 IAM 权限：

- `aws-portal:ViewAccount` ( 要查看账户详情页面 )
- `aws-portal:ModifyAccount`

1. 登录到 [Amazon Web Services Management Console](#) 因为要么 Amazon Web Services 账户 root 用户或具有最低权限的 IAM 用户或角色。
2. 选择窗口右上角的账户名称，然后选择我的账户。
3. 向下滚动到部分配置安全挑战问题然后选择编辑。

Note

系统可能会提示您批准访问此信息。Amazon 向与帐户关联的电子邮件地址和主要联系人电话号码发送请求。选择请求中的链接以在浏览器中打开它，然后批准访问权限。

4. 更改任何可用字段中的值。您可以选择提供的任何问题，然后输入适当的答案。

Important

对于专业 Amazon Web Services 账户，最佳做法是选择通用安全挑战响应 #n。  
对于每个问题，请键入一个值，例如长的随机字符串。请务必记录并安全存储此信息的副本，以便账户管理员可以在需要时检索该信息。

5. 完成您的更改后，选择更新。

Amazon CLI & SDKs

中不支持此任务 Amazon CLI 或者通过来自其中一个的 API 操作 Amazon 开发工具包。您只能使用 Amazon Web Services Management Console。

## 指定哪个 Amazon Web Services 区域你的账户可以使用

Amazon 最初启用了所有新的 Amazon Web Services 区域默认情况下，这使得您的用户能够在任何区域中创建资源。现在，什么时候 Amazon 默认情况下禁用新区域。如果希望用户能够在新区域中创建资源，请启用该区域。



## Important

Amazon 建议使用区域 Amazon Security Token Service (Amazon STS) 终端节点，而不是全局终端节点，以减少延迟。来自区域的会话令牌 Amazon STS 终端节点完全有效 Amazon 地区。如果您使用区域 Amazon STS 终端节点，您无需进行任何更改。

但是，来自全球 Amazon STS 终端节点 (<https://sts.amazonaws.com>) 仅在 Amazon Web Services 区域默认情况下启用或默认情况下启用。如果您打算为账户启用新区域，您可以使用区域中的会话令牌。Amazon STS 端点或激活全局 Amazon STS 终端节点以发出全部有效的会话令牌 Amazon Web Services 区域。在所有区域中都有效的会话令牌都会更大。如果存储会话令牌，这些较大的令牌可能会影响您的系统。

有关如何的更多信息 Amazon STS 终端节点 Amazon 地区，请参阅 [管理 Amazon STS 在 Amazon 区域](#)。

### 启用和禁用的注意事项 Amazon Web Services 区域

- 您可以使用 IAM 权限来控制对区域的访问

Amazon Identity and Access Management (IAM) 包含三个权限，可让您控制哪些用户可以启用、禁用和列出区域。有关更多信息，请参阅 [Billing and Cost Management 操作策略](#) 中的 Amazon Billing and Cost Management 用户指南。

- 启用区域是免费的

启用区域是免费的。您只需为在新区域中创建的资源付费。

- 禁用区域会禁用对区域中资源的访问

如果禁用仍包含的区域 Amazon 资源，如 Amazon Elastic Compute Cloud (Amazon EC2) 实例，您将无法访问该区域中的资源。例如，您无法使用 Amazon Web Services Management Console 或任何编程方法来查看或更改禁用区域中任何 EC2 实例的配置。

- 如果禁用区域，会继续收取活动资源费用

如果禁用仍包含的区域 Amazon 资源，这些资源费用（如果有）将继续按标准费率计算。例如，如果禁用包含 Amazon EC2 实例的区域，则即使实例不可访问，您仍然必须为这些实例支付费用。

- 禁用区域的结果并不总是立即可见

如果禁用区域，则更改需要一些时间才能在所有可能的终端节点中可见。禁用区域可能需要几秒到几分钟才能生效。

- 默认情况下启用原始区域

原始 Amazon Web Services 区域（在我们添加启用和禁用区域的能力之前存在的区域）都会默认启用，且无法禁用。有关更多信息，请参阅 [管理 Amazon Web Services 区域](#) 中的 Amazon 一般参考。

- 对于大多数账户，启用区域需要几分钟时间

启用区域通常会在几分钟内生效，但某些账户可能需要更长时间。如果启用区域的时间超过九个小时，请在 [Amazon Web Services Support Center](#) 然后使用打开一个案例 Amazon Web Services Support。

请使用以下过程启用或禁用 Amazon Web Services 区域对于中的用户 Amazon Web Services 账户。

### Amazon Web Services Management Console

要修改哪些 Amazon Web Services 区域可以通过 Amazon Web Services 账户

#### 最小权限

要执行以下过程中的步骤，IAM 用户或角色必须具有以下权限：

- `aws-portal:ViewAccount`（需要查看账户详情页面）
- `account:ListRegions`（需要查看列表）Amazon Web Services 区域以及它们当前是启用还是禁用）。



- `account:EnableRegion`
- `account:DisableRegion`

1. 登录到[Amazon Web Services Management Console](#)因为要么Amazon Web Services 账户根用户或具有最低权限的 IAM 用户或角色。
2. 在窗口右上角选择您的账户名称，然后选择我的账户。
3. 在存储库的账户设置页面上，向下滚动到部分Amazon Web Services 区域。

#### Note

系统可能会提示您批准访问此信息。Amazon向与帐户关联的电子邮件地址和主要联系人电话号码发送请求。选择请求中的链接以在浏览器中打开它，然后批准访问权限。

4. 在每个旁边Amazon Web Services 区域有一个选项操作列中，选择任一启用或者禁用这取决于您是否希望账户中的用户能够在该区域中创建和访问资源。
5. 如果出现提示，确认您的选择。
6. 完成您的所有更改后，选择更新。

#### Amazon CLI & SDKs

中不支持此任务Amazon CLI或者通过来自其中一个的 API 操作Amazon开发工具包。您只能使用Amazon Web Services Management Console。

## 设置或更改Amazon Web Services 账户alias

这些区域有：Amazon Web Services 账户根用户和Amazon Identity and Access Management(IAM) 账户中的用户使用 Web URL 登录。

如果您希望在 IAM 用户的 URL 用贵公司名称（或其他易于记住的标识）取代Amazon Web Services 账户ID，你可以创建账户别名。本节介绍以下信息：Amazon Web Services 账户列出可用于创建别名的 API 操作。

您的账户 IAM 用户的登录页面 URL 地址默认格式如下：

```
https://Your_Account_ID.signin.aws.amazon.com/console/
```

如果你创建Amazon Web Services 账户为您的别名Amazon Web Services 账户ID，IAM 用户登录页面 URL 地址类似以下示例。

```
https://Your_Account_Alias.signin.aws.amazon.com/console/
```

包含您的原始 URLAmazon Web Services 账户ID 仍然有效，创建 ID 后仍可以使用Amazon Web Services 账户别名。

#### Tip

要在 Web 浏览器中为您的账户登录页面创建书签，我们建议您在标签条目中手动键入登录 URL。请勿使用 Web 浏览器的“将此页标记为书签”功能，因为这可以捕获许多仅与您当前浏览器会话有关的信息。这些信息可能会干扰将来对该页面的访问。

#### Considerations

- 您的Amazon Web Services 账户只能有一个别名。如果为您的创建新别名Amazon Web Services 账户，新别名将覆盖之前的别名。包含之前别名的 URL 停止工作。
- 账户别名必须在所有 Amazon Web Services 产品中唯一。它必须仅包含小写字母、数字和连字符。

# 创建、删除和查看Amazon Web Services 账户alias

## Amazon Web Services Management Console

### 创建或编辑账户别名

#### 最小权限

要执行以下步骤，您必须至少具有以下 IAM 权限：

- iam:ListAccountAliases
- iam:CreateAccountAlias

1. 登录到[Amazon Web Services Management Console](#)因为要么Amazon Web Services 账户作为具有最低权限的 IAM 用户或角色。
2. 打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
3. 在导航窗格中，选择 Dashboard (控制面板)。
4. 在右侧窗格中Amazon Web Services 账户，对于此账户中 IAM 用户的登录 URL，选择自定义。如果别名已存在，则选择编辑。
5. 适用于首选别名，输入要用于别名的名称，然后选择保存更改。

#### Note

您的别名只能与您的Amazon Web Services 账户一次。如果创建新别名，原有别名将被删除，与原有别名关联的登录 URL 将失效。

### 删除账户别名

#### 最小权限

要执行以下步骤，您必须至少具有以下 IAM 权限：

- iam:ListAccountAliases
- iam:CreateAccountAlias
- iam>DeleteAccountAlias

1. 登录到[Amazon Web Services Management Console](#)因为要么Amazon Web Services 账户作为具有最低权限的 IAM 用户或角色。
2. 打开 IAM 控制台：<https://console.aws.amazon.com/iam/>。
3. 在导航窗格中，选择 Dashboard (控制面板)。
4. 在右侧窗格中Amazon Web Services 账户，对于此账户中 IAM 用户的登录 URL，选择Delete。

## Amazon CLI & SDKs

您可以使用以下 SDK API 操作或其中的创建、更新或删除账户别名。Amazon CLI等效函数：

- [ListAccountAliases](#)  

```
aws iam list-account-aliases
```
- [CreateAccountAlias](#)  

```
aws iam create-account-alias
```
- [DeleteAccountAlias](#)

```
aws iam delete-account-alias
```

### 最小权限

要执行以下步骤，您必须至少具有以下 IAM 权限：

- iam:ListAccountAliases
- iam:CreateAccountAlias
- iam>DeleteAccountAlias

要显示您的 Amazon Web Services 账户运行 ID 别名，请运行以下命令。

```
$ aws iam list-account-aliases
{
  "AccountAliases": [
    "myaccountalias"
  ]
}
```

要为您的创建别名 Amazon Web Services Management Console 运行以下命令：

```
$ aws iam create-account-alias \
  --account-alias myaliasname
```

如果成功，此命令不会产生任何输出。

删除 Amazon Web Services 账户运行 ID 别名，请运行以下命令。

```
$ aws iam delete-account-alias \
  --account-alias bisdavid
```

如果成功，此命令不会产生任何输出。

## 关闭您的 Amazon Web Services 账户

在本指南中，我们仅使用该术语 Closed 一个 Amazon Web Services 账户而不是 deleting 一个账户。的一些元素 Amazon Web Services 账户在所有账户中都是独一无二的，使用“删除”一词可能会错误地意味着其中一些元素可供将来重复使用。例如，已关闭的账户 ID Amazon Web Services 账户为永远不出于明显的安全原因重复使用。

只有 Amazon Web Services 账户 root 用户可以关闭 Amazon Web Services 账户。Amazon 无法代表您关闭账户。如果您对过程有任何问题，请联系您的客户代表或联系 Amazon Web Services Support 请帮助。有关联系的更多信息 Amazon Web Services Support 请参阅 [联系 Amazon Web Services Support](#)。

### Important

网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的 Amazon Web Services 账户 ID 号码是永远不账户关闭后重复使用。这有助于防止否则会发生的安全风险。例如，考虑是否在 Amazon Identity and Access Management (IAM) 权限策略和 ID 突然引用了一个不同且意想不到的 Amazon Web Services 账户。

### 主题

- [在您关闭 Amazon Web Services 账户 之前的注意事项 \(p. 23\)](#)
- [排除关闭时的错误 Amazon Web Services 账户 \(p. 24\)](#)
- [关闭您的 Amazon Web Services 账户 \(p. 25\)](#)
- [访问您的 Amazon Web Services 账户关闭它之后 \(p. 25\)](#)
- [后关闭期之后 \(p. 25\)](#)

## 在您关闭 Amazon Web Services 账户 之前的注意事项

在您关闭 Amazon Web Services 账户 之前，请考虑以下事项：

### 您与 Amazon 的协议

关闭您的 Amazon Web Services 账户用于向我们发出您想要取消的通知 Amazon 与客户协议或其他协议。Amazon 管理着您的 Amazon Web Services 账户，完全是关于这个具体 Amazon Web Services 账户。如果您重新打开 Amazon Web Services 账户在后关闭期（在您关闭账户后的 90 天内），则您同意相同的协议条款管辖您通过重新打开的过程访问和使用此服务产品的过程。Amazon Web Services 账户。

### Amazon Web Services Management Console 访问

您可以访问 Amazon Web Services Management Console 对于关闭 Amazon Web Services 账户受到限制。在后关闭期，您仍可以登录您的 Amazon Web Services 账户 以查看您过往的账单信息并访问 Amazon Web Services Support。在关闭的账户中，您不能访问任何其他 Amazon 服务或启动任何新的 Amazon 服务。

### 现有内容和服务仍在使用

在后关闭期之后，Amazon 自动删除您中的所有剩余内容 Amazon Web Services 账户，并终止任何 Amazon 仍在使用的服务。您应从账户中检索所有内容，然后再关闭您的账户。有关如何检索您的内容的说明，请参阅该服务的相关文档。有关后关闭期的更多信息，请参阅 [访问您的 Amazon Web Services 账户关闭它之后 \(p. 25\)](#)。

### 您的付款方式

我们会通过您指定的付款方式，向您收取在关闭 Amazon Web Services 账户 之前产生的任何使用费用。我们向您发放可能通过相同的付款方式到期的任何退款。如果您有有效的订阅（例如您按月支付的预留实例），那么即使在您的账户关闭之后，仍可能会通过指定付款方式继续针对这些订阅向您收费，直至订阅到期或根据管辖这些订阅的条款出售为止。这些收费和退款可能在您的账户关闭后发生。

此外，如果您重新打开您的账户，您可能需要支付运行费用 Amazon 在后关闭期内的服务（您关闭账户之前未停止的服务）。关闭您的 Amazon Web Services 账户 不会影响您在 Amazon.com 或其他亚马逊网站上使用的付款方式。

### 按需收费

在后关闭期内，按需收费服务的计费会停止。但是，对于在您关闭账户之前累积的任何使用量，您均需支付费用。您将需要在下个月初支付该使用费用。此外，如果您购买了具有持续支付义务的任何订阅，您可能要在账户关闭后继续为其付费。

#### Important

如果不停止或删除资源，您将继续产生成本。

### 注册到 Amazon Route 53 的域

系统不会自动删除注册到 Route 53 的域。当您关闭 Amazon Web Services 账户，您有三种选择：

- 您可以禁用自动续订，并且在注册期到期时自动删除这些域。有关更多信息，请参阅 [Amazon Route 53 开发人员指南中的为域启用或禁用自动续订](#)。
- 您可以将这些域转移到另一个 Amazon Web Services 账户。有关更多信息，请参阅 [将域转移到其他 Amazon Web Services 账户](#)。
- 您可以将这些域转移到另一个域注册商。有关更多信息，请参阅 [将域从 Route 53 转移到另一个注册商](#)。

如果您已关闭了账户，可以使用 Amazon Web Services Support 提交一个案例，以便获得有关禁用自动续订或转移您的域的帮助。有关更多信息，请参阅 [针对域注册问题联系 Amazon Web Services Support](#)。针对域注册问题提交案例时，不收取任何费用。

## 如果您重新打开 Amazon Web Services 账户，则会向您收取费用

如果您重新打开 Amazon Web Services 账户在后关闭期内，您可能需要支付任何费用 Amazon 在关闭帐户之前没有停止的服务或未删除的资源。

### Example

你重新打开你的 Amazon Web Services 账户关闭后 30 天。您的 Amazon Web Services 账户只有一个活跃 t2.micro 关闭时的 Amazon EC2 实例。在这个例子中，假设一下 t2.micro 您的中的 Amazon EC2 实例 Amazon Web Services 区域是每小时 0.01 美元。这种情况下，您可能需要为您的 Amazon 服务支付以下费用：30 天 x 24 小时 x 每小时 0.01 美元 = 7.20 美元。

## 关闭成员账户

关闭使用创建的账户时 Amazon Organizations，该账户不会从组织中删除，直到后关闭期间结束为止。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制，请在关闭组织之前，从该组织中删除成员账户。有关更多信息，请参阅 [Amazon Organizations 用户指南中的关闭 Amazon Web Services 账户](#)。

## 对您正关闭的账户的跨账户访问

在您关闭 Amazon Web Services 账户，对已关闭账户的任何访问请求 Amazon 来自其他的服务 Amazon Web Services 账户失败。即使您已向其他账户授予访问您账户的 Amazon 服务的权限，也是如此。如果您重新打开 Amazon Web Services 账户其他 Amazon Web Services 账户可以再次访问你的账户 Amazon 如果您向另一方授予了必要的权限，则服务和资源 Amazon Web Services 账户。

## 删除 Amazon VPC 对等连接

Amazon 当您关闭参与 VPC 对等连接的账户之一时，不删除 Amazon Virtual Private Cloud (Amazon VPC) 对等连接。来自其他活动账户的所有发往 VPC 对等连接的流量都将被丢弃，原因是 Amazon 终止实例并删除已关闭账户中的所有安全组。要删除 VPC 对等连接，请使用 Amazon VPC 控制台将其从您的账户中删除，Amazon Command Line Interface (Amazon CLI) 或 Amazon EC2 API。有关更多信息，请参阅 [删除 VPC 对等连接](#)

## 排除关闭时的错误 Amazon Web Services 账户

如果您在尝试关闭时收到错误消息 Amazon Web Services 账户您可以联系您的客户代表或联系您的客户 Amazon Web Services Support 开立账单或帐户支持案例以寻求帮助。您可能无法关闭您的常见原因 Amazon Web Services 账户中支持的脚本编写选项如下：

- 您的账户是中组织的管理账户 Amazon Organizations 拥有活跃的会员账户。要关闭管理账户，您必须先从中组织中删除所有成员账户。
- 您的账户有未支付的发票。

- 您未以 Amazon Web Services 账户根用户。
- 您是活跃的 Amazon Web Services Marketplace 卖家。

## 关闭您的 Amazon Web Services 账户

您可以通过以下步骤关闭您的 Amazon Web Services 账户。

Amazon Web Services Management Console

关闭您的 Amazon Web Services 账户

### 最小权限

要执行以下步骤，您必须至少具有以下 IAM 权限：

- 您必须以具有以下权限的用户或角色身份登录：
  - `portal:ModifyAccount`

1. 以具有在 Amazon Web Services 账户要关闭的。
2. 打开位于 <https://console.amazonaws.cn/billing/home#/> 处的“账单和成本管理”控制台。
3. 在右上角的导航栏中，选择账户名称（或别名），然后选择 My Account (我的账户)。
4. 在 Account Settings 页面上，滚动至页面底端的 Close Account 部分。阅读并确保您理解复选框旁的文本内容。关闭 Amazon Web Services 账户后，您无法再使用它来访问 Amazon 服务。
5. 选中此复选框以接受这些条款，然后选择 Close Account。
6. 在确认对话框中，选择 Close Account。

Amazon CLI & SDKs

中不支持此任务 Amazon CLI 或者通过来自其中一个的 API 操作 Amazon 开发工具包。您只能使用 Amazon Web Services Management Console。

## 访问您的 Amazon Web Services 账户关闭它之后

关闭 Amazon Web Services 账户后，您无法再使用它来访问 Amazon 服务。但是，在关闭账户后的 90 天内（称为后关闭期），您可以查看过去的账单信息 Amazon Web Services 账户和访问 [Amazon Web Services Support](#)。

在后关闭期内，Amazon 可能会保留任何你没删除的内容以及任何 Amazon 在关闭之前你没有停止的服务 Amazon Web Services 账户。您只能通过关闭后期间重新开立账户来访问任何剩余内容或 Amazon 服务。

您可以通过与 [Amazon Web Services Support](#) 联系以重新打开 Amazon Web Services 账户。如果你选择重新打开帐户，你可以访问你没有删除的内容，Amazon 关闭账户之前未停止的服务，但您可能要为您支付运行这些服务的费用。Amazon 后关闭期内的服务。您可以估算运行成本 Amazon 通过使用 [Amazon Pricing Calculator](#) 中的 Amazon Pricing Calculator 用户指南。

## 后关闭期之后

后关闭期之后，Amazon 永久关闭您的 Amazon Web Services 账户，你再也不能重新打开它了。您未删除的任何内容都会被永久删除，Amazon 你没停止的服务已停止。服务属性可以根据计费和管理目的的要求保留。



您无法创建新的 Amazon Web Services 账户使用注册到您的相同别名或电子邮件地址 Amazon Web Services 账户在其关闭时。

## 为您的账单 Amazon Web Services 账户

对于与您的账单相关的程序和任务 Amazon Web Services 账户，请参阅中的以下主题 [Amazon Billing and Cost Management 用户指南](#)：

- [更改您用来支付账单的货币](#)
- [更新和删除税务登记号码](#)
- [启用税务设置继承](#)

## 管理印度的账户

如果您注册新的 Amazon Web Services 账户并选择印度作为您的联系地址，您将与亚马逊互联网服务私人有限公司 (AISPL) 签订您的用户协议，该公司 Amazon India 的卖家管理您的账单，您的发票总额将以印度卢比 (INR) 而非美元 (美元) 列出。在您通过 AISPL 创建账户之后，便无法更改联系信息中的国家/地区。

如果您有现有的 Amazon Web Services 账户使用印度地址，您的账户要么是 Amazon 或者 AISPL，具体取决于你开立账户的时间。要了解您的账户是 Amazon 或者 AISPL，请参阅 [Determining which company your account is with \(p. 26\)](#)。如果您是现有 Amazon 客户，则可继续使用 Amazon Web Services 账户。你也可以选择同时拥有 Amazon Web Services 账户和 AISPL 账户，不过它们无法整合到同一个账户中 Amazon 组织。有关管理 Amazon Web Services 账户，请参阅 [管理 Amazon Web Services 账户 \(p. 6\)](#)。

如果您的账户使用 AISPL 账户，请执行本主题中的过程来管理您的账户。本主题介绍如何注册 AISPL 账户、编辑有关您的 AISPL 账户的信息以及添加或编辑您的永久账号 (PAN)。

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

主题

- [确定您的账户所属的公司 \(p. 26\)](#)
- [创建 Amazon Web Services 账户使用 AISPL \(p. 27\)](#)
- [管理您的 AISPL 账户 \(p. 27\)](#)

## 确定您的账户所属的公司

Amazon 服务是由 Amazon 和 AISPL 共同提供的。使用以下过程可确定您的账户所属的销售方。

Amazon Web Services Management Console

确定您的账户所属的公司

最小权限

要执行以下步骤，您必须至少具有以下 IAM 权限：

- 此过程不需要特殊权限。

1. 打开 Amazon Web Services Management Console ([Amazon Web Services Management Console](#))。

2. 在页脚中，查看版权声明。如果版权归亚马逊云科技所有，则您的账户属于 Amazon。如果版权归 Amazon Internet Services Private Ltd. 所有，则您的账户属于 AISPL。

#### Amazon CLI & SDKs

中不支持此任务 Amazon CLI 或者通过来自其中一个的 API 操作 Amazon 开发工具包。您只能使用 Amazon Web Services Management Console。

## 创建 Amazon Web Services 账户使用 AISPL

AISPL 是的一家当地销售方 Amazon 在印度。如果您的联系地址在印度，可使用以下过程注册 AISPL 账户。

#### Amazon Web Services Management Console

##### 注册 AISPL 账户

###### 最小权限

要执行以下步骤，您必须至少具有以下 IAM 权限：

- 因为此操作发生在您有 Amazon Web Services 账户，此操作无需使用 Amazon 权限。

1. 打开 [Amazon Web Services Management Console](#)，然后选择登录控制台。
2. 在存储库的登录页中，输入您要使用的电子邮件地址。
3. 在您的电子邮件地址下，选择 I am a new user，然后选择 Sign in using our secure server。
4. 对于每个登录凭证字段，输入您的信息，然后选择创建账户。
5. 对于每个联系信息字段，输入您的信息。
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 Create Account and Continue。
7. 在 Payment Information 页上，输入要使用的付款方式。
8. 下 PAN 信息，选择否如果您没有永久账号 (PAN) 或需要以后添加此账号，请在以后添加此账号。如果您有 PAN 并且希望立即添加它，请选择是，然后在平移字段输入你的 PAN。
9. 选择 Verify Card and Continue。您必须在验证过程中提供 CVV。在验证过程中，AISPL 将对您的卡收取 2 INR。AISPL 将在验证完成后退回 2 INR。
10. 适用于提供电话号码中，输入您的电话号码。如果您有电话分机号，请在分机号中，输入你的电话分机号码。
11. 选择 Call Me Now。稍等一段时间后，您的屏幕上将显示一个四位数的 PIN。
12. 接受来自 AISPL 的自动呼叫。在您的电话键盘上，输入屏幕上显示的四位数的 PIN。
13. 在自动呼叫验证您的联系电话之后，选择 Continue to Select Your Support Plan。
14. 在 Support Plan 页面上，选择您的支持计划，然后选择 Continue。在验证您的付款方式并激活账户后，您将收到一封确认激活账户的电子邮件。

#### Amazon CLI & SDKs

中不支持此任务 Amazon CLI 或者通过来自其中一个的 API 操作 Amazon 开发工具包。您只能使用 Amazon Web Services Management Console。

## 管理您的 AISPL 账户

除了以下任务外，管理账户的程序与在印度境外创建的账户相同。请参阅 [管理 Amazon Web Services 账户 \(p. 6\)](#)。



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

- [添加或编辑永久账号 \(PAN\)](#)
- [编辑多个永久账号 \(PAN\)](#)
- [编辑多个商品和服务税识别号 \(GST\)](#)
- [查看税务发票](#)

# 使用 Amazon Web Services 账户根用户

当您首次创建亚马逊科技 (Amazon) 账户时，最初使用的是一个对账户中所有 Amazon 服务和资源具有完全访问权限的单点登录身份。这个身份就是 Amazon Web Services 账户根用户。您可以使用在创建账户所用的电子邮件地址和密码以根用户身份登录。

## Important

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

您可以更改根用户密码，并为根用户创建、轮换、停用或删除访问密钥（访问密钥 ID 和秘密访问密钥）。拥有 root 用户凭据的任何人 Amazon Web Services 账户可以无限制地访问您账户中的所有资源，包括账单信息。

您可以前往 [Security Credentials](#) 页面更改电子邮件地址和密码。您还可以选择 Amazon 登录页面上的 [Forgot password?](#) 来重置您的密码。

本节中的主题

- [以 Amazon Web Services 账户根用户 \(p. 29\)](#)
- [在上激活 MFA Amazon Web Services 账户根用户 \(p. 30\)](#)
- [更改根用户的密码 \(p. 30\)](#)
- [创建和删除的访问密钥 Amazon Web Services 账户根用户 \(p. 31\)](#)
- [比较 Amazon Web Services 账户根用户证书和 IAM 用户证书 \(p. 33\)](#)
- [需要根用户凭证的任务 \(p. 34\)](#)

## 以 Amazon Web Services 账户根用户

建议您登录您的 Amazon Web Services 账户只有在需要执行时才作为 root 用户 [只能由 root 用户执行的任务 \(p. 34\)](#)。

Amazon Web Services Management Console

要以根用户身份登录，请导航到 [控制台登录页面](#)。

如果你看到要求的文本框账户 ID、IAM 用户名，和密码，然后您之前已使用以下方式登录到控制台 [IAM 用户凭证](#)。您的浏览器可能会记住此首选项，并在您每次尝试登录时打开此账户特定的登录页面。您不能使用此版本的登录页面以根用户身份登录。如果您看到登录页面的 IAM 用户版本，请选择使用 root 用户电子邮件登录在页面底部以返回主登录页面。从那里，您可以选择使用根用户身份登录 Amazon Web Services 账户电子邮件地址和密码。

如果您的账户的根用户激活了多重身份验证 (MFA)，则接下来会提示您从您的设备输入一次性密码。

Amazon CLI & SDKs

使用 Amazon CLI 或者以账户的根用户身份从 SDK 运行 API 操作，您必须首先拥有访问 [key pair](#) 形式的凭据。然后您可以在 [你的中使用那些 Amazon CLI 或 SDK 配置文件 \(例如 Python 和 Boto3\)](#) 对您的请求进行身份验证。

### Warning

作为最佳实践，我们强烈建议您这样做。不创建根用户的访问密钥对。[只有少数任务需要 root 用户 \(p. 34\)](#)，而且您通常不经常执行这些任务，我们建议您登录 Amazon Web Services Management Console 然后在那里执行任务。

要为根用户创建访问密钥，请参阅。[创建和删除的访问密钥 Amazon Web Services 账户根用户 \(p. 31\)](#)。

## 在上激活 MFA Amazon Web Services 账户根用户

要提高根用户凭证的安全性，我们建议您遵循为您的应用程序激活多重身份验证 (MFA) 的安全最佳实践。Amazon Web Services 账户。由于根用户可以在您的账户中执行敏感操作，因此添加此额外一层身份验证可帮助您更好地保护您的账户。有多个 MFA 类型可用。

有关 MFA 的更多信息，请参阅 Amazon 环境，请参阅[多重身份验证](#)以及中的以下主题 IAM 用户指南：

- [重新同步虚拟或硬件 MFA 设备](#)
- [停用 MFA 设备](#)
- [如果 MFA 设备丢失或停止工作怎么办？](#)

您可以激活—每个根用户或 IAM 用户的 MFA 设备（任何类型）。

您 MFA 以使用 Amazon Identity and Access Management (IAM) 控制台。根据您要激活的 MFA 设备的类型，请在 IAM 用户指南：

- [为您的启用虚拟 MFA 设备 Amazon Web Services 账户根用户](#)
- [为您的启用 U2F 安全密钥 Amazon Web Services 账户根用户](#)
- [为您的启用硬件 MFA 设备 Amazon Web Services 账户根用户](#)

## 更改根用户的密码

要更改根用户的密码，您必须以 Amazon Web Services 账户根用户而不是 IAM 用户。若要了解如何重置被遗忘了，请参阅根用户密码[重置丢失或忘记密码或访问密钥 Amazon](#)中的 IAM 用户指南。

为保护您的密码，请务必遵循以下最佳实践：

- 定期更改您的密码。
- 由于任何知道您密码的人都可以访问您的账户，因此您的密码保密
- 不要为 Amazon 使用您在其他网站上使用的密码。
- 不要使用容易猜到的密码。此类密码包括 `secret`、`password`、`amazon`、`123456` 等。此外，请避免使用字典单词、您的姓名、电子邮件地址或某人可以轻松获取的其他个人信息。

### Amazon Web Services Management Console

#### 为根用户更改密码

##### 最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 您必须以 Amazon Web Services 账户 root 用户，不需要额外的 Amazon Identity and Access Management (IAM) 权限。您无法以 IAM 用户或角色身份执行这些步骤。

1. 使用您的Amazon Web Services 账户登录的电子邮件地址和密码[Amazon Web Services Management Console](#)作为您的Amazon Web Services 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 My Account。
3. 在页面右侧，在账户设置部分，选择编辑。
4. 在存储库的密码行，选择编辑更改密码。
5. 选择一个强密码。虽然你可以为 [IAM 用户设置账户密码策略](#)，该策略不适用于根用户。

Amazon要求您的密码满足以下条件：

- 它必须至少包含 8 个字符，最多为 128 个字符。
- 它必须包含至少以下三种字符类型的组合：大写、小写、数字，以及! @ # \$ % ^ & \* ( ) < > [ ] { } | \_ + = 符号。
- 它一定不能与你的Amazon Web Services 账户姓名或电子邮件地址。

#### Note

Amazon 将会推出登录过程的改进功能。其中一项改进是为您的账户实施更加安全的密码策略。如果Amazon已升级您的账户，您需要满足前面描述的密码策略。如果Amazon那么还没升级你的账户Amazon还没有执行此政策。但是，我们强烈建议您遵循其准则，以获取更安全的密码。

#### Amazon CLI & SDKs

中不支持此任务Amazon CLI或者通过来自其中一个的 API 操作Amazon开发工具包。您只能使用Amazon Web Services Management Console。

## 创建和删除的访问密钥Amazon Web Services 账户根用户

虽然我们不推荐 (p. 39)，您可以为 root 用户创建访问密钥，以便在Amazon Command Line Interface(Amazon CLI) 或者使用其中之一的 API 操作Amazon开发工具包。

### 创建根用户的访问密钥

您可以使用 Amazon Web Services Management Console 或 Amazon 编程工具来创建根用户的访问密钥。

#### Amazon Web Services Management Console

创建的访问密钥Amazon Web Services 账户根用户

##### 最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 您必须以Amazon Web Services 账户root 用户，不需要额外的Amazon Identity and Access Management(IAM) 权限。您无法以 IAM 用户或角色身份执行这些步骤。
1. 使用您的Amazon Web Services 账户登录的电子邮件地址和密码[Amazon Web Services Management Console](#)作为您的Amazon Web Services 账户根用户。
  2. 在导航栏上选择您的账户名称，然后选择我的安全凭证。

3. 如果看到有关访问您的安全凭证的警告 Amazon Web Services 账户，选择继续前往安全凭证。
4. 展开 Access keys (access key ID and secret access key) 部分。
5. 选择 Create New Access Key。如果此选项不可用，则已达到访问密钥的数量上限。在创建新密钥之前，必须删除其中一个现有访问密钥。有关更多信息，请参阅 [IAM 对象配额](#) 中的 IAM 用户指南。

一个警告说明，您只有这一次机会可以查看或下载秘密访问密钥。您之后无法检索它。

- 如果您选择 Show Access Key，您可以从浏览器窗口复制访问密钥 ID 和私有密钥，将其粘贴到其他位置。
  - 如果您选择 Download Key File，则会接收一个包含访问密钥 ID 和私有密钥、名为 rootkey.csv 的文件。将该文件安全保存在某个位置。
6. 当您不再需要访问密钥时 [建议您删除它 \(p. 32\)](#)，或者至少选择将其标记为非活动状态 Make Inactive (转为非活动) 以便没有人可以滥用它。

## Amazon CLI & SDKs

### 要为根用户创建访问密钥

#### Note

要以 root 用户身份运行以下命令或 API 操作，您必须已有一个活动访问 key pair。如果没有访问密钥，请使用创建第一个访问密钥 Amazon Web Services Management Console。然后，您可以将第一个访问密钥中的凭据用于 Amazon CLI 创建第二个访问密钥，或者删除访问密钥。

- Amazon CLI : [aws iam create-access-key](#)

#### Example

```
$ aws iam create-access-key
{
  "AccessKey": {
    "UserName": "MyUserName",
    "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "Status": "Active",
    "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",
    "CreateDate": "2021-04-08T19:30:16+00:00"
  }
}
```

- Amazon API : [CreateAccessKey](#)

## 删除根用户的访问密钥

您可以使用 Amazon Web Services Management Console 删除根用户的访问密钥。您不能使用 Amazon CLI 或者 Amazon 删除根用户访问密钥的 API。

### Amazon Web Services Management Console

#### 删除根用户的访问密钥

##### 最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 您必须以 Amazon Web Services 账户 root 用户，不需要额外的 Amazon Identity and Access Management (IAM) 权限。您无法以 IAM 用户或角色身份执行这些步骤。

1. 使用您的 Amazon Web Services 账户登录的电子邮件地址和密码 [Amazon Web Services Management Console](#) 作为您的 Amazon Web Services 账户根用户。
2. 在导航栏上选择您的账户名称，然后选择我的安全凭证。
3. 如果看到有关访问您的安全凭证的警告 Amazon Web Services 账户，选择继续前往安全凭证。
4. 展开 Access keys (access key ID and secret access key) 部分。
5. 查找要删除的访问密钥，然后在 Actions 列下，选择 Delete。

#### Note

您可以将访问密钥标记为非活动而不是删除它。这样，您将来可以继续使用它，无需更改密钥 ID 或密钥。当密钥处于非活动状态时，任何在请求中使用密钥的任何尝试 AmazonAPI 失败并出现错误拒绝访问。

### Amazon CLI & SDKs

#### 删除根用户的访问密钥

##### 最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 您必须以 Amazon Web Services 账户 root 用户，不需要额外的 Amazon Identity and Access Management(IAM) 权限。您无法以 IAM 用户或角色身份执行这些步骤。

- Amazon CLI : [aws iam delete-access-key](#)

#### Example

```
$ aws iam delete-access-key \  
  --access-key-id AKIAIOSFODNN7EXAMPLE
```

如果成功，此命令不会产生任何输出。

- Amazon API : [DeleteAccessKey](#)

## 比较 Amazon Web Services 账户根用户证书和 IAM 用户证书

Amazon 中有两种不同类型的用户。您是账户所有者（根用户），或者是 Amazon Identity and Access Management (IAM) 用户。创建根用户时 Amazon Web Services 账户已创建。IAM 用户由根用户或账户的 IAM 管理员创建。所有 Amazon 用户都具有安全凭证。

### 根用户凭证

账户拥有者的凭证允许完全访问账户中的所有资源。您不能使用 IAM 策略以明确拒绝 root 用户对资源的访问权限。您只能使用 Amazon Organizations [服务控制策略 \(SCP\)](#) 以限制成员账户的 root 用户的权限。因此，我们建议您创建一个具有管理员权限的 IAM 用户，以用于日常 Amazon 任务并锁定根用户的访问密钥。

有些特定的任务只能由 root 用户执行。例如，只有根用户可以关闭您的账户。如果您需要执行需要根用户的任务，请使用根用户的电子邮件地址和密码登录 Amazon Web Services Management Console。有关更多信息，请参阅 [需要根用户凭证的任务 \(p. 34\)](#)。

### IAM 凭证

使用 IAM，您可以安全地控制访问 Amazon 为您的用户提供的服务和资源 Amazon Web Services 账户。例如，如果您需要管理员级别的权限，则可以 [创建 IAM 用户](#)，向该用户授予对您的账户的完整访问权，然后使用这些凭证与交互。Amazon。如果需要修改或撤销权限，您可以删除或修改与该 IAM 用户相关联的策略。

如果你有多个用户需要访问 Amazon Web Services 账户，请为每个用户创建唯一的凭证并定义哪些用户有权访问哪些资源。您不需要和不应共享凭证。例如，您可以创建具有对您的资源的只读访问权的 IAM 用户。Amazon Web Services 账户并将每个 IAM 用户的证书分发给您的其中一个用户。

## 需要根用户凭证的任务

我们建议您使用具有适当权限的 IAM 用户来执行任务和访问 Amazon 资源。不过，您只能在以账户的根用户身份登录时才能执行下列任务。

### Tasks

- [更改您的账户设置](#)。这包括账户名称、电子邮件地址、根用户密码和根用户访问密钥。其他账户设置，例如联系人信息、付款货币偏好以及 Amazon Web Services 区域，不要求根用户凭证。
- [恢复 IAM 用户权限](#)。如果唯一的 IAM 管理员意外撤消了自己的权限，您可以使用根用户身份登录来编辑策略并还原这些权限。
- [激活 IAM 对账单和成本管理控制台的访问权限](#)。
- [查看特定税务发票](#)。具有 [Amazon 门户网站：查看账单](#) 权限可以从中查看和下载增值税发票 Amazon 欧洲，但不是 Amazon Inc. 或 Amazon Internet Services Private Limited (AISPL)。
- [关闭您的 Amazon Web Services 账户](#)。
- [更改 Amazon 支持计划或取消 Amazon 支持计划](#)。有关更多信息，请参阅 [Amazon 的 IAM 支持](#)。
- 已在预留实例 Marketplace 中 [注册为卖家](#)。
- [配置 Amazon S3 存储桶以启用 MFA \(多重身份验证\)](#)。
- [编辑或删除包含无效虚拟私有云 \(VPC\) ID 或 VPC 终端节点 ID 的 Amazon 简单存储服务 \(Amazon S3\) 存储桶策略](#)。
- [注册 GovCloud](#)。



# 使用Amazon组织中的账户管理

Amazon Organizations是Amazon是否可用于管理您的服务Amazon Web Services 账户作为一组。这提供了诸如整合账单之类的功能，您账户的所有账单都归组在一起并由单个付款人处理。您还可以使用基于策略的控制来集中管理组织的安全性。

有关 Amazon Organizations 的更多信息，请参阅 [Amazon Organizations 用户指南](#)。

Amazon账户管理将该功能扩展到还包括对附加到Amazon Web Services 账户，例如备用联系信息。

当您使用时Amazon Organizations要将您的账户作为一个群组管理，组织的大多数管理任务只能由组织的管理账户。默认情况下，这仅包括与管理组织本身相关的操作。您可以将此附加功能扩展到其他功能Amazon启用服务可信访问权限在 Organizations 和该服务之间。受信任的访问授予对指定Amazon服务来访问有关组织及其包含的帐户的信息。当您为账户管理启用可信访问权限时，账户管理服务会向 Organizations 及其管理帐户授予访问组织所有成员帐户元数据的权限。

启用可信访问权限后，还可以选择将其中一个成员帐户指定为委托管理员帐户Amazon账户管理。这允许委派管理员帐户对组织中的成员帐户执行与以前只有管理帐户可以执行的相同的账户管理元数据管理任务。委托管理员帐户只能访问账户管理服务的管理任务。委托管理员帐户不具有管理帐户所拥有的组织的所有管理访问权限。

启用可信访问权限和委派管理员可以使用accountID那些中的参数[账户管理 API 操作 \(p. 65\)](#)那支持它。只有在使用管理帐户中的凭据调用操作（如果启用了可信访问），或者如果启用了可信访问权限，则可以成功使用此参数。

当你Amazon Web Services 账户是由管理的组织的一部分Amazon Organizations，那么组织的管理员可以申请[服务控制策略 \(SCP\)](#)这可能会限制会员帐户中的委托人可以做什么。SCP 永远不会授予权限；相反，它是限制成员帐户可以使用哪些权限的过滤器。用户或角色（委托人）在成员帐户中，只能执行与应用于该帐户的SCP 允许的操作以及附加到委托人的 IAM 权限策略交叉点的操作。例如，您可以使用 SCP 来防止帐户中的任何委托人修改自己帐户的备用联系人。例如，适用于的 SCPAmazon Web Services 帐户，请参阅[限制访问Amazon Organizations服务控制策略 \(p. 37\)](#)。

## 主题

- [启用可信访问权限Amazon账户管理 \(p. 35\)](#)
- [启用委托管理员帐户Amazon账户管理 \(p. 36\)](#)
- [限制访问Amazon Organizations服务控制策略 \(p. 37\)](#)

## 启用可信访问权限Amazon账户管理

要使组织中的管理帐户能够调用Amazon针对组织中其他成员帐户的账户管理 API 操作，请按以下步骤操作。

### 最小权限

要执行以下任务，您必须满足以下要求：

- 您只能从组织的管理帐户中执行此操作。
- 您的组织必须 [已启用所有功能](#)。

### Amazon Web Services Management Console

使用启用可信访问：Amazon Organizations对于 来说为Amazon账户管理

1. 登录到 [Amazon Organizations 控制台](#)。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理帐户中以根用户的身份登录（不推荐）。



2. 选择服务在导航窗格中。
3. 选择Amazon账户管理在服务列表中。
4. 选择 Enable trusted access (启用可信访问)。

#### Amazon CLI & SDKs

使用启用可信访问：Amazon Organizations对于 来说为Amazon账户管理

您可以使用以下命令允许组织中的账户管理可信访问：

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

以下示例启用可信访问Amazon调用账户组织中的账户管理。

```
$ 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。

运行此命令后，您可以使用组织管理账户中的凭据调用账户管理 API 操作，这些操作使用--  
accountId参数以引用组织中的成员账户。

## 启用委托管理员帐户Amazon账户管理

委托管理员帐户可以调用Amazon组织内其他成员账户的账户管理 API 操作。要将组织中的成员帐户指定为委派管理员帐户，请按以下步骤操作。

#### 最小权限

要执行这些任务，必须满足以下要求：

- 您只能从组织的管理帐户中执行此操作。
- 您的组织必须 [已启用所有功能](#)。
- 您必须具有 [为组织中的账户管理启用可信访问权限 \(p. 35\)](#)。

为组织指定委派管理员帐户后，该帐户中的用户和角色可以调用Amazon CLI和Amazon中的 SDK 操作account通过支持可选的命名空间可以在 Organizations 模式下工作AccountId参数。

#### Amazon Web Services Management Console

中不支持此任务Amazon账户管理控制台。您只能使用Amazon CLI或者来自其中一个的 API 操作  
Amazon开发工具包。

#### Amazon CLI & SDKs

为账户管理服务注册委派管理员帐户

您可以使用以下命令为账户管理服务启用委派管理员。

您必须指定以下服务委托人：

```
account.amazonaws.com
```

- Amazon CLI：[注册委托管理员](#)

以下示例将组织的成员账户注册为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 中的凭据来调用账户管理 Amazon CLI 和使用 `--account-id` 参数可引用组织中的成员账户。

## 限制访问 Amazon Organizations 服务控制策略

本主题提供的示例展示如何使用服务控制策略 (SCP) 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，请参阅中的以下主题。Amazon Organizations 用户指南：

- [创建 SCP](#)
- [将 SCP 附加到 OU 和账户](#)
- [SCP 的策略](#)
- [SCP 策略语法](#)

### Example 示例 1：防止帐户修改自己的备用联系人

以下示例拒绝 `PutAlternateContact` 和 `DeleteAlternateContact` API 操作不会被中的任何成员账户调用 [单独账户模式 \(p. 12\)](#)。这可以防止受影响账户中的任何委托人更改自己的备用联系人。

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

### Example 示例 2：防止任何成员帐户修改组织中任何其他成员账户的备用联系人

下面的示例概括了 `Resource` 元素改为 "\*"，这意味着它适用于两者 [独立模式请求和组织模式请求 \(p. 12\)](#)。这意味着，即使是账户管理的委派管理员帐户，如果 SCP 适用于它，也无法更改组织中任何账户的任何备用联系人。

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

```
        "Resource": [ "*" ]
      }
    ]
  }
}
```

### Example 示例 3：防止 OU 中的成员账户修改自己的备用联系人

以下示例 SCP 包含一个条件，将账户的组织路径与两个 OU 的列表进行比较。这会导致指定 OU 中任何账户中的委托人无法修改自己的备用联系人。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": "account:PutAlternateContact",
      "Resource": [
        "arn:aws:account:*:account"
      ],
      "Condition": {
        "ForAnyValue:StringLike": {
          "account:AccountResourceOrgPath": [
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/",
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/"
          ]
        }
      }
    }
  ]
}
```

# Amazon Web Services 账户的最佳实践

此部分介绍了我们建议您遵循的最佳实践 Amazon Web Services 账户。它们分为以下类别：

主题

- [保护账户根用户的最佳做法 \(p. 39\)](#)
- [管理 Amazon 访问密钥的最佳实践 \(p. 40\)](#)

## 保护账户根用户的最佳做法

以下是推荐的与根用户相关的最佳实践：Amazon Web Services 账户。

### 限制你对 root 用户执行的任务

我们强烈建议您仅将根用户用于两件事：

- 在中创建第一个管理员用户 Amazon Identity and Access Management (IAM)。有关如何执行此操作的详细信息，请参阅 [创建您的第一个 IAM 用户和组](#) 中的 IAM 用户指南。
- 执行那些可以执行的任务仅限根用户。有关这些任务的完整列表，请参阅 [需要根用户凭证的任务 \(p. 34\)](#)。

### 锁定你的 Amazon Web Services 账户 root 用户访问密钥

使用访问密钥 (访问密钥 ID 和秘密访问密钥) 以编程方式向 Amazon 提出请求。但是，我们强烈建议您不要使用您的 Amazon Web Services 账户 root 用户访问密钥。您的访问密钥 Amazon Web Services 账户根用户为所有人提供对所有资源的完全访问权限。Amazon 服务，包括您的账单信息。您无法减少与您的关联的权限。Amazon Web Services 账户 root 用户访问密钥。

您应像对待您的信用卡号或任何其他敏感机密信息一样。以下是执行该操作的一些方式：

- 访问密钥
  - 如果您还没有访问密钥 Amazon Web Services 账户除非绝对需要，否则请勿创建它。相反，请使用 root 用户来 [为自己创建 IAM 用户](#) 具有管理权限。
  - 如果您的拥有根用户的访问密钥，请删除它。
  - 如果您必须保持它可用，请定期轮换 (更改) 访问密钥。要删除或轮换根用户的访问密钥，请使用根用户登录到 [我的安全凭证页面](#) 中的 Amazon Web Services Management Console。您可以在 Access keys 部分中管理您的访问密钥。有关轮换访问密钥的更多信息，请参阅 [轮换访问密钥](#) 中的 IAM 用户指南。
- 永远不要分享你 Amazon Web Services 账户任何人都可使用根用户密码或访问密钥。
- 使用强密码有助于保护对 Amazon Web Services Management Console。有关管理您的信息 Amazon Web Services 账户有根用户的密码，请参阅 [更改根用户的密码 \(p. 30\)](#)。

- 启用Amazon您的上的多重身份验证 (MFA)Amazon Web Services 账户账户根用户。有关更多信息，请参阅《IAM 用户指南》中的[在 Amazon 中使用多重身份验证 \(MFA\)](#)。

## 管理 Amazon 访问密钥的最佳实践

当您使用时Amazon以编程方式，你提供你的Amazon访问密钥以便Amazon可以在程序化通话中验证你的身份。您的访问密钥包含一个访问密钥 ID (例如，AKIAIOSFODNN7EXAMPLE) 和一个私有访问密钥 (例如，wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY)。

拥有您的访问密钥的任何人都具有相同的访问权限级别。Amazon你做的资源。因此，Amazon 全力保护您的访问密钥并确保符合我们的[分担责任模型](#)，您也应当如此。

下述步骤可以帮助您保护访问密钥。有关背景信息，请参阅[创建和删除的访问密钥Amazon Web Services 账户根用户 \(p. 31\)](#)。

### Note

贵组织的安全要求和策略可能与本主题中介绍的有所不同。此处提供的建议旨在作为一般准则。

## 删除 (或不生成) 账户访问密钥

必须使用访问密钥来签署您使用[Amazon命令行工具](#)，[Amazon软件开发工具包](#)，或直接 API 调用。任何拥有您的访问密钥的人Amazon Web Services 账户根用户可以无限制地访问您账户中的所有资源，包括账单信息。您无法限制您的权限Amazon Web Services 账户根用户。

保护账户的最佳方法之一是不为您的设置访问密钥。Amazon Web Services 账户根用户。除非必须具有根用户访问密钥 (这种情况很少见)，否则最好不要生成根用户访问密钥。相反，[推荐的最佳实践](#)是创建一个或多个Amazon Identity and Access Management(IAM) 用户。为 IAM 用户授予必要的权限，并使用这些权限进行日常互动。Amazon.

如果您已经拥有账户的访问密钥，我们建议以下方法：找到您当前在应用程序中使用访问密钥 (如果有) 的位置，并使用 IAM 用户访问密钥替换根用户访问密钥。然后禁用并删除根用户访问密钥。有关如何替换另一个访问密钥的更多信息，请参阅。[如何轮换 IAM 用户的访问密钥](#)在Amazon安全博客。

默认情况下，Amazon不会为新账户生成访问密钥。

有关如何创建具有管理权限的 IAM 用户的信息，请参阅。[创建您的第一个 IAM 管理员用户和组](#)中的IAM 用户指南。

## 使用临时安全凭证 (IAM 角色) 代替长期访问密钥

在许多情况下，您并不需要永不过期的长期访问密钥 (如 IAM 用户访问密钥)。相反，您可以创建 IAM 角色并生成临时安全证书。临时安全证书包括访问密钥 ID 和秘密访问密钥，以及一个指示证书何时到期的安全令牌。

长期访问密钥，如与 IAM 用户相关联的访问密钥和Amazon Web Services 账户根用户将保持有效，直至手动撤销。但是，通过 IAM 角色获取的临时安全凭证和Amazon Security Token Service在短时间内过期。凭证意外泄漏时，使用临时安全凭证可帮助降低您的风险。

在以下这些情况下使用 IAM 角色和临时安全证书：

- 您有申请或Amazon CLI在 Amazon EC2 实例上运行的脚本。请勿直接在应用程序中使用访问密钥。请勿采取以下做法：将访问密钥传递给应用程序、将访问密钥嵌入应用程序中、让应用程序从任何源读取访问密钥 相反，为应用程序定义具有适当权限的 IAM 角色，并使用启动 Amazon Elastic Compute Cloud (Amazon EC2) 实例。[适用于 EC2 的角色](#)。这样做会将 IAM 角色与 Amazon EC2 实例相关联。这种做法还使应用程序能够获得临时安全凭证，然后再使用这些证书来进行编程调用。Amazon. 这些区域有：Amazon开发工具包和Amazon Command Line Interface(Amazon CLI) 可以自动获得角色的临时凭证。

- 您需要授予跨账户访问权限。使用 IAM 角色建立账户之间的信任，然后向一个账户中的用户授予有限的访问可信账户的权限。有关更多信息，请参阅 [教程：跨委托访问权限Amazon Web Services 账户使用 IAM 角色](#)中的IAM 用户指南。
- 您拥有一个移动应用程序。请勿采取以下做法：将访问密钥嵌入到应用程序中，即使是在相反，请使用[Amazon Cognito](#)管理应用程序中的用户身份。借助此服务，您可以使 Login with Amazon、Facebook、Google 或任何 OpenID Connect (OIDC) 兼容的身份提供商来验证用户身份验证。然后，您可以使用 Amazon Cognito 凭证提供程序来管理应用程序用于向发出请求的证书。Amazon. 有关更多信息，请参阅 [使用 Amazon Cognito 凭证提供程序](#)在Amazon手机博客。
- 您希望向 Amazon 进行联合身份验证且贵组织支持 SAML 2.0。如果您所在的组织具有支持 SAML 2.0 的身份提供程序，请将提供程序配置为使用 SAML。您可以使用 SAML 与 Amazon 交换身份验证信息，并获得一组临时安全证书。有关更多信息，请参阅 [关于基于 SAML 2.0 的联合身份验证](#)中的IAM 用户指南。
- 您希望向 Amazon 进行联合身份验证且贵组织拥有本地身份存储。如果用户可以在组织内部进行身份验证，您可以编写一个可向他们颁发用于访问 Amazon 资源的临时安全凭证的应用程序。有关更多信息，请参阅 [启用自定义身份代理访问Amazon Web Services Management Console](#)中的IAM 用户指南。

## 正确管理 IAM 用户访问密钥

如果您必须创建访问密钥才能对Amazon，为 IAM 用户创建它们，仅向用户授予他们所需的权限。有关更多信息，请参阅 [管理 IAM 用户的访问密钥](#)中的IAM 用户指南。

### Note

您是否将 Amazon EC2 实例与需要编程访问权限的应用程序一起使用Amazon资源？如果是这样，请使用[适用于 EC2 的 IAM 角色](#)。

使用访问密钥时，请遵守这些预防措施：

- 请勿直接将访问密钥嵌入到代码。这些区域有：[Amazon软件开发工具包](#)和[Amazon命令行工具](#)使您可以将访问密钥放在已知位置，这样就不必将访问密钥保留在代码中。

在以下任一位置中放置访问密钥：

- Amazon 凭证文件。Amazon 开发工具包和 Amazon CLI 自动使用您存储在 Amazon 凭证文件中的凭证。

有关使用 Amazon 证书文件的信息，请参阅软件开发工具包文档。示例包括[SetAmazon凭证和区域](#)中的Amazon SDK for Java开发人员指南和[配置和凭证文件](#)中的Amazon Command Line Interface用户指南。

要存储的凭据Amazon SDK for .NET和Amazon Tools for Windows PowerShell中的建议您使用开发工具包商店。有关更多信息，请参阅 [使用开发工具包商店](#)中的Amazon SDK for .NET开发人员指南。

- 环境变量。在多租户系统上，选择用户环境变量，而不是系统环境变量。

有关使用环境变量存储凭证的更多信息，请参阅 [环境变量](#)中的Amazon Command Line Interface用户指南。

- 对不同应用程序使用不同的访问密钥。这样您就可以隔离权限并撤消单个应用程序的访问密钥，如果这些应用程序已公开。为不同的应用程序设置不同的访问密钥也会在 [Amazon CloudTrail](#) 日志文件中生成不同的条目。通过此配置，您可以更轻松地确定哪个应用程序执行了特定的操作。
- 定期轮换访问密钥。定期更改访问密钥。有关详细信息，请参阅 [轮换访问密钥 \(Amazon CLI、适用于 Windows PowerShell 的工具和AmazonAPI\)](#)中的IAM 用户指南和[如何轮换 IAM 用户的访问密钥](#)在Amazon安全博客。
- 删除未使用的访问密钥。如果某个用户离开您的组织，请删除相应的 IAM 用户，这样该用户将无法再访问您的资源。要找出上次使用访问密钥的时间，请使用 [GetAccessKeyLastUsed](#) API ( Amazon CLI 命令：`aws iam get-access-key-last-used`)。
- 为最敏感的操作配置多重验证。有关更多信息，请参阅 IAM 用户指南中的[在Amazon中使用多重身份验证 \(MFA\)](#)。



## 使用 Amazon 访问密钥访问移动应用程序

您可以使用 Amazon 移动应用程序访问一组有限的 Amazon 服务和功能。该移动应用程序可帮助您在外出时支持事件响应。如需了解更多信息和下载应用程序，请参阅 [Amazon 控制台移动应用程序](#)。

您可以使用控制台密码或访问密钥登录移动应用程序。作为最佳实践，请勿使用根用户访问密钥。相反，我们强烈建议除了在移动设备上使用密码或生物识别锁定之外，您还应采取以下做法：[创建 IAM 用户管理 Amazon 资源的费用](#)。如果您的移动设备丢失了，您可以删除 IAM 用户的访问权限。有关为 IAM 用户生成访问密钥的更多信息，请参阅 [管理 IAM 用户的访问密钥](#) 中的 IAM 用户指南。

### 使用访问密钥登录（移动应用程序）

1. 在移动设备上打开该应用程序。
2. 如果这是您第一次向设备添加身份，请选择 Add an identity (添加身份)，然后选择 Access keys (访问密钥)。

如果您已使用其他身份登录，请选择菜单图标并选择 Switch identity (切换身份)。然后选择 Sign in as a different identity (以其他身份登录)，然后选择 Access keys (访问密钥)。

3. 在 Access keys (访问密钥) 页面上输入您的信息。

- 访问密钥 ID— 输入您的访问密钥 ID。
- 秘密访问密钥— 输入您的私有访问密钥。
- 身份名称— 输入将在移动应用程序中显示的身份名称。这不需要与 IAM 用户名一致。
- 身份识别码— 创建将来在登录时使用的个人身份识别码 (PIN)。

#### Note

如果您为 Amazon 移动应用程序启用了生物识别技术，系统将提示您使用指纹或面部识别（而非 PIN）进行验证。如果生物识别失败，系统可能会提示您输入 PIN。

4. 选择 Verify and add keys (验证并添加密钥)。

现在，您就可以使用移动应用程序访问一组选定的资源。

## 了解更多信息

有关保持您的最佳实践的更多信息 Amazon Web Services 账户安全，请参阅以下资源：

- [IAM 最佳实践](#) 包含使用 Amazon Identity and Access Management (IAM) 服务来帮助保护您的 Amazon resources
- 下列主题提供有关设置 Amazon 开发工具包和 Amazon CLI 要使用访问密钥：
  - [Set Amazon 凭证和区域](#) 中的 Amazon SDK for Java 开发人员指南
  - [使用开发工具包商店](#) 中的 Amazon SDK for .NET 开发人员指南
  - [向开发工具包提供凭证](#) 中的 Amazon SDK for PHP 开发人员指南
  - [配置在 Boto 3 \(Amazon 开发工具包中的文档\)](#)
  - [使用 Amazon 凭证](#) 中的 Amazon Tools for Windows PowerShell 用户指南
  - [配置和凭证文件](#) 中的 Amazon Command Line Interface 用户指南
  - [使用 IAM 角色授予访问权限](#) 中的 Amazon SDK for .NET 开发人员指南. 讨论如何使用 Amazon SDK for .NET 在 Amazon EC2 实例上运行时，可以自动获取临时安全凭证。类似的信息可用于 [Amazon 适用于 Java 的开发工具包](#)。



# 中的安全性Amazon账户管理

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

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

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

该文档帮助您了解如何在使用时应用责任共担模型。Amazon账户管理。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。您还将了解如何使用其他Amazon帮助您监控和保护您的账户管理资源的服务。

主题

- [中的数据保护Amazon账户管理 \(p. 43\)](#)
- [Amazon PrivateLink对于 来说为Amazon账户管理 \(p. 44\)](#)
- [适用于 的 Identity and Access ManagementAmazon账户管理 \(p. 45\)](#)
- [Amazon适用于 的托管策略Amazon账户管理 \(p. 57\)](#)
- [的合规性验证Amazon账户管理 \(p. 59\)](#)
- [中的故障恢复能力Amazon账户管理 \(p. 59\)](#)
- [Amazon Account Management 中的基础设施安全性 \(p. 59\)](#)

## 中的数据保护Amazon账户管理

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

出于数据保护目的，我们建议您保护 Amazon Web Services 账户凭证并使用 Amazon Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与Amazon资源进行通信。建议使用 TLS 1.2 或更高版本。
- 使用 Amazon CloudTrail 设置 API 和用户活动日志记录。
- 使用Amazon加密解决方案以及Amazon服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的个人数据。
- 如果在通过命令行界面或 API 访问Amazon时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 终端节点。有关可用的 FIPS 终端节点的更多信息，请参阅[美国联邦信息处理标准 \(FIPS\) 第 140-2 版](#)。

我们强烈建议您切勿将机密信息或敏感信息（例如您客户的电子邮件地址）放入标签或自由格式字段（例如名称字段）。这包括使用账户管理或其他工作时Amazon使用控制台、API、Amazon CLI，或者Amazon开发工具包。您在用于名称的标签或自由格式字段中输入的任何数据都可能用于计费或诊断日志。如果您向外部服务器提供 URL，我们强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

## Amazon PrivateLink对于 来说为Amazon账户管理

如果您使用 Amazon Virtual Private Cloud (Amazon VPC) 托管Amazon资源，您可以访问Amazon在 VPC 内提供账户管理服务，而无需跨越公共互联网。

亚马逊 VPC 允许您启动Amazon在自定义虚拟网络中的资源。可以使用 VPC 控制您的网络设置，例如 IP 地址范围、子网、路由表和网络网关。有关 VPC 的更多信息，请参阅[Amazon VPC User Guide](#)。

要将您的 Amazon VPC 连接到账户管理，您必须首先定义接口 VPC 终端节点，您可以将 VPC 连接到其他 VPCAmazon服务。该终端节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 终端节点 \(Amazon PrivateLink\)](#)。

### 创建终端节点

您可以创建Amazon使用 VPC 中的账户管理终端节点Amazon Web Services Management Console，Amazon Command Line Interface(Amazon CLI)，Amazon开发工具包，Amazon账户管理 API，或Amazon CloudFormation。

有关使用 Amazon VPC 控制台或Amazon CLI，请参阅[创建接口终端节点](#)中的Amazon VPC 用户指南。

#### Note

在创建终端节点时，请使用以下格式将账户管理指定为您希望您的 VPC 连接到的服务：

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

你必须完全如图所示使用字符串，指定cn-northwest-1区域。作为一项全球服务，账户管理仅托管在那一项服务中Amazon区域。

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

### Amazon VPC 终端节点策略

您可以通过在创建 Amazon VPC 终端节点时附加终端节点策略来控制可以通过此服务终端节点执行哪些操作。您可通过附加多个终端节点策略来创建复杂的 IAM 规则。有关更多信息，请参阅：

- [账户管理 Amazon Virtual Private Cloud 终端节点策略 \(p. 44\)](#)
- [使用 VPC 终端节点控制对服务的访问](#)中的Amazon PrivateLink指南。

### 账户管理 Amazon Virtual Private Cloud 终端节点策略

您可以为账户管理创建 Amazon VPC 终端节点策略，可在该策略中指定：

- 可执行操作的委托人。
- 委托人可以执行的操作。
- 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 中名为 Alice 的 IAM 用户检索和更改任何备用联系信息。Amazon Web Services 账户，但拒绝所有 IAM 用户删除任何账户上的任何备用联系人信息的权限。

```
{
```

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

如果您希望授予对属于 Amazon 组织转换为位于组织的其中一个成员账户中的委托人，然后 Resource 元素必须使用以下格式：

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

有关创建终端节点策略的更多信息，请参[使用 VPC 终端节点控制对服务的访问](#)中的 Amazon PrivateLink 指南。

## 适用于的 Identity and Access Management Amazon 账户管理

Amazon Identity and Access Management (IAM) 是一种 Amazon 服务，可以帮助管理员安全地控制对 Amazon 资源的访问。IAM 管理员控制谁可以 Audenty ( 已登录 ) 和 Augan ( 有权限 ) 可以使用账户管理资源。IAM 是一个可以免费使用的 Amazon 服务。

### 主题

- [Audience \(p. 45\)](#)
- [使用身份进行身份验证 \(p. 46\)](#)
- [使用策略管理访问 \(p. 47\)](#)
- [的方法 Amazon 账户管理与 IAM 协同工作 \(p. 48\)](#)
- [适用于的基于身份的策略示例 Amazon 账户管理 \(p. 53\)](#)
- [故障排除 Amazon 账户管理身份和访问权限 \(p. 55\)](#)

## Audience

如何使用 Amazon Identity and Access Management (IAM) 因您可以在账户管理中执行的操作而异。

服务用户— 如果您使用账户管理服务来完成工作，则您的管理员会为您提供所需的凭证和权限。当您使用更多账户管理功能来完成工作时，您可能需要额外权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问账户管理中的功能，请参[阅故障排除 Amazon 账户管理身份和访问权限 \(p. 55\)](#)。

服务管理员如果您在公司负责管理账户管理资源，则您可能具有账户管理的完全访问权限。您有责任确定您的员工应访问哪些账户管理功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与账户管理搭配使用的更多信息，请[查看方法 Amazon 账户管理与 IAM 协同工作 \(p. 48\)](#)。

IAM 管理员如果您是 IAM 管理员，您可能希望了解有关您可以如何编写策略以管理对账户管理的访问权限的详细信息。要查看您可在 IAM 中使用的基于身份的账户管理策略示例，请参阅[适用于的基于身份的策略示例 Amazon 账户管理 \(p. 53\)](#)。

## 使用身份进行身份验证

身份验证是您使用身份凭证登录 Amazon 的方法。有关使用 Amazon Web Services Management Console 登录的更多信息，请参阅[IAM 用户指南中的以 Amazon Web Services Management Console IAM 用户或根用户身份登录](#)。

您必须作为 Amazon Web Services 账户根用户、IAM 用户或代入 IAM 角色以进行身份验证（登录到 Amazon）。您还可以使用公司的单一登录身份验证方法，甚至使用 Google 或 Facebook 登录。在这些情况下，您的管理员以前使用 IAM 角色设置了联合身份验证。在您使用来自其他公司的凭证访问 Amazon 时，您间接地代入了角色。

要直接登录到 [Amazon Web Services Management Console](#)，请将密码与根用户电子邮件地址或 IAM 用户名一起使用。您可以使用根用户或 IAM 用户访问密钥以编程方式访问 Amazon。Amazon 提供了开发工具包和命令行工具，可使用您的凭证对您的请求进行加密签名。如果您不使用 Amazon 工具，则必须自行对请求签名。使用签名版本 4（用于对入站 API 请求进行验证的协议）完成此操作。有关验证请求的更多信息，请参阅《Amazon 一般参考》中的[Signature Version 4 签名流程](#)。

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

## Amazon Web Services 账户根用户

当您首次创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon 服务和资源有完全访问权限的单一登录身份。此身份称为 Amazon Web Services 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不使用根用户执行日常任务，即使是管理任务。相反，请遵循[仅使用根用户创建您的第一个 IAM 用户的最佳实践](#)。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。

## IAM 用户和组

[IAM 用户](#)是 Amazon Web Services 账户内对某个人员或应用程序具有特定权限的一个身份。IAM 用户可能有长期凭证，例如用户名和密码或一组访问密钥。要了解如何生成访问密钥，请参阅 IAM 用户指南中的[管理 IAM 用户的访问密钥](#)。为 IAM 用户生成访问密钥时，请确保查看并安全保存密钥对。您以后无法找回秘密访问密钥，而是必须生成新的访问密钥对。

[IAM 组](#)是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

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

## IAM 角色

[IAM 角色](#)是 Amazon Web Services 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过[切换角色](#)，在 [Amazon Web Services Management Console](#) 中暂时代入 IAM 角色。您可以

调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 以代入角色。有关使用角色的方法的更多信息，请参阅 IAM 用户指南 中的 [使用 IAM 角色](#)。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 临时 IAM 用户权限 – IAM 用户可以代入 IAM 角色，以暂时获得不同的权限以执行特定的任务。
- 联合身份用户访问 – 您可以不创建 IAM 用户，而是使用来自 Amazon Directory Service、您的企业用户目录或 Web 身份提供商的现有身份。这些用户被称为联合用户。在通过 [身份提供商请求访问权限](#) 时，Amazon 将为联合身份用户分配角色。有关联合身份用户的更多信息，请参阅 IAM 用户指南 中的 [联合身份用户和角色](#)。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信委托人）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 Amazon 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南 中的 [IAM 角色与基于资源的策略有何不同](#)。
- 跨服务访问 – 某些 Amazon 服务使用其他 Amazon 服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的委托人的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 委托人权限 – 当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为委托人。策略向委托人授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关操作，请参阅 [的操作、资源和条件键](#) Amazon 账户管理 中的服务授权参考。
  - 服务角色 – 服务角色是服务代表您在您的账户中执行操作而担任的 [IAM 角色](#)。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅 IAM 用户指南 中的 [创建向 Amazon 服务委派权限的角色](#)。
  - 服务相关角色 – 服务相关角色是与 Amazon 服务关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南 中的 [使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限](#)。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南 中的 [何时创建 IAM 角色（而不是用户）](#)。

## 使用策略管理访问

您将创建策略并将其附加到 IAM 身份或 Amazon 资源，以便控制 Amazon 中的访问。策略是 Amazon 中的对象；在与标识或资源相关联时，策略定义它们的权限。您可以通过 root 用户或 IAM 用户身份登录，也可以代入 IAM 角色。随后，当您提出请求时，Amazon 会评估相关的基于身份或基于资源的策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 Amazon 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅 [JSON 策略概述](#) 中的 IAM 用户指南。

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

每个 IAM 实体（用户或角色）最初没有任何权限。换言之，默认情况下，用户什么都不能做，甚至不能更改他们自己的密码。要为用户授予执行某些操作的权限，管理员必须将权限策略附加到用户。或者，管理员可以将用户添加到具有预期权限的组中。当管理员为某个组授予访问权限时，该组内的全部用户都会获得这些访问权限。

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



## 基于身份的策略

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

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是可以附加到中的多个用户、组和角色的独立策略。Amazon Web Services 账户托管策略包括 Amazon 托管策略和客户托管策略。要了解如何在托管策略或内联策略之间选择，请参阅[在托管策略与内联策略之间进行选择](#)中的 IAM 用户指南。

## 基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定委托人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[指定委托人](#)。委托人可以包括账户、用户、角色、联合身份用户或 Amazon 服务。

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

## 访问控制列表 (ACL)

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

Amazon S3、Amazon WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅[访问控制列表 \(ACL\) 概述](#)中的 Amazon Simple Storage Service 开发人员指南。

## 其他策略类型

Amazon 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体的基于身份的策略及其权限边界的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南 中的 [IAM 实体的权限边界](#)。
- 服务控制策略 (SCP) SCP 是指定中的组织或组织单位 (OU) 的最大权限的 JSON 策略。Amazon Organizations Amazon Organizations 是用于分组和集中管理多个服务 Amazon Web Services 账户的企业拥有的。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体的权限，包括每个 Amazon Web Services 账户根用户。有关 Organizations 和 SCP 的更多信息，请参阅《Amazon Organizations 用户指南》中的 [SCP 的工作原理](#)。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 [会话策略](#) 中的 IAM 用户指南。

## 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 Amazon 如何确定在涉及多种策略类型时是否允许请求，请参阅 IAM 用户指南中的 [策略评估逻辑](#)。

## 的方法 Amazon 账户管理与 IAM 协同工作

在使用 IAM 管理对账户管理的访问权限之前，请了解哪些 IAM 功能可与账户管理协同工作。

## 可与 IAM 一起使用的功能 Amazon 账户管理

IAM 功能	账户管理支持
<a href="#">基于身份的策略 (p. 49)</a>	是
<a href="#">基于资源的策略 (p. 49)</a>	否
<a href="#">策略操作 (p. 50)</a>	是
<a href="#">策略资源 (p. 50)</a>	是
<a href="#">策略条件键 (p. 51)</a>	是
<a href="#">ACL (p. 52)</a>	否
<a href="#">ABAC (策略中的标签) (p. 52)</a>	是
<a href="#">临时凭证 (p. 52)</a>	是
<a href="#">委托人权限 (p. 53)</a>	是
<a href="#">服务角色 (p. 53)</a>	否
<a href="#">服务相关角色 (p. 53)</a>	否

要了解账户管理和其他方法的概述 Amazon 服务适用于大多数 IAM 功能，请参阅 [Amazon 使用 IAM 的服务](#) 中的 IAM 用户指南。

## 针对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 [创建 IAM 策略](#) 中的 IAM 用户指南。

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

## 针对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示例，请参阅 [适用于的基于身份的策略示例 Amazon 账户管理 \(p. 53\)](#)。

## 账户管理中基于资源的策略

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，策略定义指定委托人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[指定委托人](#)。委托人可以包括账户、用户、角色、联合身份用户或 Amazon 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委托人。将跨账户委托人添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同的 Amazon Web Services 账户中时，则信任账户中的 IAM 管理员还必须授予委托人实体（用户或角色）对资源的访问权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的委托人授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的[IAM 角色与基于资源的策略有何不同](#)。

## 账户管理的策略操作

支持策略操作	是
--------	---

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

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

在策略中包含操作以授予执行相关操作的权限。

要查看账户管理操作的列表，请参阅[由定义的操作 Amazon 账户管理](#)中的服务授权参考。

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 Amazon Web Services 账户的备用联系人，包括以下操作。

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

要查看账户管理基于身份的策略示例，请参阅[适用于的基于身份的策略示例 Amazon 账户管理 \(p. 53\)](#)。

## 账户管理的政策资源

支持策略资源	是
--------	---

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

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 [Amazon Resource Name \( ARN \)](#) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

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

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

账户管理服务支持 IAM 策略中的以下特定资源类型 Resources 元素来帮助你过滤策略并区分这些类型的 Amazon Web Services 账户：

- 账户

该 resource 类型只能独立匹配 Amazon Web Services 账户不是由 Amazon Organizations 服务。

- 组织中的账户

该 resource 仅适用于类型 Amazon Web Services 账户属于由 Amazon Organizations 服务。

要查看账户管理资源类型及其 ARN 的列表，请参阅。[由 定义的资源 Amazon 账户管理 中的服务授权参考](#)。要了解您可以使用哪些操作指定每个资源的 ARN，请参阅。[由 定义的操作 Amazon 账户管理](#)。

要查看账户管理基于身份的策略示例，请参阅。[适用于 的基于身份的策略示例 Amazon 账户管理 \(p. 53\)](#)。

## 适用于账户管理的策略条件键

支持策略条件密钥	是
----------	---

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个委托人 可以对什么资源执行操作，以及在什么 条件 下执行。

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

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

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅 IAM 用户指南 中的 [IAM 策略元素：变量和标签](#)。

Amazon 支持全局条件键和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅 IAM 用户指南中的 [Amazon 全局条件上下文键](#)。

账户管理服务支持以下条件密钥，您可以使用这些密钥为 IAM 策略提供精细筛选：

- 账户：目标区域

此条件键接受一个参数，该参数包括 [Amazon 区域代码](#)。它允许您筛选策略，以仅影响应用于指定区域的那些操作。

- 账户：替代联系人类型

此条件键获取替代联系人类型的列表：

- 计费
- 操作

- SECURITY

使用此键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：账户资源或路径

此条件键接受一个参数，该参数由 ARN 的列表组成，其中包含表示组织中的帐户的通配符。它允许您筛选策略，以仅影响那些针对具有匹配 ARN 的帐户的操作。例如，以下 ARN 仅匹配指定组织中的那些帐户和指定的组织单位 (OU)。

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

- 账户：账户资源或标签

此条件键接受一个由标签键和值列表组成的参数。它允许您筛选策略，以仅影响属于组织成员且使用指定标签键和值进行标记的帐户。

要查看账户管理条件键的列表，请参阅[条件键 Amazon 账户管理](#)中的服务授权参考。要了解您可以对哪些操作和资源使用条件键，请参阅[由定义的操作 Amazon 账户管理](#)。

要查看账户管理基于身份的策略示例，请参阅[适用于的基于身份的策略示例 Amazon 账户管理 \(p. 53\)](#)。

## 账户管理中的访问控制列表

支持 ACL	否
--------	---

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

## 将基于属性的访问控制用于账户

支持 ABAC ( 策略中的标签 )	是
--------------------	---

基于属性的访问控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在 Amazon 中，这些属性称为标签。您可以将标签附加到 IAM 实体 ( 用户或角色 ) 以及 Amazon 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在委托人的标签与他们尝试访问的资源标签匹配时允许操作。

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

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

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的[什么是 ABAC ?](#)。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的[使用基于属性的访问控制 \( ABAC \)](#)。

## 将临时凭证用于账户管理

支持临时凭证	是
--------	---

某些 Amazon 服务在您使用临时凭证登录时无法正常工作。有关更多信息，包括 Amazon 服务与临时凭证配合使用，请参阅《IAM 用户指南》中的[使用 IAM 的 Amazon 服务](#)。

如果您不使用用户名和密码而用其他方法登录到 Amazon Web Services Management Console，则使用临时凭证。例如，当您使用贵公司的单点登录（SSO）链接访问 Amazon 时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的[切换到角色（控制台）](#)。

您可以使用 Amazon CLI 或者 Amazon API 创建临时凭证。之后，您可以使用这些临时凭证访问 Amazon。Amazon 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅 [IAM 中的临时安全凭证](#)。

## 账户管理的跨服务委托人权限

支持委托人权限	是
---------	---

当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为委托人。策略向委托人授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关操作，请参阅 [的操作、资源和条件键 Amazon 账户管理](#) 中的服务授权参考。

## 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 Amazon 服务委派权限的角色](#)。

## 用于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 Amazon 服务相关的服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

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

## 适用于 的基于身份的策略示例 Amazon 账户管理

默认情况下，IAM 用户和角色没有创建或修改账户管理资源的权限。它们还无法使用 Amazon Web Services Management Console、Amazon CLI 或 Amazon API 执行任务。IAM 管理员必须创建 IAM 策略，以便为用户和角色授予权限，以对所需资源执行操作。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅 IAM 用户指南 中的 [在 JSON 选项卡上创建策略](#)。

### 主题

- [策略最佳实践 \(p. 54\)](#)
- [使用中的账户管理设置页面 Amazon Web Services Management Console \(p. 54\)](#)
- [提供对“账户设置”页面的只读访问权限 Amazon Web Services Management Console \(p. 54\)](#)
- [提供对“账户设置”页面的完全访问权限 Amazon Web Services Management Console \(p. 55\)](#)

## 策略最佳实践

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

- 开始使用Amazon托管策略— 要快速开始使用账户管理，请使用Amazon托管策略，以便为您的员工授予所需的权限。这些策略已在您的账户中提供，并由 Amazon 维护和更新。有关更多信息，请参阅 IAM 用户指南中的[开始使用 Amazon 托管策略](#)中的权限。
- 授予最低权限 – 创建自定义策略时，仅授予执行任务所需的许可。最开始只授予最低权限，然后根据需要授予其他权限。这样做比起一开始就授予过于宽松的权限而后再尝试收紧权限来说更为安全。有关更多信息，请参阅 IAM 用户指南 中的[授予最低权限](#)。
- 为敏感操作启用 MFA – 为了提高安全性，要求 IAM 用户使用多重验证 (MFA) 访问敏感资源或 API 操作。有关更多信息，请参阅《IAM 用户指南》中的[在 Amazon 中使用多重身份验证 \(MFA\)](#)。
- 使用策略条件来增强安全性 – 在切实可行的范围内，定义基于身份的策略在哪些情况下允许访问资源。例如，您可编写条件来指定请求必须来自允许的 IP 地址范围。您也可以编写条件，以仅允许指定日期或时间范围内的请求，或者要求使用 SSL 或 MFA。有关更多信息，请参阅 [IAM JSON 策略元素](#)：[Condition](#)中的IAM 用户指南。

## 使用中的账户管理设置页面Amazon Web Services Management Console

要访问账户设置中的页面Amazon Web Services Management Console，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您的详细信息。Amazon Web Services 账户. 如果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或者AWSAccountManagementFullAccess Amazon适用于实体的托管策略。有关更多信息，请参阅 IAM 用户指南 中的[为用户添加权限](#)。

对于只需要调用 Amazon CLI 或 Amazon API 的用户，您无需为其提供最低控制台权限。相反，在许多情况下，您可以选择仅允许访问与您尝试执行的 API 操作相匹配的操作。

## 提供对“账户设置”页面的只读访问权限Amazon Web Services Management Console

在以下示例中，您想要为您的 IAM 用户授予Amazon Web Services 账户访问“账户设置”页面的只读访问权限Amazon Web Services Management Console. 附加了此策略的用户无法进行任何更改。

这些区域有：`aws-portal:ViewAccount`授予查看大多数设置的访问权限账户设置页. 但是，要查看当前启用的Amazon您还必须包括`account:ListRegions`action.

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

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

在以下示例中，您想要为您的 IAM 用户授予 Amazon Web Services 账户访问“账户设置”页面的完全访问权限 Amazon Web Services Management Console。附加了此策略的用户可以更改帐户的设置。

此示例策略建立在前面的示例策略之上，方法是添加 `aws-portal:ModifyAccount` 权限，允许用户更改帐户的大部分设置，还可以添加 `account:EnableRegion` 和 `account:DisableRegion` 权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GrantFullAccessToAccountSettings",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewAccount",
        "account:ListRegions",
        "aws-portal:ModifyAccount",
        "account:EnableRegion",
        "account:DisableRegion"
      ],
      "Resource": "*"
    }
  ]
}
```

## 故障排除Amazon账户管理身份和访问权限

可以使用以下信息，以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。

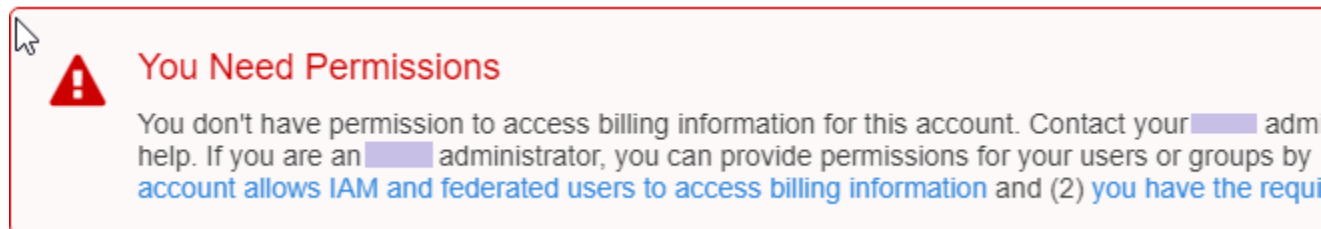
### 主题

- [我无权在账户设置页面中执行操作 \(p. 55\)](#)
- [我无权执行iam:PassRole \(p. 56\)](#)
- [我想要查看我的访问密钥 \(p. 56\)](#)
- [我是管理员并希望允许其他人访问我的账户详细信息 \(p. 56\)](#)
- [我想要允许我之外的人Amazon Web Services 账户访问我的账户详细信息 \(p. 56\)](#)

## 我无权在账户设置页面中执行操作

如果 Amazon Web Services Management Console 告诉您，您无权执行某个操作，则必须联系您的管理员寻求帮助。您的管理员是指为您提供用户名和密码的那个人。

下面的示例错误发生在 `mateojacksonIAM` 用户尝试使用控制台来查看有关其的详细信息 Amazon Web Services 账户中的 `Account Settings` 的页面 Amazon Web Services Management Console 但是没有 `aws-portal:ViewAccount` 权限。





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

如果您收到错误消息，提示您无权执行 `iam:PassRole` 操作，则必须联系您的管理员寻求帮助。您的管理员是指为您提供用户名和密码的那个人。请求该人员更新您的策略，以便允许您将角色传递给账户管理。

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

当名为的 IAM 用户时，会发生以下示例错误。marymajor 尝试使用控制台在账户管理中执行操作。但是，服务必须具有服务角色所授予的权限才可执行操作。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，Mary 请求她的管理员来更新其策略，以允许她执行 `iam:PassRole` 操作。

## 我想要查看我的访问密钥

在创建 IAM 用户访问密钥后，您可以随时查看您的访问密钥 ID。但是，您无法再查看您的秘密访问密钥。如果您丢失了私有密钥，则必须创建一个新的访问密钥对。

访问密钥包含两部分：访问密钥 ID（例如 AKIAIOSFODNN7EXAMPLE）和秘密访问密钥（例如 wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY）。与用户名和密码一样，您必须同时使用访问密钥 ID 和秘密访问密钥对请求执行身份验证。像对用户名和密码一样，安全地管理访问密钥。

### Important

请不要向第三方提供访问密钥，即便是为了帮助找到您的规范用户 ID 也不行。如果您这样做，可能会向某人提供对您的账户的永久访问权限。

当您创建访问密钥对时，系统会提示您将访问密钥 ID 和秘密访问密钥保存在一个安全位置。秘密访问密钥仅在您创建它时可用。如果丢失了您的秘密访问密钥，您必须为 IAM 用户添加新的访问密钥。您最多可拥有两个访问密钥。如果您已有两个密钥，则必须删除一个密钥对，然后再创建新的密钥。要查看说明，请参阅 IAM 用户指南中的 [管理访问密钥](#)。

## 我是管理员并希望允许其他人访问我的账户详细信息

要允许其他人访问账户管理，您必须为需要访问权限的人员或应用程序创建一个 IAM 实体（用户或角色）。它们将使用该实体的凭证访问 Amazon。然后，您必须将策略附加到实体，以便在账户管理中向其授予正确的权限。

要立即开始使用，请参阅 IAM 用户指南中的 [创建您的第一个 IAM 委派用户和组](#)。

## 我想要允许我之外的人 Amazon Web Services 账户访问我的账户详细信息

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 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

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 [的方法 Amazon 账户管理与 IAM 协同工作 \(p. 48\)](#)。
- 要了解如何为您拥有的 Amazon Web Services 账户中的资源提供访问权限，请参阅 IAM 用户指南中的 [为您拥有的另一个 Amazon Web Services 账户中的 IAM 用户提供访问权限](#)。



- 要了解如何为第三方Amazon Web Services 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的[为第三方拥有的Amazon Web Services 账户提供访问权限](#)。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南 中的[为经过外部身份验证的用户（联合身份验证）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 角色与基于资源的策略有何不同](#)。

## Amazon适用于 的托管策略Amazon账户管理

Amazon账户管理目前提供两个Amazon可供您使用的托管策略：

- [Amazon托管策略：Amazon 账户管理只读访问 \(p. 57\)](#)
- [Amazon托管策略：Amazon 账户管理完全访问 \(p. 58\)](#)
- [更新账户管理Amazon托管策略 \(p. 58\)](#)

要向用户、组和角色添加权限，与自己编写策略相比，使用 Amazon 托管策略更简单。创建仅为团队提供所需权限的 [IAM 客户托管策略](#)需要时间和专业知识。要快速入门，您可以使用我们的Amazon托管式策略。这些策略涵盖常见使用案例，可在您的Amazon Web Services 账户中使用。有关 Amazon 托管策略的更多信息，请参阅《IAM 用户指南》中的[Amazon 托管策略](#)。

Amazon服务负责维护和更新Amazon托管式策略。您无法更改Amazon托管策略中的权限。服务偶尔会向Amazon托管式策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新功能或新操作可用时，服务最有可能更新Amazon托管策略。服务不会从Amazon托管策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，Amazon还支持跨多种服务的工作职能的托管式策略。例如，ViewOnlyAccess Amazon托管策略提供对所有Amazon服务和资源的只读访问权限。当服务启动新功能时，Amazon会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅《IAM 用户指南》中的[适用于工作职能的Amazon托管式策略](#)。

## Amazon托管策略：Amazon 账户管理只读访问

您可以将 `AWSAccountManagementReadOnlyAccess` 策略附加得到 IAM 身份。

此策略提供只读权限，以便仅查看以下内容：

- 关于你的元数据Amazon Web Services 账户
- 这些区域有：Amazon Web Services 区域已启用或禁用Amazon Web Services 账户（您只能通过使用 Amazon控制台）

它通过授予运行任何`Get*`或者`List*`操作。它不提供任何修改账户元数据或启用或禁用的功能Amazon Web Services 区域对于账户。

权限详细信息

此策略包含以下权限。

- `account`— 允许委托人检索有关的元数据信息Amazon Web Services 账户。它还允许委托人列出Amazon Web Services 区域在中为账户启用的Amazon Web Services Management Console。

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

```
{
  "Effect": "Allow",
  "Action": [
    "account:Get*",
    "account:List*"
  ],
  "Resource": "*"
}
```

## Amazon托管策略：Amazon 账户管理完全访问

您可以将 `AWSAccountManagementFullAccess` 策略附加得到 IAM 身份。

此策略提供查看或修改以下内容的完全管理访问权限：

- 关于你的元数据Amazon Web Services 账户
- 这些区域有：Amazon Web Services 区域已启用或禁用Amazon Web Services 账户（您只能通过使用 Amazon控制台）

它通过授予运行任何权限来实现此目的account操作。

权限详细信息

此策略包含以下权限。

- `account`— 允许承担者查看或修改有关的元数据信息Amazon Web Services 账户。它还允许委托人列出 Amazon Web Services 区域已为账户启用并在Amazon Web Services Management Console。

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

## 更新账户管理Amazon托管策略

查看有关更新的详细信息Amazon此服务开始跟踪这些更改起，适用于账户管理的托管策略。要获得有关此页面更改的自动提示，请订阅账户管理文档历史记录页面上的 RSS 源。

更改	描述	日期
Amazon账户管理启动了新Amazon托管策略并开启跟踪更改	账户管理最初启动时有以下内容Amazon托管策略： <ul style="list-style-type: none"><li>• <a href="#">Amazon 账户管理只读访问 (p. 57)</a></li><li>• <a href="#">Amazon 账户管理完全访问 (p. 58)</a></li></ul>	2021 年 9 月 30 日

## 的合规性验证Amazon账户管理

第三方审计员评估的安全性和合规性Amazon可以在Amazon Web Services 账户作为多个组成部分Amazon 合规性计划。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

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

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

您在您的中使用服务时的合规责任Amazon Web Services 账户由您的数据的敏感性、您的公司的合规性目标以及适用的法律法规决定。Amazon以下资源来帮助实现合规性：

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

## 中的故障恢复能力Amazon账户管理

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

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

## Amazon Account Management 中的基础设施安全性

作为托管服务，Amazon您可以使用的服务Amazon Web Services 账户受保护Amazon中描述的全局网络安全程序[Amazon Web Services：概述安全过程](#)白皮书。

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

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

# 监控 Amazon 账户管理

监控是保持可靠性、可用性和性能的重要环节。Amazon 账户管理和您的其他 Amazon 解决方案。Amazon 提供以下监控工具来监控账户管理、在出现错误时进行报告并在适当的时候采取自动化措施：

- Amazon CloudTrail 捕获（记录）由您发出或代表该项目发出的 API 调用和相关事件。Amazon Web Services 账户并将日志文件写入您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶。这可以让你识别哪些用户和帐户调用了 Amazon、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 [Amazon CloudTrail 用户指南](#)。

## 日志系统 Amazon 使用账户管理 API 调用 Amazon CloudTrail

这些区域有：Amazon 账户管理 API 与 Amazon CloudTrail，提供用户、角色或用户所执行操作的记录的服务。Amazon 调用账户管理操作的服务。CloudTrail 会将所有账户管理 API 调用作为事件捕获。捕获的呼叫包括对账户管理操作的所有呼叫。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括账户管理操作的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。使用 CloudTrail 收集的信息，您可以确定调用账户管理操作的请求、发出请求的 IP 地址、发出请求的发出时间以及其他详细信息。

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

## CloudTrail 中的账户管理信息

CloudTrail 在您的 Amazon Web Services 账户当您创建账户时。当账户管理操作中发生活动时，CloudTrail 会在 CloudTrail 事件中记录该活动以及其他活动。Amazon 中的服务事件事件记录。您可以在中查看、搜索和下载最新事件 Amazon Web Services 账户。有关更多信息，请参阅 [使用 CloudTrail 事件历史记录查看事件](#)。

要持续记录 Amazon Web Services 账户（包括账户管理操作的事件），请创建跟踪。通过跟踪，CloudTrail 可将日志文件传送到 Amazon S3 存储桶。默认情况下，在中创建跟踪时 Amazon Web Services Management Console，该跟踪适用于所有 Amazon Web Services 区域。此跟踪在 Amazon 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 Amazon 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取措施。有关更多信息，请参阅下列内容：

- [创建跟踪概述](#)
- [CloudTrail 支持的服务和集成](#)
- [为 CloudTrail 配置 Amazon SNS 通知](#)
- [从多个区域接收 CloudTrail 日志文件](#)
- [从多个账户接收 CloudTrail 日志文件](#)

Amazon CloudTrail 记录在中找到的所有账户管理 API 操作 [API 参考 \(p. 64\)](#) 本指南的部分。例如，对 `CreateAccount`、`DeleteAlternateContact`，和 `PutAlternateContact` 操作会在 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。身份信息可帮助您确定以下内容：

- 请求是使用根用户发出的还是 Amazon Identity and Access Management (IAM) 用户证书

- 请求是使用 IAM 角色还是联合身份用户的临时安全凭证发出的
- 请求是否由其他 Amazon 服务发出

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

## 了解账户管理日志条目

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

示例 1：以下 CloudTrail 显示对 `GetAlternateContact` 操作来检索当前 OPERATIONS 账户的备用联系人。操作返回的值不包括在记录的信息中。

### Example 示例 1

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "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 CloudTrail 显示对 `PutAlternateContact` 添加新操作 BILLING 账户的备用联系人。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:08Z",
  "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 CloudTrail 显示对DeleteAlternateContact删除当前OPERATIONS备用联系。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {}
    }
  }
}
```

```
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-04-30T18:33:00Z"
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "DeleteAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "OPERATIONS"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```



# API 参考

账户管理中的 API 操作 ( account) 命名空间使您能够修改 Amazon Web Services 账户。

每个 Amazon Web Services 账户支持包含有关账户信息的元数据，包括与该账户关联的最多三个备用联系人的信息。除了与账户的 root 用户关联的电子邮件地址之外，这些都是补充的。您可以只指定与账户相关联的以下联系类型之一。

- 联系账单
- 联系操作
- 联系安全

默认情况下，本指南中讨论的 API 操作直接应用于调用该操作的账户。这些区域有：[身份](#)在调用该操作的账户中，通常是 IAM 角色或 IAM 用户，必须具有 IAM 策略应用的权限才能调用 API 操作。或者，您可以从中的某个身份调用这些 API 操作。Amazon Organizations 管理帐户并指定任何账户 ID 号 Amazon Web Services 账户这是该组织的成员。

## API 版本

此版本的账户 API 参考文档了账户管理 API 版本 2021-02-01。

### Note

作为直接使用 API 的替代方案，您可以使用 Amazon 开发工具包，包含各种编程语言和平台（Java、Ruby、.NET、iOS、Android 等）的库文件和示例代码。开发工具包提供便捷的方式来创建对 Amazon Organizations。例如，开发工具包执行加密签署请求、管理错误以及自动重试请求。有关 Amazon 开发工具包的更多信息（包括如何下载和安装这些工具包），请参阅[适用于 Amazon Web Services 的工具](#)。

建议您使用 Amazon SDK 用于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 Web 服务。要了解有关账户管理查询 API 的更多信息，请参阅[发出 HTTP 查询请求](#)在账户管理用户指南中。Organizations 支持所有操作的 GET 和 POST 请求。也就是说，API 不要求您使用某些操作的 GET 请求和其他操作的 POST 请求。然而，GET 请求受 URL 的大小限制。因此，对于要求更高的操作，请使用 POST 请求。

## 签署请求

当你将 HTTP 请求发送到 Amazon，你必须签署请求才能 Amazon 可以识别谁发送了他们。你用你的签署请求 Amazon 访问密钥，包含访问密钥 ID 和一个私有访问密钥密钥。我们强烈建议您不要为根账户创建访问密钥。拥有您的根账户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，请为具有管理权限的 IAM 用户账户创建访问密钥。作为另一种选择，请使用 Amazon 使用安全令牌服务生成临时安全凭证，并使用这些凭证对请求进行签名。

要签署请求，我们建议您使用[签名版本 4](#)。如果您的现有应用程序使用签名版本 2，则无需更新它即可使用签名版本 4。但是，有些操作现在需要签名版本 4。需要版本 4 的操作的文档表明了这一要求。

当您使用 Amazon 命令行界面 (Amazon CLI) 或其中一个 Amazon SDK 可以向 Amazon 中，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 Support 和反馈

我们欢迎您提供反馈。将评论发送到[feedback-awsaccounts@amazon.com](mailto:feedback-awsaccounts@amazon.com)或者，将反馈和问题发布在[账户管理支持论坛](#)。有关 Amazon 支持论坛的更多信息，请参阅[论坛帮助](#)。

## 例子是如何呈现的

账户管理作为响应您的请求而返回的 JSON 将作为单个长字符串返回，不带换行符或格式化空格。本指南的示例中显示了换行符和空格，以提高可读性。当示例输入参数也会导致超出屏幕的长字符串时，我们插入换行符以增强可读性。您应始终将输入作为单个 JSON 文本字符串提交。

#### 记录 API 请求

账户管理支持 CloudTrail，这是一项记录的服务 Amazon 您的 API 调用 Amazon Web Services 账户并将日志文件传送至 Amazon S3 存储桶。通过使用 CloudTrail 收集的信息，您可以确定向账户管理成功发出了什么请求、何人发出的请求以及发出请求的时间等。有关账户管理及其对 CloudTrail 的支持的更多信息，请参阅 [日志系统 Amazon 使用账户管理 API 调用 Amazon CloudTrail \(p. 60\)](#)。要了解有关 CloudTrail 的更多信息（包括如何启用该服务及如何查找日志文件），请参阅 [Amazon CloudTrail 用户指南](#)。

## Actions

支持以下操作：

- [DeleteAlternateContact \(p. 66\)](#)
- [GetAlternateContact \(p. 69\)](#)
- [PutAlternateContact \(p. 73\)](#)

## DeleteAlternateContact

删除指定的备用联系人Amazon Web Services 账户。

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

### Note

在更新备用联系人信息之前Amazon Web Services 账户这是由管理Amazon Organizations，您必须先启用Amazon账户管理和 Organizations。有关更多信息，请参阅[启用可信访问权限Amazon账户管理](#)。

## 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 (p. 66)

指定的 12 位数账户 ID 号Amazon要使用此操作访问或修改的账户。

如果未指定此参数，则默认为Amazon调用操作时使用的身份账户。

要使用此参数，调用者必须是**组织的管理账户**或委派管理员帐户，并且指定的账户 ID 必须是同一组织中的成员帐户。组织必须有**启用所有功能**，而且组织必须有**可信访问**为账户管理服务启用，还可以选择**委托管理员**已分配账户。

### Note

管理账户无法指定自己的AccountId; 它必须在独立上下文中调用操作，方法是不包括AccountId参数。

要对不是组织成员的帐户调用此操作，请不要指定此参数，并使用属于您希望检索或修改其联系人的帐户的身份来调用该操作。

类型: String

模式: `^\d{12}$`

: 必需 否

### AlternateContactType (p. 66)

指定要删除哪些备用联系人。

类型: String

有效值: BILLING | OPERATIONS | SECURITY

: 必需 是

## 响应语法

```
HTTP/1.1 200
```

## 响应元素

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

## Errors

有关所有操作常见错误的信息，请参阅[常见错误 \(p. 80\)](#)。

### AccessDeniedException

由于调用身份没有所需的最低权限，因此操作失败。

HTTP 状态代码：403

### InternalServerError

操作失败是因为内部的错误Amazon。请稍后重试操作。

HTTP 状态代码：500

### ResourceNotFoundException

操作失败是因为它指定了找不到的资源。

HTTP 状态代码：404

### TooManyRequestsException

操作失败是因为调用频率太高且超过了限制限制。

HTTP 状态代码：429

### ValidationException

操作失败，因为其中一个输入参数无效。

HTTP 状态代码：400

## Examples

### 示例 1

以下示例将删除其凭据用于调用该操作的账户的安全备用联系人。

#### 示例请求

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact
{ "AlternateContactType": "SECURITY" }
```

### 示例响应

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

### 示例 2

以下示例删除组织中指定成员账户的账单备用联系人。您必须使用组织管理帐户或账户管理服务的委派管理  
员帐户中的凭证。

### 示例请求

```
POST / HTTP/1.1  
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact  
  
{ "AccountId": "123456789012", "AlternateContactType": "BILLING" }
```

### 示例响应

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

## 另请参阅

有关在特定语言的Amazon软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

## GetAlternateContact

检索附加到的指定备用联系人 Amazon Web Services 账户。

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

### Note

在更新备用联系人信息之前 Amazon Web Services 账户这是由管理 Amazon Organizations，您必须先启用 Amazon 账户管理和 Organizations。有关更多信息，请参阅[启用可信访问权限 Amazon 账户管理](#)。

## 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 (p. 69)

指定的 12 位数账户 ID 号 Amazon 要使用此操作访问或修改的账户。

如果未指定此参数，则默认为 Amazon 调用操作时使用的身份账户。

要使用此参数，调用者必须是[组织的管理账户](#)或委派管理员帐户，并且指定的账户 ID 必须是同一组织中的成员帐户。组织必须有[启用所有功能](#)，而且组织必须有[可信访问](#)为账户管理服务启用，还可以选择[委托管理员](#)已分配账户。

### Note

管理账户无法指定自己的 AccountId；它必须在独立上下文中调用操作，方法是不包括 AccountId 参数。

要对不是组织成员的帐户调用此操作，请不要指定此参数，并使用属于您希望检索或修改其联系人的帐户的身份来调用该操作。

类型: String

模式: `^\d{12}$`

: 必需 否

### AlternateContactType (p. 69)

指定要检索的备用联系人。

类型: String

有效值: BILLING | OPERATIONS | SECURITY

: 必需 是

## 响应语法

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

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

## 响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回的以下数据。

[AlternateContact \(p. 70\)](#)

包含指定备用联系人的详细信息结构。

类型：[AlternateContact \(p. 78\)](#) 对象

## Errors

有关所有操作常见错误的信息，请参阅[常见错误 \(p. 80\)](#)。

### AccessDeniedException

由于调用身份没有所需的最低权限，因此操作失败。

HTTP 状态代码：403

### InternalServerError

操作失败是因为内部的错误Amazon。请稍后重试操作。

HTTP 状态代码：500

### ResourceNotFoundException

操作失败是因为它指定了找不到的资源。

HTTP 状态代码：404

### TooManyRequestsException

操作失败是因为调用频率太高且超过了限制限制。

HTTP 状态代码：429

### ValidationException

操作失败，因为其中一个输入参数无效。



HTTP 状态代码 : 400

## Examples

### 示例 1

以下示例检索其凭据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。您必须使用组织管理帐户或账户管理服务的委派管理员帐户中的凭证。

#### 示例请求

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

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

#### 示例响应

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

## 另请参阅

有关在特定语言的Amazon软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

## PutAlternateContact

修改附加到Amazon Web Services 账户。

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

### Note

在更新备用联系人信息之前Amazon Web Services 账户这是由管理Amazon Organizations，您必须先启用Amazon账户管理和 Organizations。有关更多信息，请参阅 [启用可信访问权限Amazon账户管理](#)。

## 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 (p. 73)

指定的 12 位数账户 ID 号Amazon要使用此操作访问或修改的账户。

如果未指定此参数，则默认为Amazon调用操作时使用的身份账户。

要使用此参数，调用者必须是[组织的管理账户](#)或委派管理员帐户，并且指定的账户 ID 必须是同一组织中的成员帐户。组织必须有[启用所有功能](#)，而且组织必须有[可信访问](#)为账户管理服务启用，还可以选择[委托管理员](#)已分配账户。

### Note

管理账户无法指定自己的AccountId; 它必须在独立上下文中调用操作，方法是不包括AccountId参数。

要对不是组织成员的帐户调用此操作，请不要指定此参数，并使用属于您希望检索或修改其联系人的帐户的身份来调用该操作。

类型: String

模式: `^\d{12}$`

: 必需 否

### AlternateContactType (p. 73)

指定要创建或更新哪个备用联系人。

类型: String

有效值: BILLING | OPERATIONS | SECURITY

: 必需 是

#### [EmailAddress \(p. 73\)](#)

指定备用联系人的电子邮件地址。

类型: String

长度约束: 最小长度为 1。最大长度为 64。

模式: `[\w+=,.-]+@[ \w.- ]+\.[ \w ]+`

: 必需 是

#### [Name \(p. 73\)](#)

指定备用联系人的姓名。

类型: String

长度约束: 最小长度为 1。最大长度为 64。

: 必需 是

#### [PhoneNumber \(p. 73\)](#)

指定备用联系人的电话号码。

类型: String

长度约束: 最小长度为 1。长度上限为 25。

模式: `^\s0-9()+-]+$`

: 必需 是

#### [Title \(p. 73\)](#)

指定备用联系人的标题。

类型: String

长度约束: 最小长度为 1。长度上限为 50。

: 必需 是

## 响应语法

```
HTTP/1.1 200
```

## 响应元素

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

## Errors

有关所有操作常见错误的信息，请参阅[常见错误 \(p. 80\)](#)。

#### AccessDeniedException

由于调用身份没有所需的最低权限，因此操作失败。

HTTP 状态代码：403

#### InternalServerErrorException

操作失败是因为内部的错误Amazon. 请稍后重试操作。

HTTP 状态代码：500

#### TooManyRequestsException

操作失败是因为调用频率太高且超过了限制限制。

HTTP 状态代码：429

#### ValidationException

操作失败，因为其中一个输入参数无效。

HTTP 状态代码：400

## Examples

### 示例 1

以下示例为其凭据用于调用该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

以下示例设置或覆盖组织中指定成员账户的账单备用联系人。您必须使用组织管理帐户或账户管理服务的委派管理员帐户中的凭证。

#### 示例请求

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

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

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

### 示例响应

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

## 另请参阅

有关在特定语言的Amazon软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

## 其他中的相关操作Amazon服务

以下操作与相关：Amazon Account Management但是是是是是Amazon Organizations命名空间：

- [CreateAccount](#) (p. 76)
- [CreateGovCloudAccount](#) (p. 76)
- [DescribeAccount](#) (p. 76)

## CreateAccount

这些区域有：CreateAccountAPI 操作仅可在由Amazon Organizations服务。API 操作在该服务的命名空间中定义。

有关更多信息，请参阅。[CreateAccount](#)中的Amazon OrganizationsAPI 参考。

## CreateGovCloudAccount

这些区域有：CreateGovCloudAccountAPI 操作仅可在由Amazon Organizations服务。API 操作在该服务的命名空间中定义。

有关更多信息，请参阅。[创建 GovCloud账户](#)中的Amazon OrganizationsAPI 参考。

## DescribeAccount

这些区域有：DescribeAccountAPI 操作仅可在由Amazon Organizations服务。API 操作在该服务的命名空间中定义。

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

## 数据类型

支持以下数据类型：

- [AlternateContact](#) (p. 78)



# AlternateContact

一种结构，其中包含与Amazon账户

## Contents

### AlternateContactType

备用联系人的类型。

类型: String

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: String

长度约束: 最小长度为 1。最大长度为 64。

模式: `[\w+=,.-]+@[\w.-]+\.[\w]+`

: 必需 否

### Name

与此备用联系人关联的姓名。

类型: String

长度约束: 最小长度为 1。最大长度为 64。

: 必需 否

### PhoneNumber

与此备用联系人关联的电话号码。

类型: String

长度约束: 最小长度为 1。长度上限为 25。

模式: `^\s0-9()+-]+$`

: 必需 否

### Title

与此备用联系人关联的标题。

类型: String

长度约束: 最小长度为 1。长度上限为 50。

: 必需 否

## 另请参阅

有关在特定语言的Amazon软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- [Amazon SDK for C++](#)
- [Amazon SDK for Go](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

## 常见参数

以下列表包含所有操作用于使用查询字符串对签名版本 4 请求进行签名的参数。所有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[签名版本 4 签名流程](#)中的 Amazon Web Services 一般参考。

### Action

要执行的操作。

类型：字符串

：必需 是

### Version

请求所针对的 API 版本，格式为 YYYYYYYY-MM-DD。

类型：字符串

：必需 是

### X-Amz-Algorithm

用于创建请求签名的哈希算法。

条件：在查询字符串而不是 HTTP 授权标头中包含身份验证信息时，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、目标区域、所请求的服务和终止字符串（“aws4\_request”）。此值采用以下格式表示：access\_key/YYYYMMDD/区域/服务/aws4\_请求。

有关更多信息，请参阅 [任务 2：为签名版本 4 创建待签字符串](#) 中的 Amazon Web Services 一般参考。

条件：在查询字符串而不是 HTTP 授权标头中包含身份验证信息时，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（YYYYYYMMDD'THHMMSS'Z'）。例如，以下日期时间是有效的 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。如果使用 ISO 8601 基本格式指定日期标头，则无需 X-Amz Date。使用 X-Amz Date 时，它始终会覆盖日期标头的值。有关更多信息，请参阅 [处理签名版本 4 中的日期](#) 中的 Amazon Web Services 一般参考。

类型：字符串

：必需 条件

X-Amz-Security-Token

通过致电获得的临时安全令牌(Amazon Security Token Service Amazon STS)。有关支持临时安全证书的服务列表，请访问 [Security Token Service Amazon 与 IAM 结合使用的服务](#) 中的 IAM 用户指南。

条件：如果您使用的临时安全凭证来自 Amazon 安全令牌服务，您必须包括安全令牌。

类型：字符串

：必需 条件

X-Amz-Signature

指定从待签字符串和派生的签名密钥计算的十六进制编码签名。

条件：在查询字符串而不是 HTTP 授权标头中包含身份验证信息时，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 [任务 1：创建签名版本 4 的规范请求](#) 中的 Amazon Web Services 一般参考。

条件：在查询字符串而不是 HTTP 授权标头中包含身份验证信息时，请指定此参数。

类型：字符串

：必需 条件

## 常见错误

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

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：400

IncompleteSignature

请求签名不符合 Amazon 标准。

HTTP 状态代码：400

InternalFailure

由于未知错误、异常或故障，请求处理失败。

HTTP 状态代码：500

InvalidAction

所请求的操作无效。验证操作是否已正确键入。

HTTP 状态代码：400

#### InvalidClientTokenId

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

HTTP 状态代码：403

#### InvalidParameterCombination

不得共用的参数被一起使用。

HTTP 状态代码：400

#### InvalidParameterValue

为输入参数提供的值无效或超出范围。

HTTP 状态代码：400

#### InvalidQueryParameter

这些区域有：Amazon 查询字符串格式异常或未遵循 Amazon 标准。

HTTP 状态代码：400

#### MalformedQueryString

查询字符串包含语法错误。

HTTP 状态代码：404

#### MissingAction

请求中遗漏了一个操作或必需参数。

HTTP 状态代码：400

#### MissingAuthenticationToken

请求中必须包含有效的（已注册的）Amazon 访问密钥 ID 或 X.509 证书。

HTTP 状态代码：403

#### MissingParameter

未提供用于指定操作的必需参数。

HTTP 状态代码：400

#### NotAuthorized

您没有执行该操作的权限。

HTTP 状态代码：400

#### OptInRequired

Amazon 访问密钥 ID 需要订阅服务。

HTTP 状态代码：403

#### RequestExpired

请求到达服务的时间超过请求上的日期戳或请求到期日期（如针对预签名 URL）15 分钟，或者请求上的日期戳离到期还有 15 分钟以上。

HTTP 状态代码：400

#### ServiceUnavailable

由于服务器发生临时故障而导致请求失败。

HTTP 状态代码：503

ThrottlingException

由于请求限制而导致请求被拒绝。

HTTP 状态代码：400

ValidationError

输入未能满足Amazon服务。

HTTP 状态代码：400

## 通过提出 HTTP 查询请求来调用 API

此部分大致介绍了如何使用适用于的查询 APIAmazon账户管理。有关 API 操作和错误的详细信息，请参阅 [API 参考 \(p. 64\)](#)。

Note

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

使用适用于的查询 APIAmazon账户管理，你可以调用服务操作。查询 API 请求是必须包含Action参数以指示要执行的操作。Amazon支持账户管理GET和POST请求所有操作。也就是说，API 不要求您使用GET对于一些操作和POST对于其他地址。但是，GET请求受 URL 的大小限制。尽管此限制与浏览器相关，但典型的限制为 2,048 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 \(p. 64\)](#)中的各个操作页面。

主题

- [Endpoints \(p. 82\)](#)
- [必须使用 HTTPS \(p. 82\)](#)
- [SIGNAmazon账户管理 API 请求 \(p. 82\)](#)

## Endpoints

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

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

## 必须使用 HTTPS

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

## SIGNAmazon账户管理 API 请求

必须使用访问密钥 ID 和秘密访问密钥签署请求。我们强烈建议您不要使用您的Amazon用于日常工作的根账户凭证Amazon账户管理。您可以使用凭证用于Amazon Identity and Access Management(IAM) 用户或临时凭证，例如您用于 IAM 角色的临时凭证。

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

有关更多信息，请参阅以下内容：

- [Amazon 安全凭证](#)— 提供有关您可用于访问的凭证类型的一般信息 Amazon。
- [IAM 最佳实践](#)— 提供有关使用 IAM 服务的建议，以帮助保护您的 Amazon 资源，包括中的资源 Amazon 账户管理。
- [临时证书](#)— 介绍如何创建和使用临时安全凭证。

# Amazon Account Management 的配额

您的 Amazon Web Services 账户每个配额都具有默认配额（以前称为限制）Amazon 服务。除非另有说明，否则每个配额是 Amazon Web Services 区域特定于的。

每个 Amazon Web Services 账户具有以下与账户管理相关的配额。

资源	配额
中的备用联系人数 Amazon Web Services 账户	3-每个一个 BILLING、SECURITY, 和 OPERATIONS
速率 GetAlternateContact 每个账户的 API 操作	每秒 3 次，突发至每秒 5 次
速率 PutAlternateContact 每个账户的 API 操作	每秒 1 次，突发至每秒 2 次
速率 DeleteAlternateContact 每个账户的 API 操作	每秒 1 个



# 排除的故障 Amazon Web Services 账户

使用以下主题中的信息可帮助您诊断和修复与 Amazon Web Services 账户。

## 故障排除主题

- [排查的相关问题 Amazon Web Services 账户创建 \(p. 85\)](#)
- [排查根用户的相关问题 \(p. 86\)](#)
- [排查的相关问题 Amazon Web Services 账户登录 \(p. 87\)](#)
- [排查其他问题 Amazon Web Services 账户 \(p. 87\)](#)

## 排查的相关问题 Amazon Web Services 账户创建

使用此处的信息可帮助您排查与创建 Amazon Web Services 账户。

### 问题

- [我没收到来自的电话 Amazon 验证我的新账户 \(p. 85\)](#)
- [当我尝试验证我的时候，我收到有关“最大失败尝试次数”错误的错误 Amazon Web Services 账户通过电话 \(p. 86\)](#)

## 我没收到来自的电话 Amazon 验证我的新账户

创建时 Amazon Web Services 账户，您必须提供一个可以接收短信或语音通话的电话号码。您可以指定使用哪种方法来验证数字。

如果您未收到消息或电话，请验证：

- 在注册过程中，您输入了正确的电话号码并选择正确的国家/地区代码。
- 如果你使用的是移动电话，请确保你有手机信号来接收短信或来电。
- 您为自己输入的信息 [支付方法](#) 以下内容正确。

如果你没有收到短信或电话来完成身份验证过程，Amazon Web Services Support 可以帮助你激活 Amazon Web Services 账户手动。使用以下步骤：

1. 确保您可以通过 [电话号码](#) 你为你提供的 Amazon Web Services 账户。
2. 打开 [Amazon Web Services Support 控制台](#) 选择，然后选择创建案例。
  - a. 选择账户和账单支持。
  - b. 适用于类型选择，选择账户。
  - c. 适用于类别选择，选择激活。
  - d. 在案例描述部分中，提供可以联系到您的日期和时间。
  - e. 在联系选项部分，选择聊天对于 来说为联系方式。
  - f. 选择 Submit。

## Note

您可以使用创建案例Amazon Web Services Support即使你Amazon Web Services 账户尚未激活。

# 当我尝试验证我的时候，我收到有关“最大失败尝试次数”错误的错误Amazon Web Services 账户通过电话

Amazon Web Services Support可以帮助你手动激活帐户。按照以下步骤进行操作：

1. [登录您的Amazon Web Services 账户](#)使用您在创建账户时指定的电子邮件地址和密码。
2. 打开[Amazon Web Services Support控制台](#)选择，然后选择创建案例。
3. 选择账户和账单 Support.
4. 适用于类型选择，选择账户。
5. 适用于类别选择，选择激活。
6. 在案例描述部分中，提供可以联系到您的日期和时间。
7. 在联系选项部分，选择聊天对于 来说为联系方式。
8. 选择 Submit。

Amazon Web Services Support将与你联系并尝试手动激活Amazon Web Services 账户。

## 排查根用户的相关问题

使用此处的信息可帮助您排查与根用户相关的相关问题。Amazon Web Services 账户。

### 问题

- [我无法执行以账户根用户身份登录时期望能够执行的任务 \(p. 86\)](#)
- [我忘记了我的 root 用户密码Amazon Web Services 账户 \(p. 86\)](#)
- [我无权访问我的电子邮件Amazon Web Services 账户 \(p. 86\)](#)

## 我无法执行以账户根用户身份登录时期望能够执行的任务

如果在以账户根用户身份登录时无法完成任务，则您的账户可能是中的组织的成员。Amazon Organizations。如果是，并且组织管理员使用服务控制策略 (SCP) 来限制账户的权限，则所有用户，包括根用户，都会受到影响。有关更多信息，请参阅 [服务控制策略](#)中的Amazon Organizations用户指南。

## 我忘记了我的 root 用户密码Amazon Web Services 账户

如果您是根用户，并且丢失或忘记了您的密码。Amazon Web Services 账户，您可以重置密码。您必须知道用于创建Amazon Web Services 账户，并且必须有权访问该电子邮件账户。有关更多信息，请参阅 [重置丢失或忘记的密码或访问密钥Amazon](#)。

## 我无权访问我的电子邮件Amazon Web Services 账户

创建时Amazon Web Services 账户，您需要提供电子邮件地址和密码。这些是的凭证Amazon Web Services 账户根用户。如果您不确定与您的关联的电子邮件地址Amazon Web Services 账户中，检查从

no-reply@amazon.com 到您组织的任何电子邮件地址的已保存通信，它们可能已用于打开 Amazon Web Services 账户。

如果您知道电子邮件地址，但无法再访问电子邮件，请首先尝试使用以下选项之一恢复对电子邮件的访问权限：

- 如果您拥有该电子邮件地址的域，则可以恢复已删除的电子邮件地址。或者，您可以为电子邮件账户设置“全部捕获”，该功能将捕获发送到邮件服务器中不再存在的电子邮件地址的所有邮件，并将其重定向到另一个电子邮件地址。
- 如果账户上的电子邮件地址属于您的公司电子邮件系统，我们建议您联系 IT 系统管理员。它们也许能够帮助您重新获得电子邮件的访问权限。

如果你仍然无法登录 Amazon Web Services 账户，你可以在这里找到替代支持选项 [联系我们](#)。Expand 我无法登录我的 Amazon Web Services 账户然后选择请求 Support Amazon Web Services 账户凭证。在窗体中提供信息，然后选择 Submit (提交)。

## 排查的相关问题 Amazon Web Services 账户登录

使用此处的信息可帮助您排查与以用户身份登录相关的问题排查 Amazon Web Services 账户。

### Note

本主题是关于登录 Amazon Web Services 账户的。如果您在登录您的过程中遇到问题 Amazon.com 购物账户，请参阅 [Amazon 客户服务](#) 相反。

### 问题

- [我需要我的 Amazon Web Services 账户 ID 或别名 \(p. 87\)](#)
- [我忘记了 IAM 用户名或密码 \(p. 87\)](#)

## 我需要我的 Amazon Web Services 账户 ID 或别名

如果您是 Amazon Identity and Access Management (IAM) 用户并且您尚未登录，您必须向管理员询问 Amazon Web Services 账户要么 Amazon Web Services 账户别名。您需要此信息以及您的 IAM 用户名和密码才能登录 Amazon Web Services 账户。

## 我忘记了 IAM 用户名或密码

如果您是 IAM 用户，管理员会提供您的凭证。如果您忘记了密码，则必须要求管理员重置密码。

出于安全考虑，Amazon 无权查看、提供或更改您的凭证。

## 排查其他问题 Amazon Web Services 账户

使用此处的信息可帮助您排查与您的相关问题 Amazon Web Services 账户。

### 问题

- [我需要为我的信用卡更改 Amazon Web Services 账户 \(p. 88\)](#)
- [我需要举报欺诈 Amazon Web Services 账户活动 \(p. 88\)](#)
- [我需要关闭我的 Amazon Web Services 账户 \(p. 88\)](#)

## 我需要为我的信用卡更改Amazon Web Services 账户

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

## 我需要举报欺诈Amazon Web Services 账户活动

如果你怀疑使用你的欺诈活动Amazon Web Services 账户并且想做一份报告，请参阅[如何举报滥用Amazonresources](#)。

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

## 我需要关闭我的Amazon Web Services 账户

有关帮助解决关闭Amazon Web Services 账户请参阅[关闭您的 Amazon Web Services 账户](#) (p. 22)。

# 账户管理用户指南的文档历史记录

下表介绍了的文档版本。Amazon账户管理。

更新-历史记录-更改	update-history-description	update-history-date
<a href="#">首次发布 (p. 89)</a>	的初始版本Amazon账户管理参考指南	2021 年 9 月 30 日

# Amazon词汇表

有关最新Amazon术语，请参阅《Amazon一般参考》中的[Amazon术语表](#)。

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。