aws

参考指南

AWS 账户管理

AWS 账户管理: 参考指南

Table of Contents

欢迎阅读AWS账户管理参考指南

AWS 账户是访问AWS服务的基本组成部分。

A AWS 账户 有两个基本功能：

- 容器 — AWS 账户 是您作为AWS客户创建的所有AWS资源的基本容器。例如，亚马逊简单存储服务 (Amazon S3) 存储桶、亚马逊关系数据库服务 (Amazon RDS) 数据库和亚马逊弹性计算云 (Amazon EC2) 实例都是资源。每个资源都由亚马逊资源名称 (ARN) 进行唯一标识，该名称包括包含或拥有该资源的账户的账户 ID。
- 安全边界 — AWS 账户 也是您AWS资源的基本安全边界。您在账户中创建的资源可供拥有您的账户凭证的用户使用。

  您可以在账户中创建的关键资源包括身份，例如用户和角色。身份具有用户可以用来登录（身份验证）的凭据AWS。身份还具有权限策略，用于指定用户可以对账户中的资源执行的操作（授权）。

  作为安全最佳实践，要求您的用户在访问时使用临时证书AWS。要提供临时证书，您可以使用联合身份验证和身份提供商，例如 AWS IAM Identity Center（IAM Identity Center）。如果您的公司已经在使用身份提供商，请将其与联合身份验证一起使用，以简化您提供对自己资源的访问权限的方式 AWS 账户。

  有关安全最佳实践的信息，请参阅 IAM 用户指南中的 IAM 安全最佳实践。

主题

我需要多个吗AWS 账户?

AWS 账户作为基本安全边界AWS. 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AWS 账户有助于您在云环境中支持以下原则：

- 安全控制— 不同的应用程序可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AWS 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AWS 账户是一个安全保护单位。应将潜在风险和安全威胁包含在AWS 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。你可以通过将团队移动到分开来防止他们互相干扰AWS 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AWS 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AWS Organizations和整合账单），同时将行项目分隔为AWS 账户.
- 配额分配–AWS每个服务配额分别强制执行AWS 账户. 将工作负载分为不同AWS 账户阻止他们互相消耗配额。

本文档中描述的所有建议和程序都符合AWS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AWS 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，建议您使用AWS Organizations，这是一个免费的AWS服务来管理所有AWS 账户在组织中。

AWS还优惠AWS Control Tower，它添加了层AWS管理 Organizations 的自动化并自动将其与其他组织集成AWS类似服务AWS CloudTrail、AWS Config、Amazon CloudWatchAWS Service Catalog，以及其他人。这些服务可能会产生额外费用。有关更多信息，请参阅AWS Control Tower定价。

入门：你是首次AWS使用吗？

如果您是首次使用AWS，则第一步是注册. AWS 账户 注册时，AWS 账户使用您提供的详细信息AWS创建一个，并将该帐户分配给您。创建后AWS 账户，以 root 用户身份登录，为根用户激活多重身份验证 (MFA)，然后为用户分配管理权限。

步骤

先决条件

要注册AWS 账户，您需要提供以下信息：

- 账户名称-账户名称出现在多个位置，例如发票上，以及控制台（例如账单和成本管理）控制面板和AWS Organizations控制台中。

  我们建议您使用标准方式命名您的账户，这样您就可以为账户指定易于识别的名称。对于公司账户，可以考虑使用命名标准，例如组织-目的-环境（例如，AnyCompany-审计-生产）。对于个人帐户，可以考虑使用命名标准，例如名字-姓氏-用途（例如 paulo-santos-testaccount）。

  有关更改账户名称的信息，请参阅如何更改我的账户名称AWS 账户？。
- 地址 — 如果您的联系地址在印度，则您的账户的用户协议是与印度当地AWS卖家 Amazon Internet Services Private Limited (AISPL) 签订的。您必须在验证过程中提供 CVV。您可能还需要输入一次性密码，具体取决于您的银行。作为验证过程的一部分，AISPL 会向您的付款方式收取 2 印度卢比。AISPL 将在验证完成后退回 2 INR。
- 电子邮件地址-电子邮件地址用作 root 用户的登录名，是恢复账户所必需的。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，必须确认自己有权访问发送到该地址的电子邮件。

  > **Important**
  >
  > 如果此帐户适用于企业，请使用安全的公司通讯组列表（例如`it.admins@example.com`），这样AWS 账户即使员工变更职位或离开公司，您的公司也可以保留访问该列表的权限。由于电子邮件地址可用于重置账户的根用户凭证，因此请保护对该通讯组列表或地址的访问权限。
- 电话号码-此号码可用于确认您的账户所有权。您必须能够通过此电话号码接听电话。

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

第 1 步：创建你的 AWS 账户

1. 在浏览器中，打开AWS主页。
2. 选择 “创建” AWS 账户。

> **Note**
>
> 如果您AWS最近登录过，请选择登录。如果 “创建新账户” 选项AWS 账户不可见，请先选择 “登录其他账户”，然后选择 “创建新账户” AWS 账户。

3. 输入您的账户信息，然后选择 “验证电子邮件地址”。这会将验证码发送到您指定的电子邮件地址。
4. 输入您的验证码，然后选择 “验证”。
5. 为 root 用户输入一个强密码，进行确认，然后选择 “继续”。 AWS要求您的密码满足以下条件：
   - 它必须至少包含 8 个字符，最多 128 个字符。
   - 它必须至少包含以下三种字符类型组合：大写、小写、数字和! @ # $% ^ & * () <> [] {} | _+-= 符号。
   - 它不得与您的AWS 账户姓名或电子邮件地址相同。
6. 选择 “商务” 或 “个人”。这些选项之间的区别在于我们要求您提供的信息。两种账户类型具有相同的特性和功能。
7. 输入您的企业或个人信息。请参阅 “先决条件” 部分中有关电子邮件地址和电话号码的建议。
8. 阅读并接受《AWS客户协议》。请务必阅读并理解AWS客户协议的条款。
9. 选择 Continue（继续）。此时，您将收到一封电子邮件，确认您的设备AWS 账户已准备就绪。您可以使用在注册时提供的电子邮件地址和密码登录您的新帐户。但是，在完成激活帐户之前，您无法使用任何AWS服务。
10. 输入有关您的付款方式的信息。如果您想使用其他地址进行计费，请选择使用新地址。
11. 选择验证并继续。

12. 在列表中输入您的国家或地区代码，然后输入在接下来的几分钟内可以联系到您的电话号码。输入验证码并提交。
13. 当自动系统与您联系时，请输入您收到的 PIN，然后提交。
14. 选择您的AWS Support套餐。有关可用套餐的描述，请参阅比较AWS Support套餐。
15. 选择 “完成注册”。将出现一个确认页面，表明您的账户正在激活。
16. 检查您的电子邮件和垃圾邮件文件夹中是否有确认您的帐户已激活的电子邮件。激活通常需要几分钟，但有时可能需要长达 24 小时。

    收到激活消息后，您可以完全访问所有AWS服务。

> **Note**
>
> 如果您在激活账户时遇到问题，请参阅the section called “账户创建问题”。

第 2 步：为您的根用户激活 MFA

我们强烈建议您为根用户激活 MFA。MFA 大大降低了有人在未经您授权的情况下访问您的账户的风险。

1. 选择 Root user（根用户）并输入您的 AWS 账户 电子邮件地址，以账户拥有者身份登录 AWS Management Console。在下一页上，输入您的密码。

   有关使用根用户登录的帮助，请参阅《AWS Management Console登录用户指南》中的以根用户身份AWS登录。
2. 为您的根用户启用 MFA。

   有关说明，请参阅《IAM 用户指南》中的为 AWS 账户根用户启用虚拟 MFA 设备（控制台）。

步骤 3：创建管理员用户

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。取而代之的是，在 IAM Identity Center 中为管理用户分配管理访问权限，然后以该管理用户身份登录以执行您的日常管理任务。

有关说明，请参阅 IAM 身份中心用户指南中的为 IAM 身份中心管理员用户设置AWS 账户访问权限。

相关主题

- 有关保护根用户证书的信息，请参阅 IAM 用户指南中的保护根用户的证书。
- 有关需要根用户的任务列表，请参阅 IAM 用户指南中的需要根用户证书的任务。

使用 AWS 账户根用户

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

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

要避免使用 root 用户执行日常任务，请在中学习如何设置管理用户AWS IAM Identity Center。有关其他根用户安全建议，请参阅您的 root 用户最佳实践AWS 账户。

您可以更改或重置 root 用户密码，以及创建或删除 root 用户的访问密钥（访问密钥 ID 和私有访问密钥）。有关使用 root 用户登录的帮助，请参阅《AWS Management Console登录用户指南》中的以 root 用户身份AWS登录。

管理你的AWS 账户

本节包含描述如何管理您的主题AWS 账户。

> **Note**
>
> 如果你的AWS 账户是通过使用在印度创建的Amazon Internet Services Private Limited(AISPL)，还有其他注意事项。有关更多信息，请参阅 在印度管理账户。

主题

创建独立版 AWS 账户

本主题介绍如何创建不由管理AWS 账户的独立服务器AWS Organizations。如果您想创建属于由管理的组织的账户AWS Organizations，请参阅《AWS Organizations用户指南》中的在组织中创建成员账户。

这些说明用于在印度AWS 账户境外创建一个。有关在印度创建账户的信息，请参阅创建一个AWS 账户用 AISPL。

AWS Management Console

创建 AWS 账户

1. 打开亚马逊 Web Services 主页。
2. 选择 “创建” AWS 账户。

> **Note**
>
> 如果您AWS最近登录过，则该选项可能不存在。而是选择 “登录控制台”。然后，如果 “创建新账户” AWS 账户 仍不可见，请先选择 “登录其他账户”，然后选择 “创建新账户” AWS 账户。

3. 输入您的账户信息，然后选择 “验证电子邮件地址”。这会将验证码发送到您指定的电子邮件地址。

> **Important**
>
> 由于该账户的 root 用户非常重要，因此我们强烈建议您使用可由群组访问的电子邮件地址，而不仅仅是个人可以访问的电子邮件地址。这样，如果注册的人AWS 账户离开了公司，仍然AWS 账户可以使用，因为电子邮件地址仍然可以访问。
> 如果您无法访问与关联的电子邮件地址AWS 账户，那么如果您丢失了密码，则无法恢复对该帐户的访问权限。

4. 输入您的验证码，然后选择 “验证”。
5. 为 root 用户输入一个强密码，进行确认，然后选择 “继续”。 AWS要求您的密码满足以下条件：

   - 长度必须至少 8 个字符，最多 128 个字符。
   - 必须至少包含以下字符类型中三种的组合：大写字母、小写字母、数字，以及 ! @ # $ % ^ & * () <> [] {} | _+-= 符号。
   - 不得与您的 AWS 账户名称或电子邮件地址相同。

6. 选择 “商务” 或 “个人”。个人账户和企业账户的特点和功能相同。
7. 输入您的公司或个人信息。

> **Important**
>
> 对于企业而言AWS 账户，最佳做法是输入：

- 公司电话号码，而不是个人电话的号码。
- 一个电子邮件地址，其域名属于将要使用该帐户的公司或组织。

为账户的 root 用户配置个人电子邮件地址或个人电话号码可能会使您的账户不安全。

8. 阅读并接受《AWS客户协议》。请务必阅读并理解AWS客户协议的条款。
9. 选择 Continue（继续）。此时，您将收到一封电子邮件，确认您的设备AWS 账户已准备就绪。您可以使用在注册时提供的电子邮件地址和密码登录您的新帐户。但是，在完成激活帐户之前，您无法使用任何AWS服务。
10. 输入有关您的付款方式的信息，然后选择 “验证并继续”。如果您想使用不同的账单地址作为账AWS单信息，请选择使用新地址。

    在添加有效的付款方式之前，您无法继续注册流程。
11. 在列表中输入您的国家或地区代码，然后输入在接下来的几分钟内可以联系到您的电话号码。
12. 输入验证码中显示的验证码，然后提交。
13. 当自动系统与您联系时，请输入您收到的 PIN，然后提交。
14. 选择一个可用AWS Support计划。有关可用的 Support 计划及其优势的描述，请参阅比较AWS Support计划。
15. 选择 “完成注册”。此时会出现一个确认页面，表明您的账户已被激活。
16. 检查您的电子邮件和垃圾邮件文件夹中是否有确认您的帐户已激活的电子邮件。激活通常需要几分钟，但有时可能需要长达 24 小时。

    收到激活消息后，您可以完全访问所有AWS服务。

AWS CLI & SDKs

您可以在组织中创建成员账户，该组织AWS Organizations通过在登录组织管理账户时运行CreateAccount操作进行管理。

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

查看 AWS 账户 标识符

AWS 为每 AWS 账户人分配以下唯一标识符：

AWS 账户 ID

一个 12 位数字，例如 012345678901，用于唯一标识。 AWS 账户许多 AWS 资源的 Amazon 资源名称 (ARN) 中都包含账户 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 AWS Identity and Access Management (IAM) 用户，则可以使用账户 ID 或账户别名登录。 AWS Management Console 虽然账户 ID 与任何识别信息一样，应谨慎使用和共享，但不应将其视为机密、敏感或机密信息。

规范用户 ID

一种字母数字标识符，例如`79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`，它是 ID 的混淆形式。 AWS 账户 在使用亚马逊简单存储服务 (Amazon S3) 授予对存储桶和对象的跨账户访问权限 AWS 账户 时，您可以使用此 ID 来识别。您可以以根用户或 IAM 用户的身份检索您的 AWS 账户 规范用户 ID。

您必须通过身份验证 AWS 才能查看这些标识符。

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

找到你的 AWS 账户 身份证

您可以使用 AWS Management Console 或 AWS Command Line Interface (AWS CLI) 来查找 AWS 账户 ID。在控制台中，账户 ID 的位置取决于您是以根用户身份还是以 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 都相同。

以 root 用户身份查找您的账户 ID

AWS Management Console

在以 root 用户 AWS 账户 身份登录时查找你的 ID

> **最小权限**
>
> 要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当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，选择您的账户名或账号，然后选择安全凭证。

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

2. 在 “账户详情” 部分下，账号显示在 AWS 账户 ID 旁边。

AWS CLI & SDKs

要查找您的 AWS 账户 身份证，请使用 AWS CLI

> **最小权限**
>
> 要执行下列步骤，您必须至少具有以下 IAM 权限：
>
> - 当您以根用户身份运行命令时，您不需要任何 IAM 权限。

按照如下所示使用 get-caller-identity 命令。

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

以 IAM 用户身份查找您的账户 ID

AWS Management Console

以 IAM 用户 AWS 账户 身份登录时查找您的 ID

> **最小权限**
>
> 要执行下列步骤，您必须至少具有以下 IAM 权限：
>
> - `account:GetAccountInformation`

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

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

2. 在页面顶部的账户详情下，账号显示在 AWS 账户 ID 旁边。

AWS CLI & SDKs

要查找您的 AWS 账户 身份证，请使用 AWS CLI

> **最小权限**
>
> 要执行下列步骤，您必须至少具有以下 IAM 权限：
>
> - 当您以 IAM 用户或角色的身份运行命令时，您必须具备：
>   - `sts:GetCallerIdentity`

按照如下所示使用 get-caller-identity 命令。

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

```
123456789012
```

查找您的规范用户 ID AWS 账户

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

以根用户或 IAM 用户的身份查找规范 ID

AWS Management Console

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：
>
> - 当您以根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：
>   - `account:GetAccountInformation`

1. 以根用户或 IAM 用户身份登录。 AWS Management Console
2. 在右上角的导航栏中，选择您的账户名或账号，然后选择安全凭证。

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

3. 在 “账户详情” 部分下，规范用户 ID 显示在 Canonical 用户 ID 旁边。您可以使用您的规范用户 ID 来配置 Amazon S3 访问控制列表 (ACL)。

AWS CLI & SDKs

要查找规范用户 ID，请使用 AWS CLI

同样的 AWS CLI ，API 命令适用于 AWS 账户根用户、IAM 用户或 IAM 角色。

按如下方式使用 list-buckets 命令。

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

以具有 IAM 角色的联合用户身份查找规范 ID

AWS Management Console

以具有 IAM 角色的联合用户身份登录控制台时查找账户的规范 ID

> **最小权限**
>
> - 您必须拥有列出和查看 Amazon S3 存储桶的权限。

1. 以具有 IAM 角色的联合用户身份登录。 AWS Management Console
2. 在 Amazon S3 控制台中，选择存储桶名称以查看有关存储桶的详细信息。
3. 选择 Permissions（权限）选项卡。
4. 在 “访问控制列表” 部分的存储桶所有者下，将显示您的 AWS 账户 规范 ID。

AWS CLI & SDKs

要查找规范用户 ID，请使用 AWS CLI

同样的 AWS CLI ，API 命令适用于 AWS 账户根用户、IAM 用户或 IAM 角色。

按如下方式使用 list-buckets 命令。

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

更新 root 用户的AWS 账户姓名、电子邮件地址或密码

要编辑您的AWS 账户姓名或更改 root 用户的密码或电子邮件地址，请执行以下过程中的步骤。此电子邮件地址和密码是您用来登录的凭据AWS 账户根用户。

> **Note**
>
> 对的更改AWS 账户最多可能需要四个小时才能传播到任何地方。

AWS Management Console

编辑您的AWS 账户姓名、root 用户密码或 root 用户电子邮件地址

> **最小权限**
>
> 要执行下列步骤，您必须至少具有以下 IAM 权限：
>
> - 您必须以身份登录AWS 账户根用户，这不需要其他 IAM 权限。您无法以 IAM 用户或角色身份执行这些步骤。

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

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

4. 在更新账户设置页面上，选择要更新的字段旁边的编辑。

   a. 对于姓名 — 在 “更新您的账户名称” 页面上，在新账户名称中，输入新的账户名称，然后选择保存更改。

> **Note**
>
> 如果您无法修改AWS 账户名称，请检查中是否存在限制访问权限`account`或设置为拒绝操作AWS Organizations的服务控制策略(SCP)。`iam:UpdateAccountName`

b. 对于电子邮件 — 在 “更新您的电子邮件地址” 页面上，填写 “新电子邮件地址”、“确认新电子邮件地址” 字段，然后确认您当前的密码。然后选择 Save changes（保存更改）。验证码将从发送到您的新电子邮件地址`no-reply@verify.signin.aws`。在 “验证您的新电子邮件地址” 页面的 “验证码” 下，输入您从电子邮件中收到的验证码，然后选择 “保存更改”。

> **Note**
>
> 验证码最多可能需要 5 分钟才能送达。如果您在收件箱中没有看到该电子邮件，请检查您的垃圾邮件和垃圾文件夹。

c. 对于密码-在 “更新您的密码” 页面上，填写 “当前密码”、“新密码” 和 “确认新密码” 字段。然后选择 Save changes（保存更改）。有关其他指导，包括设置根用户密码的最佳实践，请参阅 IAM 用户指南AWS 账户根用户中的更改密码。

5. 完成所有更改后，选择完成。

AWS CLI & SDKs

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

了解 API 的操作模式

使用的 API 操作AWS 账户的属性始终在以下两种操作模式之一中起作用：

- 独立上下文— 当账户中的用户或角色访问或更改账户属性时，将使用此模式同一账户. 独立上下文模式在您执行以下操作时自动使用Don't加入`AccountId`当你调用其中一个账户管理时参数AWS CLI要么AWS开发工具包操作。
- Organizations 上下文— 当组织中一个账户中的用户或角色访问或更改同一组织中其他成员账户的账户属性时，将使用此模式。在执行以下操作时，将自动使用组织上下文模式：做加入`AccountId`当

你调用其中一个账户管理时参数AWS CLI要么AWS开发工具包操作。在此模式下，您只能从组织的管理账号或账户管理的委派管理员账户调用操作。

这些区域有：AWS CLI和AWSSDK 操作可以在独立环境或组织上下文中运行。

- 如果您Don't加入`AccountId`参数，则操作将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账户。不管账户是否为组织的成员，都是如此。
- 如果你确实包含了`AccountId`参数，则操作将在Organizations 上下文中运行，并且操作在指定的“组织” 帐户上运行。
  - 如果调用操作的账户是 Account Management 服务的管理账户或委派的管理员账户，则您可以在`AccountId`参数以更新指定的账户。
  - 组织中唯一可以调用某个备用联系人操作并在中指定自己的账号的账户`AccountId`参数是指定为委托管理员账户用于账户管理服务。任何其他账户，包括管理账户，都会收到`AccessDenied`例外。
- 如果您在独立模式下运行操作，则必须允许您使用包含`Resource`任一的元素`"*"`允许所有资源，或者使用独立账户语法的 ARN.
- 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，该策略包含`Resource`任一的元素`"*"`允许所有资源，或者使用组织中成员账户语法的 ARN.

授予更新账户属性的权限

和大多数人一样AWS操作，您授予添加、更新或删除帐户属性的权限AWS 账户通过使用IAM 权限策略. 当您将 IAM 权限策略附加到 IAM 委托人（用户或角色）可在什么和条件下对哪些资源进行哪些资源下对哪些资源进行哪些资源下对哪些资源进行哪些资源下对哪些资源进行哪些资源下对哪些资源进行哪些资源下对哪些资源进行哪些资源下对哪些资源

以下是账户管理在创建权限策略时的一些特定注意事项。

的 Amazon 资源名称格式AWS 账户

- 这些区域有：Amazon 资源名称 (ARN)换一个AWS 账户你可以将其包含在`resource`根据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会有所不同。请参阅上一部分了解 API 的操作模式.
  - 独立账户的账户 ARN：

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

在独立模式下运行帐户属性操作时，必须使用此格式，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}
```

在组织模式下运行帐户属性操作时，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几种账户管理特定于服务的条件键提供对您授予的权限的细粒度控制。

account:AccountResourceOrgPaths

上下文密钥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 包含的成员账户符合条件。以下示例代码段将策略限制为仅应用于位于两个指定 OU 中任一的账户。

由于account:AccountResourceOrgPaths是多值字符串类型，则必须使用ForAnyValue要么ForAllValues多值字符串运算符. 另外，请注意，条件键的前缀是account，即使您引用的是组织中 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

上下文密钥account:AccountResourceOrgTags允许您引用可附加到组织中账户的标签。标签是一个键/值字符串对，可用于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AWS 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？AWS中的IAM 用户指南. 以下示例代码段将策略限制为仅适用于组织中具有带密钥的标签的账户project和任一的值blue要么red.

由于account:AccountResourceOrgTags是多值字符串类型，则必须使用ForAnyValue要么ForAllValues多值字符串运算符. 另外，请注意，条件键的前缀是account，即使你引用的是组织成员账户上的标签。

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

> **Note**
>
> 您只能将标签附加到组织中的一个账户。你不能将标签附加到独立的AWS 账户.

更新你的AWS 账户联系信息

您可以存储有关以下内容的联系信息主要账户联系人为了你AWS 账户。您还可以添加或编辑以下联系信息备用账户联系人:

- 账单— 备用账单联系人将收到账单相关通知，例如发票可用性通知。
- 运营— 备用运营联系人将收到与运营相关的通知。
- 安全— 备用安全联系人将收到与安全相关的通知，包括来自的通知AWS滥用小组。

主题

更新您的备用联系人 AWS 账户

备用联系人AWS最多可以联系三个与该账户关联的备用联系人。备用联系人不必是特定的联系人。如果您拥有负责管理账单、运营和安全相关问题的团队，则可以添加电子邮件分发列表。除此之外，还有与该账户的 root 用户关联的电子邮件地址。主账户联系人将继续收到发送到主账户电子邮件的所有电子邮件通信。

您只能指定与账户关联的以下每种联系人类型中的一种。

- 账单联系人
- 运营联系人
- 安全联系人

您可以以不同的方式添加或编辑备用联系人，具体取决于这些账户是独立账户还是组织的一部分：

- 独立 AWS 账户 — 对于AWS 账户未与组织关联的组织，您可以使用AWS管理控制台或通过 AWS CLI 和 SDK 更新自己的备用联系人。要了解如何执行此操作，请参阅更新独立AWS 账户备用联系人。
- AWS 账户组织内部-对于属于组织的成员账户，管理账户或委托管理员账户中的用户可以从AWS Organizations控制台集中更新AWS组织中的任何成员账户，也可以通过 AWS CLI 和 SDK 以编程方式更新组织中的任何成员账户。要了解如何执行此操作，请参阅更新组织中的AWS 账户备用联系人。

主题

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

电话号码和电子邮件地址要求

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

- 电话号码只能包含数字、空格和以下字符：”+-()”。

- 电子邮件地址的长度最多为 254 个字符，除了标准的字母数字字符外，还可以在电子邮件地址的本地部分包含以下特殊字符：“” +=.#|!&-_。

更新独立版的备用联系人 AWS 账户

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

AWS Management Console

为独立版添加或编辑备用联系人 AWS 账户

> **最小权限**
>
> 要执行下列步骤，您必须至少具有以下 IAM 权限：
>
> - `account:GetAlternateContact`（查看备用联系方式）
> - `account:PutAlternateContact`（设置或更新备用联系人）
> - `account:DeleteAlternateContact`（删除备用联系人）

1. 以具有最低权限AWS Management Console的 IAM 用户或角色的身份登录。
2. 在窗口的右上角选择您的账户名称，然后选择账户。
3. 在“帐户”页面上，向下滚动到“备用联系人”，然后在标题右侧选择“编辑”。

   > **Note**
   >
   > 如果您没有看到“编辑”选项，则可能是您不是以账户的根用户身份登录的，也不是以具有上述最低权限的用户身份登录。

4. 更改任何可用字段中的值。

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

5. 完成所有更改后，选择 “更新”。

AWS CLI & SDKs

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

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **注意事项**
>
> - 要通过管理账户或组织中的委托管理员账户对成员账户执行这些操作，必须为账户服务启用可信访问权限。

> **最小权限**
>
> 对于每个操作，您必须拥有映射到该操作的权限：
>
> - `GetAlternateContact`（查看备用联系方式）
> - `PutAlternateContact`（设置或更新备用联系人）
> - `DeleteAlternateContact`（删除备用联系人）
>
> 如果您使用这些个人权限，则可以授予某些用户仅读取联系人信息的权限，而授予其他用户同时读取和写入的权限。

Example

以下示例检索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

以下示例为来电者的账户设置了新的运营备用联系人。

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

如果成功，此命令不会产生任何输出。

Example

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

Example

以下示例删除来电者账户的安全备用联系人。

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

如果成功，此命令不会产生任何输出。

> **Note**
>
> 如果您尝试多次删除同一个联系人，则第一个会以静默方式成功。以后的所有尝试都会生成ResourceNotFound异常。

更新组织中任何AWS 账户成员的备用联系人

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

要求

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

- 您的组织必须启用所有功能才能管理您的成员账户的设置。这允许管理员控制成员帐户。这是在创建组织时默认设置的。如果您的组织设置为仅限整合账单，并且您想要启用所有功能，请参阅启用组织中的所有功能。
- 您需要为AWS账户管理服务启用可信访问权限。要进行此设置，请参阅为AWS账户管理启用可信访问权限。

> **Note**
>
> AWS Organizations托管策略AWSOrganizationsReadOnlyAccess或AWSOrganizationsFullAccess已更新，提供访问AWS账户管理 API 的权限，以便您可以从AWS Organizations控制台访问账户数据。要查看更新的托管策略，请参阅 Organizati ons AWS 托管策略的更新。

AWS Management Console

为组织AWS 账户中的任何成员添加或编辑备用联系人

1. 使用组织的管理账户凭据登录AWS Organizations控制台。

2. 从中 AWS 账户，选择要更新的账户。
3. 选择 “联系人信息”，然后在 “备用联系人” 下找到联系人类型：账单联系人、安全联系人或运营联系人。
4. 要添加新联系人，请选择添加，或者要更新现有联系人，请选择编辑。
5. 更改任何可用字段中的值。

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

6. 完成所有更改后，选择 “更新”。

AWS CLI & SDKs

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

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **注意事项**
>
> - 要通过管理账户或组织中的委托管理员账户对成员账户执行这些操作，必须为账户服务启用可信访问权限。
> - 您无法访问与您用于调用操作的组织不同的组织中的帐户。

> **最小权限**
>
> 对于每个操作，您必须拥有映射到该操作的权限：
>
> - `GetAlternateContact`（查看备用联系方式）
> - `PutAlternateContact`（设置或更新备用联系人）

- DeleteAlternateContact（删除备用联系人）

如果您使用这些个人权限，则可以授予某些用户仅读取联系人信息的权限，而授予其他用户同时读取和写入的权限。

Example

以下示例检索组织中来电者账户的当前账单备用联系人。使用的凭证必须来自组织的管理账户，或者来自账户管理的委托管理员账户。

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

Example

以下示例为组织中的指定成员账户设置运营备用联系人。使用的凭证必须来自组织的管理账户，或者来自账户管理的委托管理员账户。

```
$ aws account put-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

如果成功，此命令不会产生任何输出。

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

Example

以下示例删除组织中指定成员账户的安全备用联系人。使用的凭证必须来自组织的管理账户，或者来自账户管理的委托管理员账户。

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

如果成功，此命令不会产生任何输出。

Example

> **Note**
>
> 如果您尝试多次删除同一个联系人，则第一个会以静默方式成功。以后的所有尝试都会生成ResourceNotFound异常。

账户：AlternateContactTypes上下文密钥

您可以使用上下文密钥account:AlternateContactTypes指定 IAM 策略允许（或拒绝）三种账单类型中的哪一种。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组织中特定账户的BILLING备用联系人，但不能修改这些联系人。

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

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

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

更新您的主要联系人 AWS 账户

您可以更新与您的账户关联的主要联系信息，包括联系人的全名、公司名称、邮寄地址、电话号码和网站地址。

您可以以不同的方式编辑主要账户联系人，具体取决于这些账户是独立账户还是组织的一部分：

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

主题

- 电话号码和电子邮件地址要求
- 更新独立版的主要联系人 AWS 账户
- 更新组织AWS 账户中任何人的主要联系人

电话号码和电子邮件地址要求

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

- 电话号码只能包含数字、空格和以下字符：”+-()”。
- 电话号码必须以+和国家/地区代码开头，并且国家/地区代码后面不得有任何前导零或额外的空格。例如，+1（美国/加拿大）或+44（英国）。
- 电话号码应在区号、交换代码和本地代码之间包含连字符 - “”。例如，+1 202-555-0179。

> **Note**
>
> 在为 root 用户重置 MFA 设备时，输入不带连字符的电话号码可能会导致在电话号码验证过程中无法接听电话。有关更多信息，请参阅如何重置我的AWS根用户账户 MFA 设备？ 。

- 出于安全考虑，电话号码必须能够接收来自的短信AWS。不接受免费电话号码，因为大多数号码都不支持短信。
- 对于企业而言AWS 账户，最佳做法是输入公司的电话号码和电子邮件地址，而不是个人的电话号码和电子邮件地址。为账户根用户配置个人的电子邮件地址或电话号码会使该人离开公司后难以恢复您的帐户。

更新独立版的主要联系人 AWS 账户

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

AWS Management Console

编辑独立版的主要联系人 AWS 账户

> **最小权限**
>
> 要执行下列步骤，您必须至少具有以下 IAM 权限：
>
> - `account:GetContactInformation`（查看主要联系方式）

- account:PutContactInformation（更新主要联系方式）

1. 以具有最低权限AWS Management Console的 IAM 用户或角色的身份登录。
2. 在窗口的右上角选择您的账户名称，然后选择账户。
3. 向下滚动到 “联系信息” 部分，然后在其旁边选择 “编辑”。
4. 更改任何可用字段中的值。
5. 完成所有更改后，选择 “更新”。

AWS CLI & SDKs

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

- GetContactInformation
- PutContactInformation

注意事项

- 要通过管理账户或组织中的委托管理员账户对成员账户执行这些操作，必须为账户服务启用可信访问权限。

最小权限

对于每个操作，您必须拥有映射到该操作的权限：

- account:GetContactInformation
- account:PutContactInformation

如果您使用这些个人权限，则可以授予某些用户仅读取联系人信息的权限，而授予其他用户同时读取和写入的权限。

Example

以下示例检索来电者账户的当前主要联系人信息。

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

Example

以下示例为来电者的账户设置了新的主要联系人信息。

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

如果成功，此命令不会产生任何输出。

更新组织AWS 账户中任何人的主要联系人

要在组织中编辑您的主要联系人详细信息，请执行以下过程中的步骤。AWS 账户

其他要求

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

- 您的组织必须启用所有功能才能管理您的成员账户的设置。这允许管理员控制成员帐户。这是在创建组织时默认设置的。如果您的组织设置为仅限整合账单，并且您想要启用所有功能，请参阅启用组织中的所有功能。
- 您需要为AWS账户管理服务启用可信访问权限。要进行此设置，请参阅为AWS账户管理启用可信访问权限。

AWS Management Console

编辑组织AWS 账户中任何人的主要联系人

1. 使用组织的管理账户凭据登录AWS Organizations控制台。
2. 从中 AWS 账户，选择要更新的账户。
3. 选择联系人信息，然后找到主要联系人，
4. 选择编辑。
5. 更改任何可用字段中的值。
6. 完成所有更改后，选择 “更新”。

AWS CLI & SDKs

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

- GetContactInformation
- PutContactInformation

> **注意事项**
>
> - 要通过管理账户或组织中的委托管理员账户对成员账户执行这些操作，必须为账户服务启用可信访问权限。
> - 您无法访问与您用于调用操作的组织不同的组织中的帐户。

> **最小权限**
>
> 对于每个操作，您必须拥有映射到该操作的权限：

- account:GetContactInformation
- account:PutContactInformation

如果您使用这些个人权限，则可以授予某些用户仅读取联系人信息的权限，而授予其他用户同时读取和写入的权限。

Example

以下示例检索组织中指定成员账户的当前主要联系人信息。使用的凭证必须来自组织的管理账户，或者来自账户管理的委托管理员账户。

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

Example

以下示例设置组织中指定成员账户的主要联系人信息。使用的凭证必须来自组织的管理账户，或者来自账户管理的委托管理员账户。

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

如果成功，此命令不会产生任何输出。

更新安全挑战问题

安全质询问题是一种验证方法，以前用于在账户恢复场景中验证身份。它们不如更现代的验证形式（例如多因素身份验证 (MFA)）那么安全。如果您当前有安全质疑问题处于活动状态AWS 账户，则AWS Support可以使用这些问题来帮助验证您作为账户所有者的身份。

> **Important**
>
> 从 2024 年 1 月 5 日起，对于尚未启用和使用安全挑战问题的账户，AWS将不再支持这些问题。这将删除从 “帐户” 页面中添加新的安全质询问题的选项AWS Management Console。如果您已经设置了安全挑战问题，或者已经在AWS组织的管理账户中设置了这些问题，则可以继续使用这些问题。2025 年 1 月 6 日之后，AWS将不再支持所有剩余客户的安全挑战问题。我们建议您改为添加 MFA。有关更多信息，请参阅AWS账户停止使用安全质询问题。

要编辑现有的安全质询问题并提供答案，请执行以下过程中的步骤。

AWS Management Console

编辑您的安全挑战问题 AWS 账户

> **最小权限**
>
> 要执行下列步骤，您必须至少具有以下 IAM 权限：
>
> - `account:GetChallengeQuestions`（查看安全挑战问题）
> - `account:PutChallangeQuestions`（设置或更新安全质询问题）

1. 以AWS 账户根用户或的AWS Management Console身份登录，以具有最低权限的 IAM 用户或角色的身份登录。
2. 在窗口的右上角选择您的账户名称，然后选择账户。
3. 向下滚动到安全挑战问题部分，然后选择编辑。

> **Note**
>
> 如果您没有看到 “编辑” 选项，则可能是您不是以账户的 root 用户身份登录的，也不是以具有上述最低权限的用户身份登录。

4. 更改任何可用字段中的值。您可以选择任何提供的问题，然后输入相应的答案。
5. 完成更改后，选择更新。

AWS CLI & SDKs

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

指定 AWS 区域 您的账户可以使用哪个

AWS 区域是世界上有多个可用区的物理位置。可用区由一个或多个独立 AWS 的数据中心组成，每个数据中心都具有冗余电源、网络和连接，位于不同的设施中。这意味着每个区域在物理上 AWS 区域都是孤立的，并且独立于其他区域。区域提供容错能力、稳定性和弹性，还可以减少延迟。有关可用区域和即将推出区域的地图，请参阅 区域和可用区。

除非您明确使用 AWS 服务提供的复制功能，否则您在一个区域创建的资源不存在于任何其他区域。例如，Amazon S3 和 Amazon EC2 支持跨区域复制。某些服务，例如 AWS Identity and Access Management (IAM)，没有区域资源。

您的账户确定了适用于您的区域。

- AWS 账户 提供了多个区域，因此您可以在满足您要求的位置启动 AWS 资源。例如，您可能希望在欧洲启动 Amazon EC2 实例，以便更接近您的欧洲客户或满足法律要求。
- AWS GovCloud （美国西部）账户提供对 AWS GovCloud （美国西部）地区和 AWS GovCloud （美国东部）地区的访问权限。有关更多信息，请参阅 AWS GovCloud (US)。
- 亚马逊 AWS （中国）账户仅提供北京和宁夏地区的访问权限。有关更多信息，请参阅 中国的 Amazon Web Services。

有关区域名称及其相应代码的列表，请参阅《AWS 通用参考指南》中的区域终端节点。有关每个区域（不含终端节点）支持的 AWS 服务列表，请参阅AWS 区域服务列表。

> **Important**
>
> AWS 建议您使用区域 AWS Security Token Service (AWS STS) 终端节点而不是全球终端节点来减少延迟。来自区域 AWS STS 终端节点的会话令牌在所有 AWS 区域都有效。如果您使用区域 AWS STS 终端节点，则无需进行任何更改。但是，来自全局 AWS STS 终端节点 (https://sts.amazonaws.com) 的会话令牌仅在 AWS 区域 您启用或默认启用的情况下才有效。如果您打算为账户启用新区域，则可以使用来自区域 AWS STS 终端节点的会话令牌，也可以激活全球 AWS STS 终端节点来发放全部有效的会话令牌 AWS 区域。在所有区域有效的会话令牌更大。如果您存储会话令牌，这些较大的令牌可能会影响您的系统。有关 AWS STS 终端节点如何与 AWS 区域配合使用的更多信息，请参阅AWS STS 在 AWS 区域中管理。

主题

启用和禁用区域之前的注意事项

在启用或禁用区域之前，请务必考虑以下几点：

- 2019 年 3 月 20 日之前推出的区域默认处于启用状态， AWS 最初 AWS 区域 默认启用所有新区域，这意味着您可以立即开始在这些区域中创建和管理资源。您无法启用或禁用默认已启用的区域。如今，当 AWS 添加区域时，新区域默认处于禁用状态。如果您希望您的用户能够在新区域中创建和管理资源，则需要先启用该区域。默认情况下，以下区域处于禁用状态。

名称	代码
非洲（开普敦）	af-south-1
亚太地区（香港）	ap-east-1
亚太地区（海得拉巴）	ap-south-2
亚太地区（雅加达）	ap-southeast-3
亚太地区（墨尔本）	ap-southeast-4

名称	代码
加拿大（卡尔加里）	ca-west-1
欧洲地区（米兰）	eu-south-1
欧洲（西班牙）	eu-south-2
欧洲（苏黎世）	eu-central-2
以色列（特拉维夫）	il-central-1
中东（巴林）	me-south-1
中东（阿联酋）	me-central-1

- 您可以使用 IAM 权限来控制对区域的访问权限 — AWS Identity and Access Management (IAM) 包括四种权限，允许您控制哪些用户可以启用、禁用、获取和列出区域。有关更多信息，请参阅《AWS Billing and Cost Management 用户指南》中的 Billing and Cost Management 操作策略。您也可以使用`aws:RequestedRegion`条件键来控制对 AWS 服务 中的访问权限 AWS 区域。
- 启用区域是免费的 — 启用区域不收取任何费用。您只需为在新区域中创建的资源付费。
- 禁用某个区域会禁用 IAM 对该区域资源的访问权限 — 如果您禁用仍包含 AWS 资源的区域，例如亚马逊弹性计算云 (Amazon EC2) 实例，则您将失去对该区域资源的 IAM 访问权限。例如，您不能使用 AWS Management Console 来查看或更改禁用区域中任何 EC2 实例的配置。
- 如果您禁用某个区域，则活动资源将继续收费 — 如果您禁用了仍包含 AWS 资源的区域，则这些资源（如果有）的费用将继续按标准费率累计。例如，如果禁用包含 Amazon EC2 实例的区域，则即使实例不可访问，您仍然必须为这些实例支付费用。
- 禁用区域并不总是立即可见 ——禁用区域后，服务和控制台可能会暂时可见。禁用区域可能需要几分钟到几小时才能生效。
- 在某些情况下，启用区域需要几分钟到几小时的时间 — 当您启用某个区域时， AWS 会执行一些操作来准备您在该区域的账户，例如将您的 IAM 资源分配到该区域。对于大多数账户，此过程需要几分钟，但有时可能需要几个小时。在此过程完成之前，您无法使用区域。
- O@@ rganizations 可以在给定时间在整个 AWS 组织中打开 50 个区域选择请求 — 管理账户在任何时候都可能有 50 个待处理的请求等待其组织完成。一个请求等于为一个账户启用或禁用一个特定区域。
- 一个账户在任何给定时间可以有 6 个区域选择请求正在处理中 — 一个请求等于为一个账户启用或禁用一个特定区域。

- Amazon EventBridge 集成 — 客户可以在中订阅区域选项状态更新通知。 EventBridge EventBridge 系统将为每次状态更改创建通知，允许客户自动执行工作流程。
- Expressive Region-opt 状态 — 由于启用/禁用选择加入区域的异步性质，因此区域选择请求有四种潜在状态：
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

  当选择加入或选择退出处于任`ENABLING`一状态时，您无法将其取消。`DISABLING`否则，`ConflictException`将抛出 a。已完成（启用/禁用）区域选择请求取决于关键底层服务的配置。 AWS 尽管状态为，但有些 AWS 服务可能无法立即使用`ENABLED`。
- 与完全集成 AWS Organizations — 管理账户可以修改或读取 region-opt 以选择该 AWS 组织的任何成员账户。成员账户也可以读取/写入其所在地区的状态。

为独立账户启用或禁用区域

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

AWS Management Console

为独立版启用或禁用区域 AWS 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：
>
> - `account:ListRegions`（需要查看列表 AWS 区域 以及它们当前处于启用还是禁用状态）。
> - `account:EnableRegion`
> - `account:DisableRegion`

1. 以 AWS 账户根用户 或的AWS Management Console身份登录，以具有最低权限的 IAM 用户或角色的身份登录。

2. 在窗口的右上角选择您的账户名称，然后选择账户。
3. 在 “帐户” 页面上，向下滚动到该部分AWS 区域。

> **Note**
>
> 系统可能会提示您批准对这些信息的访问权限。 AWS 向与该账户关联的电子邮件地址和主要联系人电话号码发送请求。选择请求中的链接以在浏览器中将其打开，然后批准访问权限。

4. 在每个 AWS 区域 “操作” 列中都有选项的旁边，选择 “启用” 或 “禁用”，具体取决于您是否希望账户中的用户能够在该区域创建和访问资源。
5. 如果出现提示，请确认您的选择。
6. 完成所有更改后，选择 “更新”。

AWS CLI & SDKs

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

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

> **最小权限**
>
> 要执行以下步骤，您必须拥有映射到该操作的权限：
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

如果您使用这些个人权限，则可以授予某些用户仅读取区域选择信息的权限，而授予其他用户同时读取和写入的权限。

以下示例为组织中的指定成员账户启用区域。使用的凭证必须来自组织的管理账户，或者来自账户管理的委托管理员账户。

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

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

如果成功，此命令不会产生任何输出。

该操作是异步的。以下命令将允许您查看请求的最新状态。

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

在组织中启用或禁用某个区域

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

> **Note**
>
> AWS Organizations 托管策略AWSOrganizationsReadOnlyAccess或AWSOrganizationsFullAccess已更新，提供访问 AWS 账户管理 API 的权限，以便您可以从 AWS Organizations 控制台访问账户数据。要查看更新的托管策略，请参阅 Organizati ons AWS 托管策略的更新。

> **Note**
>
> 在通过管理账户或组织中的委托管理员账户执行这些操作以用于成员账户之前，您必须：
>
> - 启用组织中的所有功能以管理成员账户的设置。这允许管理员控制成员帐户。这是在创建组织时默认设置的。如果您的组织设置为仅限整合账单，并且您想启用所有功能，请参阅启用组织中的所有功能。

- 为 AWS 账户管理服务启用可信访问权限。要进行设置，请参阅为AWS账户管理启用可信访问。

AWS Management Console

在组织中启用或禁用区域

1. 使用贵组织的管理账户凭据登录 AWS Organizations 控制台。
2. 在AWS 账户页面上，选择要更新的账户。
3. 选择 “账户设置” 选项卡。
4. 在 “区域” 下，选择要启用或禁用的区域。
5. 选择 “操作”，然后选择 “启用” 或 “禁用” 选项。
6. 如果您选择了 “启用” 选项，请查看显示的文本，然后选择 “启用区域”。
7. 如果您选择了 “禁用” 选项，请查看显示的文本，键入 “禁用” 进行确认，然后选择 “禁用区域”。

AWS CLI & SDKs

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

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

最小权限

要执行以下步骤，您必须拥有映射到该操作的权限：

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

如果您使用这些个人权限，则可以授予某些用户仅读取区域选择信息的权限，而授予其他用户同时读取和写入的权限。

以下示例为组织中的指定成员账户启用区域。使用的凭证必须来自组织的管理账户，或者来自账户管理的委托管理员账户。

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

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

如果成功，此命令不会产生任何输出。

> **Note**
>
> 一个组织在给定时间最多只能有 20 个区域请求。否则，您将收到`TooManyRequestsException`.

该操作是异步的。以下命令将允许您查看请求的最新状态。

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

创建或更新您的AWS 账户别名

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

要了解如何创建或更新账户别名，请参阅 IAM 用户指南中的创建、删除和列出AWS 账户别名。

为您的账单AWS 账户

对于与您的账单相关的程序和任务AWS 账户，请参阅中的以下主题AWS 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

在印度管理账户

如果你注册一个新的AWS 账户然后选择印度作为您的联系地址，您的用户协议是Amazon Internet Services Private Limited(AISPL)，当地人AWSIndia.aispl 的卖家管理您的账单，您的发票总额以印度卢比 (INR) 而不是美元 (USD) 列出。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。

如果你有现有AWS 账户如果是印度地址，则您的账户是AWS或 AISPL，取决于您开设账户的时间。要了解您的账户是否在AWS或者 AISPL，请参见Determining which company your account is with。如果您是现有 AWS 客户，则可继续使用 AWS 账户。你也可以选择同时拥有AWS 账户还有一个 AISPL 账户，尽管它们无法合并到同一个账户中AWS组织。有关管理的信息AWS 账户，参见管理你的AWS 账户。

如果您的账户是 AISPL，请按照本主题中的步骤管理您的账户。本主题介绍如何注册 AISPL 账户、编辑有关 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

- 确定您的账户在哪家公司
- 创建一个AWS 账户用 AISPL
- 管理你的 AISPL 账户

确定您的账户在哪家公司

AWS 服务是由 AWS 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。

AWS Management Console

确定您的账户所属的公司

> **最小权限**
>
> 要执行以下步骤，您必须至少拥有以下 IAM 权限：
>
> - 此过程不需要特殊权限。

1. 打开 AWS Management Console (AWS Management Console)。
2. 在页面底部的页脚中，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 AWS。如果版权归 Amazon Internet Services Private Ltd. 所有，则您的账户属于 AISPL。

AWS CLI & SDKs

中不支持此任务AWS CLI或者通过其中一个的 API 操作AWS软件开发工具包。您只能通过使用来执行此任务AWS Management Console。

创建一个AWS 账户用 AISPL

AISPL 是以下产品的本地销售商AWS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。

AWS Management Console

注册 AISPL 账户

> **最小权限**
>
> 要执行以下步骤，您必须至少拥有以下 IAM 权限：
>
> - 因为这个操作是在你做完之前发生的AWS 账户，此操作不需要AWS权限。

1. 打开AWS Management Console，然后选择登录到控制台。
2. 在登入页面，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. 在每个登录凭据字段中，输入您的信息，然后选择创建账户。
5. 在每个联系信息字段中，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，选择没有如果您没有永久账号 (PAN) 或想稍后再添加。如果您有 PAN 并想立即添加，请选择是的，并在平底锅字段输入您的 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. 对于提供电话号码，输入您的电话号码。如果你有电话分机号，用于分机，输入您的电话分机号。
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。在电话键盘上，输入屏幕上显示的四位数 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。验证您的付款方式并激活您的帐户后，您会收到一封确认激活帐户的电子邮件。

AWS CLI & SDKs

中不支持此任务AWS CLI或者通过其中一个的 API 操作AWS软件开发工具包。您只能通过使用来执行此任务AWS Management Console。

管理你的 AISPL 账户

除以下任务外，管理账户的程序与在印度境外创建的账户相同。请参阅管理你的AWS 账户。

使用AWS Management Console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号 (GST)
- 查看税务发票

关闭一个 AWS 账户

如果您不再需要您的 AWS 账户，可以按照本节中的说明随时将其关闭。关闭账户后，您可以在关闭账户之日起 90 天内将其重新打开。从您关闭账户之日到 AWS 永久关闭账户之间的时间跨度称为关闭后时段。

在关闭账户之前你需要知道什么

在关闭之前 AWS 账户，应考虑以下几点：

- 关闭您的账户将作为您终止该账户的 AWS 客户协议的通知。
- 在关闭资源 AWS 账户 之前，您无需删除其中的资源。但是，我们建议您备份要保留的所有资源或数据。有关如何备份特定资源的说明，请参阅该服务的相应AWS 文档。
- 您可以在关闭后的期间重新开设账户。如果您重新打开账户，则账户中剩余的服务将重新开始收费。您还需对任何未付的发票以及未偿还的预留实例和 Savings Pl ans 负责。
- 您仍需对账户关闭前所用服务的所有未付费用和费用负责。关闭账户后，您将在下个月收到账 AWS 单。例如，如果您在 1 月 15 日关闭了账户，则将在 2 月初收到账单，用于 1 月 1 日至 1 月 15 日期间产生的使用量。关闭账户后，您将继续收到预留实例和 S avin gs Plans 的发票，直到它们到期。
- 您将无法再访问您账户中以前提供的 AWS 服务。但是，在关闭后 AWS 账户 期间，您只能登录并访问已关闭的账单信息、访问账户设置或联系方式。AWS Support
- 您不能使用关闭时 AWS 账户 在您注册的电子邮件地址与其他电子邮件地址相同的主电子邮件地址 AWS 账户。如果您想为不同的电子邮件地址使用相同的电子邮件地址 AWS 账户，我们建议您在关闭之前对其进行更新。有关更新电子邮件地址的说明，请参阅更新 root 用户的AWS 账户姓名、电子邮件地址或密码。
- 如果您在根用户上启用了多重身份验证 (MFA)，或者在 IAM 用户上配置了 MFA 设备，那么在 AWS 账户您关闭账户时，MFA 不会自动删除。如果您选择在关闭后的 90 天内启用 MFA，请保持 MFA 设备处于活动状态，直到关闭后的期限到期，以防您需要在此期间访问账户。请注意，永久关闭您的账户后，硬件 TOTP 令牌设备无法与其他用户关联。如果您想稍后与其他用户一起使用硬件 TOTP 令牌，则可以选择在关闭账户之前停用硬件 MFA 设备。适用于 IAM 用户的 MFA 设备必须由账户管理员删除。

成员账户的其他注意事项

- 当您关闭成员账户时，该账户要等到关闭后期过后才会从组织中删除。在后关闭期内，已关闭的成员账户仍会计入组织中的账户配额。为避免账户计入配额，请参阅在关闭组织成员账户之前将其从组织中移除。

- 在连续 30 天的周期内，您只能关闭 10% 的成员账户。此限额不受日历月的限制，而是在您关闭账户时开始。在首次关闭账户后的 30 天内，您不能超过 10% 的账户关闭限额。即使有 10% 的账户超过 1000 个，账户关闭的最低限度为 10 个，最大账户关闭量为 1000 个。有关 Organizations 配额的更多信息，请参阅配额 AWS Organizations。
- 如果您使用 Cont AWS rol Tower，则需要先取消对成员账户的管理，然后再尝试关闭该账户。请参阅《 AWS Control Tower 用户指南》中的 取消管理成员账户。

特定于服务的注意事项

- AWS Marketplace 账户关闭后，订阅不会自动取消。如果您有任何订阅，请先终止订阅中的所有软件实例。然后，前往 AWS Marketplace 控制台的 “管理订阅” 页面并取消您的订阅。
- 系统不会自动删除注册到 Route 53 的域。在关闭之前 AWS 账户，您有四个选择：
  - 您可以禁用自动续订，域名将在注册期到期后自动删除。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 AWS 账户。有关更多信息，请参阅将域转移到其他 AWS 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。
  - 如果您已经关闭了账户，则可以向其提交一个案例， AWS Support寻求域名转移方面的帮助。

如何关闭账户

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

如果您在关闭账户的过程中遇到任何问题，请参阅对 AWS 账户 关闭问题进行故障排除。

Standalone account

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

从 “账户” 页面关闭独立账户

1. 在要关闭 AWS Management Console 的中，以 root 用户身份登录。 AWS 账户 作为 IAM 用户或角色登录时，您无法关闭账户。
2. 在右上角的导航栏上，选择您的账户名或账号，然后选择账户。
3. 在 “账户” 页面上，滚动至页面底部的 “关闭账户” 部分。阅读并确保您了解账户关闭流程。

4. 选择 “关闭账户” 按钮以启动账户关闭流程。
5. 几分钟后，您应该会收到一封电子邮件，确认您的账户已关闭。

> **Note**
>
> 其中一个 AWS 软件开发工具包 AWS CLI 的 API 操作不支持此任务。只有使用才能执行此任务 AWS Management Console。

Member account

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

通过 AWS Organizations 控制台关闭成员账户

1. 登录 AWS Organizations 控制台。
2. 在 AWS 账户 页面上，找到并选择您想要关闭的成员账户的名称。您可以导航 OU 层次结构，或查看没有 OU 结构的账户的平面列表。
3. 选择页面顶部的账户名称旁边的 Close（关闭）。处于整合账单模式的 Organizations 将无法在控制台中看到 “关闭” 按钮。要在整合账单模式下关闭账户，您需要按照 “独立账户” 选项卡中的步骤操作。
4. 选中每个复选框以确认所有必需的账户关闭报表。
5. 输入成员账户 ID，然后选择关闭账户。

从 “账户” 页面关闭成员账户

或者，您可以直接从中的账户页面关闭 AWS 成员账户 AWS Management Console。如需 step-by-step指导，请按照 “独立账户” 选项卡中的说明进行操作。

使用 AWS CLI 和 SDK 关闭成员账户

有关如何使用 AWS CLI 和软件开发工具包关闭成员账户的说明，请参阅AWS Organizations 用户指南中的关闭组织中的成员账户。

Management account

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

> **Note**
>
> 您不能直接从 AWS Organizations 控制台关闭管理账户。

从 “账户” 页面关闭管理账户

1. 以您要关闭 AWS Management Console 的管理账户的 root 用户身份登录。作为 IAM 用户或角色登录时，您无法关闭账户。
2. 确认您的组织中没有剩余的活跃成员账户。为此，请前往AWS Organizations 控制台，确保所有成员账户都显示在账户名称Suspended旁边。如果您的会员账户仍处于活跃状态，则需要遵循成员账户选项卡中提供的账户关闭指导方针，然后才能进入下一步操作。
3. 在右上角的导航栏上，选择您的账户名或账号，然后选择账户。
4. 在 “账户” 页面上，滚动至页面底部的 “关闭账户” 部分。阅读并确保您了解账户关闭流程。
5. 选择 “关闭账户” 按钮以启动账户关闭流程。
6. 几分钟后，您应该会收到一封电子邮件，确认您的账户已关闭。

> **Note**
>
> 其中一个 AWS 软件开发工具包 AWS CLI 的 API 操作不支持此任务。只有使用才能执行此任务 AWS Management Console。

AWS GovCloud (US) account

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

关闭 AWS GovCloud (US) 账户

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

关闭账户后会发生什么

关闭账户后，将立即发生以下情况：

- 您将收到一封电子邮件，确认账户已关闭 root 用户的电子邮件地址。如果您在几个小时内没有收到此电子邮件，请参阅对 AWS 账户 关闭问题进行故障排除。
- 您关闭的任何成员账户都将在 AWS Organizations 控制台的账户名称旁边显示一个SUSPENDED标签。
- 如果您已 AWS 账户 向其他账户授予访问您中服务的权限，则账户关闭后，从这些账户发出的任何访问请求都将失败。如果您重新打开 AWS 账户，如果您向其他人授予了必要的权限，则他们 AWS 账户 可以再次访问您账户的 AWS 服务和资源。

关闭后期

关闭后期是指从您关闭账户之日到 AWS 永久关闭账户 AWS 账户之间的时间长度。关闭后的期限为90天。在关闭后期间，您只能通过重新打开帐户来访问您的内容和 AWS 服务。关闭后期过后，将 AWS 永久关闭您的 AWS 账户，您将无法再重新开放。 AWS 还将删除您账户中的所有内容和资源。账户永久关闭后，其 AWS 账户 ID 将永远无法重复使用。

重新打开你的 AWS 账户

您的账户将在 90 天后永久关闭，之后您将无法重新打开账户， AWS 并将删除账户中剩余的内容。要在账户永久关闭之前重新开设账户，(1) 您必须AWS Support尽快联系；(2) 我们必须在账户关闭之日起 60 天内收到所有未付余额的全额付款，包括提供发票上规定的必要信息。

在您的组织中使用AWS账户管理

AWS Organizations是一项可用于以群组AWS 账户形式管理您的AWS服务。这提供了诸如整合账单之类的功能，将所有账户的账单分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。有关 AWS Organizations 的更多信息，请参阅《AWS Organizations 用户指南》。

可信访问权限

当您AWS Organizations使用群组管理帐户时，组织的大多数管理任务只能由组织的管理帐户执行。默认情况下，这仅包括与管理组织本身相关的操作。通过启用组织与该AWS服务之间的可信访问，您可以将此附加功能扩展到其他服务。可信访问向指定AWS服务授予访问有关组织及其所含帐户信息的权限。当您为账户管理启用可信访问时，账户管理服务会向组织及其管理账户授予访问该组织所有成员账户的元数据（例如主要或备用联系人信息）的权限。

有关更多信息，请参阅为AWS账户管理启用可信访问：

委派管理员

启用可信访问后，您还可以选择将您的一个成员账户指定为账户管理的委托管理员AWS帐户。这允许委托的管理员账户为组织中的成员账户执行与以前只有管理账户才能执行的相同的账户管理元数据管理任务。委托的管理员账户只能访问账户管理服务的管理任务。委托管理员账户不具有管理账户对组织的所有管理访问权限。

有关更多信息，请参阅启用委托管理员账户AWS账户管理：

服务控制策略

当您AWS 账户属于由AWS Organizations其管理的组织时，该组织的管理员可以应用服务控制策略(SCP)，限制成员账户中的委托人可以做什么。SCP 从不授予权限；相反，它是一个限制成员账户可以使用的权限的过滤器。成员账户中的用户或角色（委托人）只能执行那些与适用于该账户的 SCP 和关联到委托人的 IAM 权限策略相交的操作。例如，您可以使用 SCP 来防止账户中的任何委托人修改自己账户的备用联系人。

例如，适用于的 SCPAWS 账户，请参阅有关限制访问AWS Organizations服务控制策略。

为AWS账户管理启用可信访问

为AWS账户管理启用可信访问权限允许管理账户的管理员修改中每个成员账户的特定信息和元数据（例如，主要或备用联系人详细信息）AWS Organizations。有关更多信息，请参阅AWS账户管理和

AWS Organizations《AWS Organizations用户指南》。有关可信访问的工作原理的一般信息，请参阅与其他AWS服务AWS Organizations一起使用。

启用可信访问后，您可以在支持该accountID参数的账户管理 API 操作中使用该参数。只有使用管理账户的凭证调用操作，或者如果您启用了来自组织的委托管理员账户，则只有在调用操作时，才能成功使用此参数。有关更多信息，请参阅启用委托管理员账户AWS账户管理：

使用以下步骤为组织中的账户管理启用可信访问权限。

> 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执行此操作。
> - 您的组织必须已启用所有功能。

AWS Management Console

为AWS账户管理启用可信访问权限

1. 登录到 AWS Organizations 控制台。您必须以 IAM 用户身份登录、担任 IAM 角色，或以组织管理账户中的根用户身份登录（但不建议这样操作）。
2. 在导航窗格中选择服务。
3. 在服务列表中选择AWS账户管理。
4. 选择 Enable trusted access (启用可信访问)。
5. 在 “为AWS账户管理启用可信访问” 对话框中，键入 enab le 进行确认，然后选择 “启用可信访问”。

AWS CLI & SDKs

为AWS账户管理启用可信访问权限

运行以下命令后，您可以使用组织管理账户的证书调用账户管理 API 操作，这些操作使用--accountId参数引用组织中的成员账户。

- AWS CLI: enable-aws-service-access

  以下示例在呼叫账户的组织中为AWS账户管理启用可信访问权限。

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

如果成功，此命令不会产生任何输出。

启用委托管理员账户AWS账户管理

委托管理员帐户可以调用AWS组织内的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，您必须满足以下要求：
>
> - 您只能从组织的管理账户执行此操作。
> - 您的组织必须已启用所有功能。
> - 您必须具有为组织中的账户管理启用了可信访问.

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AWS CLI和AWS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。

AWS Management Console

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

AWS 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托管理员。

您必须指定以下服务委托人：

```
account.amazonaws.com
```

- AWS 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AWS CLI和使用`--account-id`参数可引用组织内的成员账户。

有关限制访问AWS Organizations服务控制策略

本主题提供的示例说明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AWS 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：防止账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独立账户模式. 这样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：防止任何成员账户修改组织中任何其他成员账户的备用联系人

以下示例概括了Resource元素改为 “*”，这意味着它同时适用于两者独立模式请求和组织模式请求. 这意味着，即使是 Account Management 的委派管理员帐户（如果适用了 SCP），也无法更改组织中任何帐户的任何备用联系人。

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

Example 示例 3：阻止 OU 中的成员账户修改自己的备用联系人

以下示例 SCP 包含一个条件，用于将账户的组织路径与两个 OU 的列表进行比较。这会导致阻止指定 OU 中任何账户的委托人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/"
                    ]
                }
            }
    ]
}
```

中的安全性AWS账户管理

AWS 的云安全性的优先级最高。作为 AWS 客户，您将从专为满足大多数安全敏感型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AWS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 – AWS负责保护在 AWS Cloud 中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。第三方审核员定期测试和验证我们的安全性的有效性，作为 AWS Compliance Programs 的一部分. 要了解适用于账户管理的合规性计划，请参阅AWS 服务在合规计划范围内.
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您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。AWS账户管理。它介绍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AWS帮助您监控和保护您的账户管理资源的服务。

主题

- AWS账户管理中的数据保护
- AWS PrivateLink为了AWS账户管理
- 用于AWS账户管理的 Identity and Access Management
- AWS的托管策略AWS账户管理
- AWS账户管理合规性验证
- 中的故障恢复能力AWS账户管理
- AWS Account Management 中的基础设施安全性

AWS账户管理中的数据保护

分AWS担责任模型适用于AWS账户管理中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 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。您还负责您所使用的 AWS 服务的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

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

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务 中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您AWS 服务使用控制台、API 或 AWS SDK 进行账户管理或其他操作时。AWS CLI您在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，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。

AWS PrivateLink为了AWS账户管理

如果您使用 Amazon Virtual Private Cloud (Amazon VPC) 托管AWS资源，您可以访问AWS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AWS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，允许您将 VPC 连接到其他 VPCAWS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 (AWS PrivateLink)。

创建终端节点

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

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

> **Note**
>
> 在创建终端节点时，请采用以下格式将账户管理指定为您希望 VPC 连接到的服务：
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> 你必须完全如图所示使用字符串，指定us-east-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AWS区域。

有关使用 AWS CloudFormation 创建和配置端点的信息，请参阅 AWS 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。您可以通过附加多个终端节点策略创建复杂的 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
- 使用 VPC 终端节点控制对服务的访问中的AWS 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，在该策略中指定以下内容：

- 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。AWS 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AWS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元素必须采用以下格式：

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

有关创建终端节点策略，请参阅使用 VPC 终端节点控制对服务的访问中的AWS PrivateLink指南.

用于AWS账户管理的 Identity and Access Management

AWS Identity and Access Management（IAM）是一项 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用账户管理资源。IAM 是一项无需额外费用即可使用的 AWS 服务。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- AWS账户管理如何与 IAM 配合使用

- 账户管理基于身份的策略示AWS例
- 使用基于身份的策略（IAM 策略）进行AWS账户管理
- AWS账户管理身份和访问权限疑难解答

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在账户管理中所做的工作。

服务用户-如果您使用账户管理服务完成工作，则您的管理员会为您提供所需的凭证和权限。当你使用更多的账户管理功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问账户管理中的某项功能，请参阅AWS账户管理身份和访问权限疑难解答。

服务管理员-如果您负责公司的账户管理资源，则可能拥有账户管理的完全访问权限。您的工作是确定您的服务用户应访问哪些账户管理功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解贵公司如何将 IAM 与账户管理结合使用，请参阅AWS账户管理如何与 IAM 配合使用。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理账户管理的访问权限。要查看您可以在 IAM 中使用的基于身份的账户管理策略示例，请参阅。账户管理基于身份的策略示AWS例

使用身份进行身份验证

身份验证是使用身份凭证登录 AWS 的方法。您必须作为 AWS 账户根用户、IAM 用户或通过分派 IAM 角色进行身份验证（登录到 AWS）。

您可以使用通过身份源提供的凭证以联合身份登录到 AWS。AWS IAM Identity Center（IAM Identity Center）用户、您公司的单点登录身份验证以及您的 Google 或 Facebook 凭证都是联合身份的示例。当您以联合身份登录时，管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合身份验证访问 AWS 时，您就是在间接分派角色。

根据用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录到 AWS 的更多信息，请参阅《AWS 登录 用户指南》中的如何登录到您的 AWS 账户。

如果您以编程方式访问 AWS，则 AWS 将提供软件开发工具包（SDK）和命令行界面（CLI），以便使用您的凭证以加密方式签署您的请求。如果您不使用 AWS 工具，则必须自行对请求签名。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的签署 AWS API 请求。

无论使用何种身份验证方法，您都可能需要提供其它安全信息。例如，AWS 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《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的在 AWS 中使用多重身份验证（MFA）。

AWS 账户 根用户

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

联合身份

作为最佳实操，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 AWS 服务。

联合身份是来自企业用户目录、Web 身份提供程序、AWS Directory Service、Identity Center 目录的用户，或任何使用通过身份来源提供的凭证来访问 AWS 服务的用户。当联合身份访问 AWS 账户时，他们担任角色，而角色提供临时凭证。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和组，也可以连接并同步到您自己的身份来源中的一组用户和组以跨所有 AWS 账户和应用程序使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？

IAM 用户和组

IAM 用户 是 AWS 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组 是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 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分派。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 AWS 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 AWS Management Console 中暂时分派 IAM 角色。您可以调用 AWS CLI 或 AWS 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：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户或角色可分派 IAM 角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户存取权限的主要方式。但是，对于某些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为座席）。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 AWS 服务使用其它 AWS 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主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话：当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。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启动另一个操作。FAS 使用主体调用 AWS 服务 的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务 委派权限的角色。
  - 服务相关角色 - 服务相关角色是与 AWS 服务关联的一种服务角色。服务可以代入角色来代表您执行操作。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。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 AWS CLI 或 AWS 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 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文

件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 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 AWS 身份或资源，以控制 AWS 中的访问。策略是 AWS 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，AWS 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 AWS 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《IAM 用户指南》中的 JSON 策略概览。

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

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

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

基于身份的策略

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

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AWS 账户中的多个用户、组和角色的独立策略。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅 IAM 用户指南 中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略 和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资

源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。主体可以包括账户、用户、角色、联合用户或 AWS 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 AWS 托管策略。

访问控制列表（ACL）

访问控制列表（ACL）控制哪些主体（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、AWS 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《Amazon Simple Storage Service 开发人员指南》 中的访问控制列表（ACL）概览。

其他策略类型

AWS 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。您可以为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 字段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 JSON 策略，指定了组织或组织单位（OU）在 AWS Organizations 中的最大权限。AWS Organizations 服务可以分组和集中管理您的企业拥有的多个 AWS 账户 账户。如果在组织内启用了所有特征，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（包括每个 AWS 账户根用户）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS 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用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 AWS 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。

AWS账户管理如何与 IAM 配合使用

在使用 IAM 管理账户管理访问权限之前，请先了解账户管理中可以使用哪些 IAM 功能。

您可以在AWS账户管理中使用的 IAM 功能

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

要全面了解账户管理和其他AWS服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS服务。

账户管理基于身份的政策

支持基于身份的策略	是

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

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

账户管理基于身份的策略示例

要查看账户管理基于身份的政策示例，请参阅。账户管理基于身份的策略示AWS例

账户管理中基于资源的政策

支持基于资源的策略	否

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

要启用跨账户存取，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当主体和资源处于不同的 AWS 账户 中时，则信任账户中的 IAM 管理员还必须授予主体实体（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主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

账户管理的政策措施

支持策略操作	是

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

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

在策略中包含操作以授予执行关联操作的权限。

要查看账户管理操作列表，请参阅《服务授权参考》中AWS账户管理定义的操作。

账户管理中的策略操作在操作前使用以下前缀。

```
account
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

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

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

要查看账户管理基于身份的政策示例，请参阅。账户管理基于身份的策略示AWS例

账户管理的政策资源

支持策略资源	是

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

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

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

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

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

- account

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

- accountInOrganization

  此resource类型仅匹配由AWS 账户该AWS Organizations服务管理的组织中的成员帐户。

要查看账户管理资源类型及其 ARN 的列表，请参阅服务授权参考中的AWS账户管理定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅AWS账户管理定义的操作。

要查看账户管理基于身份的政策示例，请参阅。账户管理基于身份的策略示AWS例

账户管理的政策条件密钥

支持特定于服务的策略条件键	有

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

在 Condition 元素（或 Condition 块）中，您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 元素中指定多个密钥，则 AWS 使用逻辑 AND 运算评估它们。如果您要为单个条件键指定多个值，则 AWS 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。

您也可以在指定条件时使用占位符变量。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。

AWS 支持全局条件键和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅《IAM 用户指南》中的 AWS 全局条件上下文键。

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

- 账户:TargetRegion

  此条件键采用一个由AWS区域代码列表组成的参数。它允许您筛选策略，使其仅影响适用于指定区域的操作。

- 账户:AlternateContactTypes

  此条件键采用备用联系人类型的列表：

  - 计费
  - OPERATIONS（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:AccountResourceOrgPaths

  此条件键采用一个参数，该参数由带有通配符的 ARN 列表组成，这些通配符代表组织中的账户。它允许您筛选策略，使其仅影响那些针对具有匹配的 ARN 的账户的操作。例如，以下 ARN 仅匹配指定组织和指定组织单位 (OU) 中的那些账户。

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

- 账户:AccountResourceOrgTags

  此条件键采用一个由标签键和值列表组成的参数。它允许您筛选策略，使其仅影响那些属于组织成员且标有指定标签键和值的账户。

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

要查看账户管理基于身份的政策示例，请参阅。账户管理基于身份的策略示AWS例

账户管理中的访问控制列表

支持 ACL	否

访问控制列表（ACL）控制哪些主体（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。

使用账户管理实现基于属性的访问控制

支持 ABAC（策略中的标签）	有

基于属性的访问权限控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在 AWS 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 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

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

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

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

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的什么是 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权限控制（ABAC）。

在账户管理中使用临时证书

支持临时凭证	有

某些 AWS 服务 在使用临时凭证登录时无法正常工作。有关更多信息，包括 AWS 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 AWS 服务。

如果您不使用用户名和密码而用其他方法登录到 AWS 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 AWS 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，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 AWS CLI 或者 AWS API 创建临时凭证。之后，您可以使用这些临时凭证访问 AWS。AWS 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。

账户管理的跨服务主体权限

支持转发访问会话 (FAS)	有

当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用 AWS 服务 的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

账户管理的服务角色

支持服务角色	否

服务角色是由一项服务代入、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务 委派权限的角色。

账户管理的服务相关角色

支持服务相关角色	否

服务相关角色是一种与 AWS 服务相关的服务角色。服务可以担任代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

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

账户管理基于身份的策略示AWS例

默认情况下，用户和角色无权创建或修改账户管理资源。他们也无法使用 AWS Management Console、AWS Command Line Interface（AWS CLI）或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。然后，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的 创建 IAM policy。

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

主题

- 策略最佳实践
- 使用中的 “账户” 页面 AWS Management Console
- 提供对账户页面的只读访问权限 AWS Management Console
- 提供对 “账户” 页面的完全访问权限 AWS Management Console

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除账户管理资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- AWS 托管策略及转向最低权限许可入门 – 要开始向用户和工作负载授予权限，请使用 AWS 托管策略来为许多常见使用场景授予权限。您可以在 AWS 账户中找到这些策略。建议通过定义特定于您的使用场景的 AWS 客户管理型策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略 或 工作职能的 AWS 托管策略。
- 应用最低权限 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 AWS 服务（例如 AWS CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，有助于制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Access Analyzer 策略验证。
- 需要多重身份验证 (MFA) – 如果您所处的场景要求您的 AWS 账户 中有 IAM 用户或根用户，请启用 MFA 来提高安全性。要在调用 API 操作时要求 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用中的 “账户” 页面 AWS Management Console

要访问中的账户页面AWS Management Console，您必须拥有最低限度的权限。这些权限必须允许您列出和查看有关您的详细信息AWS 账户。如果您创建的基于身份的策略比所需的最低权限更严格，则无法为具有该策略的实体（IAM 用户或角色）正常运行控制台。

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

对于只需要调用 AWS CLI 或 AWS 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，您可以选择只允许访问与您尝试执行的 API 操作相匹配的操作。

提供对账户页面的只读访问权限 AWS Management Console

在以下示例中，您想授予一个 IAM 用户对中账户页面的AWS 账户只读访问权限AWS Management Console。附加了此政策的用户无法进行任何更改。

该`account:GetAccountInformation`操作授予查看 “帐户” 页面上大多数设置的权限。但是，要查看当前启用的AWS区域，您还必须包括该`account:ListRegions`操作。

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

提供对 “账户” 页面的完全访问权限 AWS Management Console

在以下示例中，您想授予一个 IAM 用户对中账户页面的AWS 账户完全访问权限AWS Management Console。附加了此政策的用户可以更改账户的设置。

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

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

使用基于身份的策略（IAM 策略）进行AWS账户管理

有关 AWS 账户和 IAM 用户的全面讨论，请参阅 IAM 用户指南中的什么是 IAM？。

有关如何能更新客户托管策略的说明，请参阅 IAM 用户指南中的编辑客户托管策略（控制台）。

AWS账户管理操作政策

此表汇总了授予您账户设置访问权限的权限。有关使用这些权限的策略示例，请参阅AWS账户管理策略示例。

> **Note**
>
> 要向 IAM 用户授予对账户页面中特定账户设置的写入GetAccountInformation权限AWS Management Console，除了要用于修改该设置的权限（或许可）之外，您还必须允许该权限。

权限名称	访问级别	描述
account:ListRegions	列出	授予列出可用区域的权限。
account:GetAccountInformation	读取	授予检索账户账户信息的权限。
account:GetAlternateContact	读取	授予检索账户备用联系人的权限。
account:GetChallengeQuestions	读取	授予检索账户质询问题的权限。
account:GetContactInformation	读取	授予检索账户主要联系信息的权限。
account:GetRegionOptStatus	读取	授予获取区域选择加入状态的权限。
account:CloseAccount	写入	授予关闭账户的权限。 **Note** 此权限仅适用于控制台。此权限不支持 API 访问。
account:DeleteAlternateContact	写入	授予删除账户备用联系人的权限。
account:DisableRegion	写入	授予禁用区域的权限。
account:EnableRegion	写入	授予允许使用某个区域的权限。
account:PutAlternateContact	写入	授予修改账户备用联系人的权限。

权限名称	访问级别	描述
account:PutChallengeQuestions	写入	授予修改账户质询问题的权限。 **Note** 此权限仅适用于控制台。此权限不支持 API 访问。
account:PutContactInformation	写入	授予更新账户主要联系信息的权限。

AWS账户管理身份和访问权限疑难解答

使用以下信息来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。

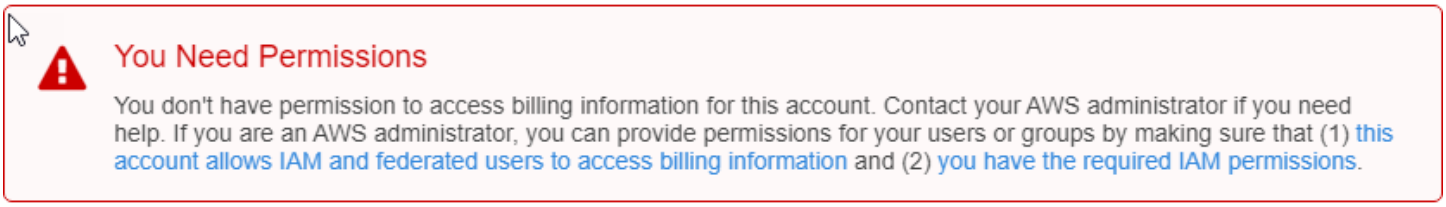
主题

- 我无权在 “账户” 页面中执行任何操作
- 我无权执行 iam:PassRole
- 我想允许我以外的人AWS 账户访问我的账户信息

我无权在 “账户” 页面中执行任何操作

如果AWS Management Console告诉您，无权执行某个操作，则必须联系管理员寻求帮助。管理员是指提供用户名和密码的人员。

当 mateojackson IAM 用户尝试使用控制台在的 “账户” 页面AWS 账户中查看其详细信息AWS Management Console但没有account:GetAccountInformation权限时，就会出现以下示例错误。



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

我无权执行 iam:PassRole

如果您收到错误消息，说您无权执行该iam:PassRole操作，则必须更新您的政策，以允许您将角色传递给账户管理。

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

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

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

如果您需要帮助，请联系 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人AWS 账户访问我的账户信息

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表（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AWS账户管理如何与 IAM 配合使用。
- 要了解如何为您拥有的 AWS 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 AWS 账户 中的 IAM 用户提供访问权限。
- 要了解如何为第三方 AWS 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 AWS 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。

AWS的托管策略AWS账户管理

AWS账户管理目前提供两个AWS可供您使用的托管策略：

- AWS托管策略：AWSAccountManagementReadOnlyAccess
- AWS托管策略：AWSAccountManagementFullAccess
- 账户管理更新至AWS托管策略

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

请记住，AWS 托管式策略可能不会为您的特定使用场景授予最低权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

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

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS托管策略：AWSAccountManagementReadOnlyAccess

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

此策略提供只读权限，仅可查看以下内容：

- 关于你的元数据AWS 账户
- 该AWS 区域已启用或禁用的AWS 账户（您只能使用以下方法查看账户中区域的状态AWS控制台）

它通过授予运行任何内容的权限来实现此目的`Get*`要么`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AWS 区域用于账户。

权限详细信息

此策略包含以下权限。

- `account`— 允许校长检索有关的元数据信息AWS 账户。它还允许校长列出AWS 区域中为账户启用的AWS Management Console。

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

AWS托管策略：AWSAccountManagementFullAccess

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

此策略提供查看或修改以下内容的完全管理权限：

- 关于你的元数据AWS 账户
- 该AWS 区域已启用或禁用的AWS 账户（您只能使用以下方法查看状态或启用或禁用您的账户的区域AWS控制台）

它通过授予运行任何权限来做到这一点account操作。

权限详细信息

此策略包含以下权限。

- account— 允许校长查看或修改有关的元数据信息AWS 账户。它还允许校长列出AWS 区域已为该帐户启用并在中启用或禁用它们AWS Management Console。

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

```
        }
    ]
}
```

账户管理更新至AWS托管策略

查看有关更新的详细信息AWS自该服务开始跟踪这些更改以来，账户管理的托管政策。有关此页面变更的自动提醒，请订阅 “账户管理文档历史记录” 页面上的 RSS feed。

更改	说明	日期
AWS账户管理推出新版AWS管理策略并开始跟踪更改	账户管理最初启动时使用了以下内容AWS托管策略： • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	2021 年 9 月 30 日

AWS账户管理合规性验证

第三方审计师评估可在您的AWS 账户多个合规计划中运行的AWS服务的安全性和AWS合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其它。

有关特定合规计划范围内的AWS服务列表，请参阅按合规计划划分AWS 服务的范围和按合规计划AWS 服务。有关常规信息，请参阅AWS合规性计划。

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

在使用您的服务时，您的合规责任AWS 账户由您的数据的敏感性、贵公司的合规目标以及适用的法律和法规决定。 AWS提供以下资源以帮助实现合规性：

- 安全性与合规性快速入门指南 – 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署以安全性和合规性为重点的基准环境的步骤。
- Amazon Web Services 上的 HIPAA 安全性和合规性架构设计– 该白皮书介绍了公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。

> **Note**
>
> 并非所有 AWS 服务都符合 HIPAA 要求。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- AWS Config 开发人员指南中的使用规则评估资源 – 此 AWS Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub：此 AWS 服务 提供了 AWS 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践规范。
- AWS Audit Manager – 此 AWS 服务可帮助您持续审计您的 AWS 使用情况，以简化管理风险以及与相关法规和行业标准的合规性的方式。

中的故障恢复能力AWS账户管理

这些区域有：AWS围绕构建全球基础设施AWS 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AWS 区域和可用区的更多信息，请参阅AWS全球基础设施。

AWS Account Management 中的基础设施安全性

作为托管AWS服务，在您中运行的服务AWS 账户受到AWS全球网络安全的保护。有关 AWS 安全服务以及 AWS 如何保护基础架构的信息，请参阅 AWS 云安全。要按照基础设施安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的 基础设施保护。

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

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

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

监控AWS账户管理

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

- AWS CloudTrail捕获（记录）由您或代表您进行的 API 调用AWS 账户和相关事件，并将日志文件写入您指定的亚马逊简单存储服务 (Amazon S3) 存储桶。这使您可以识别哪些用户和帐户拨打了电话AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 AWS CloudTrail 用户指南。
- 亚马逊 EventBridge通过自动响应系统事件（例如应用程序可用性问题或资源更改）来提高您的AWS服务的自动化程度。来自AWS服务的事件几乎实时 EventBridge 地传送到。您可以编写简单的规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。有关更多信息，请参阅亚马逊 EventBridge 用户指南。

日志系统AWS使用账户管理 API 调用AWS CloudTrail

这些区域有：AWS账户管理 API 与AWS CloudTrail，该服务提供用户、角色或AWS调用账户管理操作的服务。CloudTrail 会将所有账户管理 API 调用捕获为事件。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）。如果您不配置跟踪记录，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、请求的发出时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅 AWS CloudTrail 用户指南。

CloudTrail 中的账户管理信息

在您的中，CloudTrail 已启用AWS 账户在您创建账户时。当账户管理操作发生活动时，该活动将记录在 CloudTrail 事件中，并与其他活动一同保存在 CloudTrailAWS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。AWS 账户. 有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录中的事件AWS 账户（包括账户管理运营的事件），请创建跟踪。通过跟踪记录，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。默认情况下，在中创建跟踪时AWS Management Console，该跟踪适用于所有AWS 区域. 此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Amazon S3 存储桶。您可以配置其它 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取措施。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- 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

AWS CloudTrail记录在中找到的所有账户管理 API 操作API 参考本指南的部分。例如，对 `CreateAccount`、`DeleteAlternateContact` 和 `PutAlternateContact` 操作的调用将在 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：

- 请求是针对根用户发出的请求还是AWS 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
- 请求是否由其它 AWS 服务发出

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解账户管理日志条目

跟踪记录是一种配置，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。一个事件表示一个来自任何源的请求，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": "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": "2021-04-30T18:33:00Z"
      }
    }
  },
  "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操作以删除当前OPERATIONS备用联系。

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

使用监控账户管理事件 EventBridge

亚马逊 EventBridge（以前称为“CloudWatch 事件”）可帮助您监控特定于其他的事件并启动使用其他事件的目标操作AWS 服务。来自AWS 服务的事件以近乎实时 EventBridge 的方式传送到。

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

有关更多信息，请参阅亚马逊 EventBridge 用户指南 EventBridge中的亚马逊入门。

账户管理活动

以下示例显示了账户管理的事件。事件会尽可能生成。

目前，只有特定于通过 CloudTrail启用和禁用区域和 API 调用的事件才可用于账户管理。

事件类型

- 启用和禁用区域的活动

启用和禁用区域的活动

当您通过控制台或 API 启用或禁用账户中的某个区域时，异步任务就会启动。初始请求将作为 CloudTrail 事件记录在目标账户中。此外，当启用或禁用过程开始时，将向调用者账户发送一个 EventBridge 事件，并在任一过程完成后再次发送一个事件。

以下示例事件显示了如何发送请求，表明`2020-09-30`该`ap-east-1`地区是`ENABLED`针对账户的`123456789012`。

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

```
      "status":"ENABLED"
   }
}
```

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

- ENABLED— 已成功为accountId指定区域启用
- ENABLING— 该地区正在为accountId所示的启用中
- DISABLED— 已成功禁用accountId指定区域
- DISABLING— 该地区正在被accountId指定禁用

以下示例事件模式创建了一个捕获所有 Region 事件的规则。

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

以下示例事件模式创建了一个仅捕获DISABLED区域事件ENABLED的规则。

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

API 引用

账户管理中的 API 操作 (account) 命名空间使您能够修改您的AWS 账户。

每个AWS 账户支持包含有关帐户信息的元数据，包括与该帐户关联的最多三个备用联系人的信息。除此之外，还有与之相关的电子邮件地址root 用户账户的。您只能指定与账户关联的以下每种联系人类型中的一种。

- 账单联系人
- 运营联系人
- 安全联系人

默认情况下，本指南中讨论的 API 操作直接适用于调用该操作的账户。这个身份在调用该操作的账户中通常是 IAM 角色或 IAM 用户，并且必须拥有 IAM 策略申请的权限才能调用 API 操作。或者，您可以从中的身份调用这些 API 操作AWS Organizations管理账户，并指定任何账户的账户 ID 号AWS 账户那是该组织的成员。

API 版本

此版本的账户 API 参考记录了账户管理 API 版本 2021-02-01。

> **Note**
>
> 作为直接使用 API 的替代方法，您可以使用以下任一项AWS软件开发工具包，由适用于各种编程语言和平台（Java、Ruby、.NET、iOS、安卓等）的库和示例代码组成。SDK 提供了一种创建编程访问权限的便捷方式AWS组织。例如，软件开发工具包负责对请求进行加密签名、管理错误和自动重试请求。有关 AWS 开发工具包的更多信息（包括如何下载和安装这些工具包），请参阅适用于 Amazon Web Services 的工具。

我们建议您使用AWS用于对账户管理服务进行编程 API 调用的 SDK。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，请参阅通过提出 HTTP 查询请求来调用 API在《账户管理用户指南》中。组织支持所有操作的 GET 和 POST 请求。也就是说，API 不要求您使用某些操作的 GET 请求和其他操作的 POST 请求。然而，GET 请求受 URL 的大小限制。因此，对于需要更大尺寸的操作，请使用 POST 请求。

签署请求

当你向发送 HTTP 请求时AWS，你必须签署请求，这样AWS可以识别是谁寄来的。你用你的签名来签署请求AWS访问密钥，由访问密钥 ID 和私有访问密钥组成。我们强烈建议您不要为您的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不受限制地访问您账户中的所有资源。相反，为具有管理权限的 IAM 用户创建访问密钥。作为另一种选择，使用AWS安全令牌服务生成临时安全证书，并使用这些证书签署请求。

要签署请求，我们建议您使用签名版本 4。如果您有使用签名版本 2 的现有应用程序，则无需对其进行更新即可使用签名版本 4。但是，现在某些操作需要签名版本 4。需要版本 4 的操作的文档指出了这一要求。有关更多信息，请参阅《IAM 用户指南》中的签署 AWS API 请求。

当你使用AWS命令行界面 (AWSCLI) 或其中一个AWS向其发出请求的 SDKAWS，这些工具会使用您在配置工具时指定的访问密钥自动为您签署请求。

对账户管理的支持和反馈

我们欢迎您提供反馈。将您的评论发送至feedback-awsaccounts@amazon.com或者将您的反馈和问题发布在账户管理支持论坛。有关 AWS 支持论坛的更多信息，请参阅论坛帮助。

示例是如何呈现的

账户管理作为对您的请求的响应而返回的 JSON 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。当示例输入参数还会导致超出屏幕的长字符串时，我们会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，一项记录服务AWS您的 API 调用AWS 账户并将日志文件传送到 Amazon S3 存储桶。通过使用收集的信息CloudTrail，您可以确定哪些请求已成功向账户管理发出、谁发出了请求、何时发出，等等。有关账户管理及其支持的更多信息CloudTrail，参见日志系统AWS使用账户管理 API 调用AWS CloudTrail。要了解有关以下内容的更多信息CloudTrail，包括如何将其打开和查找您的日志文件，请参阅AWS CloudTrail《用户指南》。

操作

支持以下操作：

- DeleteAlternateContact
- DisableRegion
- EnableRegion

- GetAlternateContact
- GetContactInformation
- GetRegionOptStatus
- ListRegions
- PutAlternateContact
- PutContactInformation

DeleteAlternateContact

从中删除指定的备用联系人AWS 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**
>
> 在更新由AWS Organizations管理的备用联系人信息之前AWS 账户，必须先启用AWS账户管理与 Organizations 之间的集成。有关更多信息，请参阅为AWS账户管理启用可信访问权限。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

AccountId

指定要通过此操作访问或修改的AWS账户的 12 位数账户 ID 号。

如果未指定此参数，则默认为用于调用操作的身份的AWS帐户。

要使用此参数，来电者必须是组织管理账户中的身份或委托管理员账户，并且指定的账户 ID 必须是同一组织中的成员账户。组织必须启用所有功能，组织必须为账户管理服务启用可信访问权限，并可选择分配委派管理员帐户。

> **Note**
>
> 管理账户无法自行指定AccountId；它必须不包括AccountId参数，从而在独立上下文中调用该操作。

要对不是组织成员的账户调用此操作，请不要指定此参数，而是使用属于您想要检索或修改其联系人的账户的身份调用该操作。

类型：字符串

模式：^\d{12}$

必需：否

AlternateContactType

指定要删除的备用联系人。

类型：字符串

有效值：BILLING | OPERATIONS | SECURITY

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

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

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

操作失败，因为主叫身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerException

由于内部错误，操作失败AWS。请稍后重试您的操作。

HTTP 状态代码：500

ResourceNotFoundException

操作失败，因为它指定了找不到的资源。

HTTP 状态代码：404

TooManyRequestsException

该操作失败，因为调用频率过高且超过了油门限制。

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

示例

示例 1

以下示例删除了使用其凭据调用操作的账户的安全备用联系人。

示例请求

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

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

示例响应

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

示例 2

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

示例请求

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

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

示例响应

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

另请参阅

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

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

DisableRegion

禁用（选择退出）账户的特定区域。

> **Note**
>
> 禁用某个区域的行为将移除对该区域内任何资源的所有 IAM 访问权限。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求体

请求接受采用 JSON 格式的以下数据。

AccountId

指定您要通过此操作访问或修改 AWS 账户 的 12 位帐户 ID 号。如果未指定此参数，则默认为用于调用操作 AWS 账户 的标识的。要使用此参数，来电者必须是组织管理账户中的身份或委派的管理员账户。指定的账户 ID 还必须是同一组织中的成员账户。组织必须启用所有功能，组织必须为账户管理服务启用可信访问权限，并可选择分配委派管理员帐户。

> **Note**
>
> 管理账户无法指定自己的账户AccountId。它必须不包括AccountId参数，从而在独立上下文中调用该操作。

要对不是组织成员的账户调用此操作，请不要指定此参数。相反，请使用属于您想要检索或修改其联系人的账户的身份来调用该接口。

类型：字符串

模式：^\d{12}$

必需：否

RegionName

为给定区域名称指定区域代码（例如，af-south-1）。当您禁用某个区域时， AWS 会执行操作以在您的账户中停用该区域，例如销毁该区域中的 IAM 资源。对大多数账户而言，此过程需要几分钟时间，但也有可能要用数小时的时间。在禁用过程完全完成之前，您无法启用该区域。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

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

错误

有关所有操作的常见错误信息，请参阅常见错误。

AccessDeniedException

操作失败，因为主叫身份没有所需的最低权限。

HTTP 状态代码：403

ConflictException

由于资源的当前状态存在冲突，无法处理该请求。例如，如果您尝试启用当前处于禁用状态（处于禁用状态）的区域，就会发生这种情况。

HTTP 状态代码：409

InternalServerException

由于内部存在错误，操作失败 AWS。请稍后重试您的操作。

HTTP 状态代码：500

TooManyRequestsException

该操作失败，因为调用频率过高且超过了油门限制。

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

另请参阅

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

- AWS 命令行界面
- AWS 适用于 .NET 的 SDK
- AWS 适用于 C++ 的 SDK
- AWS 适用于 Go 的 SDK
- AWS 适用于 Java 的 SDK V2
- AWS JavaScript V3 版软件开发工具包
- AWS 适用于 PHP 的 SDK V3
- AWS Python 软件开发工具包
- AWS 适用于 Ruby V3 的 SDK

EnableRegion

为账户启用（选择加入）特定区域。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

AccountId

指定您要通过此操作访问或修改AWS 账户的 12 位帐户 ID 号。如果未指定此参数，则默认为用于调用操作AWS 账户的标识的。要使用此参数，来电者必须是组织管理账户中的身份或委派的管理员账户。指定的账户 ID 还必须是同一组织中的成员账户。组织必须启用所有功能，组织必须为账户管理服务启用可信访问权限，并可选择分配委派管理员帐户。

> **Note**
>
> 管理账户无法指定自己的账户AccountId。它必须不包括AccountId参数，从而在独立上下文中调用该操作。

要对不是组织成员的账户调用此操作，请不要指定此参数。相反，请使用属于您想要检索或修改其联系人的账户的身份来调用该接口。

类型：字符串

模式：^\d{12}$

必需：否

RegionName

为给定区域名称指定区域代码（例如，af-south-1）。在启用一个区域时，AWS 将执行操作以准备您在该区域内的账户，例如将您的 IAM 资源分发给该区域。对于大多数账户，此过程需要几分钟，但可能需要几个小时。在此过程完成之前，您无法使用区域。此外，在启用过程完全完成之前，您无法禁用该区域。

类型：字符串

长度限制：最小长度为 0。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。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

操作失败，因为主叫身份没有所需的最低权限。

HTTP 状态代码：403

ConflictException

由于资源的当前状态存在冲突，无法处理该请求。例如，如果您尝试启用当前处于禁用状态（处于禁用状态）的区域，就会发生这种情况。

HTTP 状态代码：409

InternalServerException

由于内部存在错误，操作失败AWS。请稍后重试您的操作。

HTTP 状态代码：500

TooManyRequestsException

该操作失败，因为调用频率过高且超过了油门限制。

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

另请参阅

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

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

GetAlternateContact

检索附加到的指定备用联系人。AWS 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**
>
> 在更新由AWS Organizations管理的备用联系人信息之前AWS 账户，必须先启用AWS账户管理与 Organizations 之间的集成。有关更多信息，请参阅为AWS账户管理启用可信访问权限。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

AccountId

指定要通过此操作访问或修改的AWS账户的 12 位数账户 ID 号。

如果未指定此参数，则默认为用于调用操作的身份的AWS帐户。

要使用此参数，来电者必须是组织管理账户中的身份或委托管理员账户，并且指定的账户 ID 必须是同一组织中的成员账户。组织必须启用所有功能，组织必须为账户管理服务启用可信访问权限，并可选择分配委派管理员帐户。

> **Note**
>
> 管理账户无法自行指定AccountId；它必须不包括AccountId参数，从而在独立上下文中调用该操作。

要对不是组织成员的账户调用此操作，请不要指定此参数，而是使用属于您想要检索或修改其联系人的账户的身份调用该操作。

类型：字符串

模式：^\d{12}$

必需：否

AlternateContactType

指定您要检索的备用联系人。

类型：字符串

有效值：BILLING | OPERATIONS | SECURITY

必需：是

响应语法

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回的以下数据。

AlternateContact

一种包含指定备用联系人详细信息的结构。

类型：AlternateContact 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

操作失败，因为主叫身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerException

由于内部存在错误，操作失败AWS。请稍后重试您的操作。

HTTP 状态代码：500

ResourceNotFoundException

操作失败，因为它指定了找不到的资源。

HTTP 状态代码：404

TooManyRequestsException

该操作失败，因为调用频率过高且超过了油门限制。

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

示例

示例 1

以下示例检索使用其凭据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。您必须使用来自组织管理账户或账户管理服务的委托管理员账户的证书。

示例请求

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

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

示例响应

```
HTTP/1.1 200 OK
```

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

另请参阅

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

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

GetContactInformation

检索的主要联系人信息。AWS 账户

有关如何使用主要联系人操作的完整详细信息，请参阅更新主要联系人和备用联系人信息。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

AccountId

指定您要通过此操作访问或修改AWS 账户的 12 位帐户 ID 号。如果未指定此参数，则默认为用于调用操作AWS 账户的标识的。要使用此参数，来电者必须是组织管理账户中的身份或委派的管理员账户。指定的账户 ID 还必须是同一组织中的成员账户。组织必须启用所有功能，组织必须为账户管理服务启用可信访问权限，并可选择分配委派管理员帐户。

> **Note**
>
> 管理账户无法指定自己的账户AccountId。它必须不包括AccountId参数，从而在独立上下文中调用该操作。

要对不是组织成员的账户调用此操作，请不要指定此参数。相反，请使用属于您想要检索或修改其联系人的账户的身份来调用该接口。

类型：字符串

模式：^\d{12}$

必需：否

响应语法

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回的以下数据。

ContactInformation

包含与相关的主要联系人信息的详细信息AWS 账户。

类型：ContactInformation 对象

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

操作失败，因为主叫身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerException

由于内部存在错误，操作失败AWS。请稍后重试您的操作。

HTTP 状态代码：500

ResourceNotFoundException

操作失败，因为它指定了找不到的资源。

HTTP 状态代码：404

TooManyRequestsException

该操作失败，因为调用频率过高且超过了油门限制。

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

另请参阅

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

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK

- 适用于 Ruby V3 的 AWS SDK

GetRegionOptStatus

检索特定地区的选择加入状态。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

AccountId

指定您要通过此操作访问或修改AWS 账户的 12 位帐户 ID 号。如果未指定此参数，则默认为用于调用操作AWS 账户的标识的。要使用此参数，来电者必须是组织管理账户中的身份或委派的管理员账户。指定的账户 ID 还必须是同一组织中的成员账户。组织必须启用所有功能，组织必须为账户管理服务启用可信访问权限，并可选择分配委派管理员帐户。

> **Note**
>
> 管理账户无法指定自己的账户AccountId。它必须不包括AccountId参数，从而在独立上下文中调用该操作。

要对不是组织成员的账户调用此操作，请不要指定此参数。相反，请使用属于您想要检索或修改其联系人的账户的身份进行操作。

类型：字符串

模式：^\d{12}$

必需：否

RegionName

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

类型：字符串

长度限制：最小长度为 0。长度上限为 50。

必需：是

响应语法

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回的以下数据。

RegionName

传入的地区代码。

类型：字符串

长度限制：最小长度为 0。长度上限为 50。

RegionOptStatus

区域可能处于的潜在状态之一（启用、启用、已禁用、禁用、启用_By_Default）。

类型：字符串

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

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

操作失败，因为主叫身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerException

由于内部存在错误，操作失败AWS。请稍后重试您的操作。

HTTP 状态代码：500

TooManyRequestsException

该操作失败，因为调用频率过高且超过了油门限制。

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

另请参阅

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

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ListRegions

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

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

AccountId

指定您要通过此操作访问或修改AWS 账户的 12 位帐户 ID 号。如果未指定此参数，则默认为用于调用操作AWS 账户的标识的。要使用此参数，来电者必须是组织管理账户中的身份或委派的管理员账户。指定的账户 ID 还必须是同一组织中的成员账户。组织必须启用所有功能，组织必须为账户管理服务启用可信访问权限，并可选择分配委派管理员帐户。

> **Note**
>
> 管理账户无法指定自己的账户AccountId。它必须不包括AccountId参数，从而在独立上下文中调用该操作。

要对不是组织成员的账户调用此操作，请不要指定此参数。相反，请使用属于您想要检索或修改其联系人的账户的身份进行操作。

类型：字符串

模式：^\d{12}$

必需：否

MaxResults

命令输出中要返回的项目总数。如果可用项目总数大于指定值，则命令输出中会提供 a NextToken。要恢复分页，请在后续命令的 starting-token 参数中提供 NextToken 值。请勿直接在 AWS CLI 之外使用NextToken响应元素。有关用法示例，请参阅《AWS命令行界面用户指南》中的分页。

类型：整数

有效范围：最小值为 1。最大值为 50。

必需：否

NextToken

用于指定从何处开始分页的标记。这是之前截NextToken断的响应。有关用法示例，请参阅《AWS命令行界面用户指南》中的分页。

类型：字符串

长度限制：最小长度为 0。最大长度为 1000。

必需：否

RegionOptStatusContains

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

类型：字符串数组

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

必需：否

响应语法

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

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

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回的以下数据。

NextToken

如果有更多数据要返回，则会填充该数据。它应该传递到的next-token请求参数中list-regions。

类型：字符串

Regions

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

类型：Region 对象数组

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

操作失败，因为主叫身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerException

由于内部存在错误，操作失败AWS。请稍后重试您的操作。

HTTP 状态代码：500

TooManyRequestsException

该操作失败，因为调用频率过高且超过了油门限制。

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

另请参阅

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

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

PutAlternateContact

修改附加到的指定备用联系人。AWS 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**
>
> 在更新由AWS Organizations管理的备用联系人信息之前AWS 账户，必须先启用AWS账户管理与 Organizations 之间的集成。有关更多信息，请参阅为AWS账户管理启用可信访问权限。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

AccountId

指定您要通过此操作访问或修改的AWS账户的 12 位数账户 ID 号。

如果未指定此参数，则默认为用于调用操作的身份的AWS帐户。

要使用此参数，来电者必须是组织管理账户中的身份或委托管理员账户，并且指定的账户 ID 必须是同一组织中的成员账户。组织必须启用所有功能，组织必须为账户管理服务启用可信访问权限，并可选择分配委派管理员帐户。

> **Note**
>
> 管理账户无法自行指定AccountId；它必须不包括AccountId参数，从而在独立上下文中调用该操作。

要对不是组织成员的账户调用此操作，请不要指定此参数，而是使用属于您想要检索或修改其联系人的账户的身份调用该操作。

类型：字符串

模式：`^\d{12}$`

必需：否

AlternateContactType

指定您要创建或更新的备用联系人。

类型：字符串

有效值：`BILLING | OPERATIONS | SECURITY`

必需：是

EmailAddress

为备用联系人指定电子邮件地址。

类型：字符串

长度限制：最小长度为 0。最大长度为 64。

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

必需：是

Name

为备用联系人指定姓名。

类型：字符串

长度限制：最小长度为 0。最大长度为 64。

必需：是

PhoneNumber

为备用联系人指定电话号码。

类型：字符串

长度限制：最小长度为 0。最大长度为 25。

模式：`^[\s0-9()+-]+$`

必需：是

Title

为备用联系人指定头衔。

类型：字符串

长度限制：最小长度为 0。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。

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

操作失败，因为主叫身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerException

由于内部存在错误，操作失败AWS。请稍后重试您的操作。

HTTP 状态代码：500

TooManyRequestsException

该操作失败，因为调用频率过高且超过了油门限制。

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

示例

示例 1

以下示例为使用其凭据调用操作的账户设置账单备用联系人。

示例请求

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

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

示例响应

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

示例 2

以下示例设置或覆盖组织中指定成员账户的账单备用联系人。您必须使用来自组织管理账户或账户管理服务的委托管理员账户的证书。

示例请求

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

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

示例响应

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

另请参阅

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

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

PutContactInformation

更新的主要联系人信息AWS 账户。

有关如何使用主要联系人操作的完整详细信息，请参阅更新主要联系人和备用联系人信息。

请求语法

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

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

URI 请求参数

该请求不使用任何 URI 参数。

请求正文

请求接受采用 JSON 格式的以下数据。

AccountId

指定您要通过此操作访问或修改AWS 账户的 12 位帐户 ID 号。如果未指定此参数，则默认为用于调用操作AWS 账户的标识的。要使用此参数，来电者必须是组织管理账户中的身份或委派的管理

员账户。指定的账户 ID 还必须是同一组织中的成员账户。组织必须启用所有功能，组织必须为账户管理服务启用可信访问权限，并可选择分配委派管理员帐户。

> **Note**
>
> 管理账户无法指定自己的账户AccountId。它必须不包括AccountId参数，从而在独立上下文中调用该操作。

要对不是组织成员的账户调用此操作，请不要指定此参数。相反，请使用属于您想要检索或修改其联系人的账户的身份进行操作。

类型：字符串

模式：^\d{12}$

必需：否

ContactInformation

包含与相关的主要联系人信息的详细信息AWS 账户。

类型：ContactInformation 对象

必需：是

响应语法

```
HTTP/1.1 200
```

响应元素

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

错误

有关所有操作返回的常见错误的信息，请参阅常见错误。

AccessDeniedException

操作失败，因为主叫身份没有所需的最低权限。

HTTP 状态代码：403

InternalServerException

由于内部错误，操作失败AWS。请稍后重试您的操作。

HTTP 状态代码：500

TooManyRequestsException

该操作失败，因为调用频率过高且超过了油门限制。

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

另请参阅

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

- AWS 命令行界面
- 适用于 .NET 的 AWS SDK
- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- AWS JavaScript V3 版软件开发工具包
- 适用于 PHP V3 的 AWS SDK
- 适用于 Python 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

其他中的相关操作AWS服务

以下操作与相关：AWS Account Management但是是是是的一部分AWS Organizations命名空间:

- CreateAccount

- 创建 GovCloud账户
- DescribeAccount

CreateAccount

这些区域有：`CreateAccount`API 操作仅在由AWS 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AWS OrganizationsAPI 参考.

创建 GovCloud账户

这些区域有：`CreateGovCloudAccount`API 操作仅可在由AWS 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AWS OrganizationsAPI 参考.

DescribeAccount

这些区域有：`DescribeAccount`API 操作仅在由AWS 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AWS OrganizationsAPI 参考.

数据类型

支持以下数据类型：

- AlternateContact
- ContactInformation
- Region
- ValidationExceptionField

AlternateContact

包含与AWS账户关联的备用联系人详细信息的结构

目录

AlternateContactType

备用联系人的类型。

类型：字符串

有效值：`BILLING | OPERATIONS | SECURITY`

必需：否

EmailAddress

与该备用联系人关联的电子邮件地址。

类型：字符串

长度限制：最小长度为 1。最大长度为 64。

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

必需：否

Name

与该备用联系人相关的姓名。

类型：字符串

长度限制：最小长度为 1。最大长度为 64。

必需：否

PhoneNumber

与备用联系人关联的电话号码。

类型：字符串

长度限制：最小长度为 1。长度上限为 25。

模式：^[\s0-9()+-]+$

必需：否

Title

与该备用联系人相关的职务。

类型：字符串

长度限制：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 AWS 软件开发工具包中使用此 API 的更多信息，请参阅以下内容：

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ContactInformation

包含与相关的主要联系人信息的详细信息AWS 账户。

内容

AddressLine1

主要联系人地址的第一行。

类型：字符串

长度限制：长度下限为 1。最大长度为 60。

必需：是

City

主要联系人地址所在的城市。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：是

CountryCode

主要联系地址的 ISO-3166 双字母国家/地区代码。

类型：字符串

长度限制：固定长度为 2。

必需：是

FullName

主要联系人地址的全名。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：是

PhoneNumber

主要联系人信息的电话号码。该号码将经过验证，并在某些国家/地区进行激活检查。

类型：字符串

长度限制：长度下限为 1。最大长度为 20。

模式：`^[+][\s0-9()-]+$`

必需：是

PostalCode

主要联系地址的邮政编码。

类型：字符串

长度限制：长度下限为 1。最大长度为 20。

必需：是

AddressLine2

主要联系人地址的第二行（如果有）。

类型：字符串

长度限制：长度下限为 1。最大长度为 60。

必需：否

AddressLine3

主要联系人地址的第三行（如果有）。

类型：字符串

长度限制：长度下限为 1。最大长度为 60。

必需：否

CompanyName

与主要联系人信息关联的公司名称（如果有）。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：否

DistrictOrCounty

主要联系地址的地区或县（如果有）。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：否

StateOrRegion

主要联系人地址的州或地区。如果邮寄地址位于美国 (US) 境内，则此字段中的值可以是两个字符的州代码（例如NJ），也可以是州全名（例如New Jersey）。以下国家/地区必须填写此字段：USCA、GB、DE、JP、IN、和BR。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：否

WebsiteUrl

与主要联系信息关联的网站网址（如果有）。

类型：字符串

长度约束：最小长度为 1。长度上限为 256。

必需：否

另请参阅

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

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK

- 适用于 Ruby V3 的 AWS SDK

Region

这种结构表示给定账户的区域，由名称和选择加入状态组成。

内容

RegionName

给定区域的区域代码（例如，us-east-1）。

类型：字符串

长度限制：长度下限为 1。最大长度为 50。

必需：否

RegionOptStatus

区域可能处于的潜在状态之一（启用、启用、已禁用、禁用、启用_By_Default）。

类型：字符串

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

必需：否

另请参阅

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

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

ValidationExceptionField

输入未能满足AWS服务在指定字段中指定的限制。

目录

message

关于验证异常的消息。

类型：字符串

必需：是

name

检测到无效条目的字段名称。

类型：字符串

必需：是

另请参阅

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

- 适用于 C++ 的 AWS SDK
- 适用于 Go 的 AWS SDK
- 适用于 Java V2 的 AWS SDK
- 适用于 Ruby V3 的 AWS SDK

常见参数

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

Action

要执行的操作。

类型：字符串。

必需：是

Version

编写请求所针对的 API 版本，格式为 YYYY-MM-DD。

类型：字符串。

必需：是

X-Amz-Algorithm

您用于创建请求签名的哈希算法。

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

类型：字符串

有效值：AWS4-HMAC-SHA256

必需：条件

X-Amz-Credential

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

有关更多信息，请参阅《IAM 用户指南》中的创建已签名的 AWS API 请求。

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

类型：字符串

必需：条件

X-Amz-Date

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

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

类型：字符串

必需：条件

X-Amz-Security-Token

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

条件：如果您使用来自 AWS STS 的临时安全凭证，则必须包含安全令牌。

类型：字符串

必需：条件

X-Amz-Signature

指定从要签名的字符串和派生的签名密钥计算的十六进制编码签名。

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

类型：字符串

必需：条件

X-Amz-SignedHeaders

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

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

类型：字符串

必需：条件

常见错误

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

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

HTTP 状态代码：400

IncompleteSignature

请求签名不符合 AWS 标准。

HTTP 状态代码：400

InternalFailure

由于未知错误、异常或故障，请求处理失败。

HTTP 状态代码：500

InvalidAction

所请求的操作无效。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 AWS 访问密钥 ID。

HTTP 状态代码：403

NotAuthorized

您无权执行此操作。

HTTP 状态代码：400

OptInRequired

AWS 访问密钥 ID 需要订阅服务。

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 AWS 服务指定的约束。

HTTP 状态代码：400

通过提出 HTTP 查询请求来调用 API

本节包含有关使用查询 API 的一般信息AWS账户管理。有关 API 操作和错误的详细信息，请参阅 API 引用。

> **Note**
>
> 而不是直接打电话给AWS账户管理查询 API，您可以使用其中一个AWS软件开发工具包。AWS 开发工具包中包含适用于各种编程语言和平台（Java、Ruby、.NET、iOS、Android 等）的库和示例代码。SDK 提供了一种创建编程访问权限的便捷方式AWS账户管理和AWS。例如，开发工具包执行以下类似任务：加密签署请求、管理错误以及自动重试请求。有关 AWS 开发工具包的信息（包括如何下载及安装），请参阅适用于 Amazon Web Services 的工具。

使用查询 APIAWS账户管理，您可以调用服务操作。查询 API 请求是 HTTPS 请求，必须包含`Action`用于指示要执行的操作的参数。AWS账户管理支持`GET`和`POST`请求所有操作。也就是说，API 不需要你使用`GET`用于某些操作和`POST`为了其他人。但是，`GET`请求受到 URL 大小限制的约束。尽管此限制取决于浏览器，但典型限制为 2,048 字节。因此，对于需要更大尺寸的查询 API 请求，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 引用中的各个操作页面。

主题

- 端点
- 必须使用 HTTPS

- 签署AWS账户管理 API 请求

端点

AWS账户管理有一个托管在美国东部（弗吉尼亚北部）的单一全球 API 终端节点AWS 区域。

有关以下内容的更多信息AWS所有服务的终端节点和区域，请参阅区域和终端节点在AWS 一般参考。

必须使用 HTTPS

由于查询 API 可以返回安全证书等敏感信息，因此必须使用 HTTPS 加密所有 API 请求。

签署AWS账户管理 API 请求

必须使用访问密钥 ID 和秘密访问密钥签署请求。我们强烈建议您不要使用您的AWS用于日常工作的根账户证书AWS账户管理。您可以将凭证用于AWS Identity and Access Management(IAM) 用户或临时证书，例如您在 IAM 角色中使用的证书。

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

有关更多信息，请参阅下列内容：

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

AWS Account Management 的配额

对于每项 AWS 服务，您的 AWS 账户都具有默认配额（以前称为限制）。除非另有说明，否则每个配额都是AWS 区域特定的。

每个AWS 账户都有以下与账户管理相关的配额。

资源	配额
一个中的备用联系人数 AWS 账户	3-BILLING、和SECURITY、各一个OPERATIONS
每个账户的并发区域选项请求数	6
每个组织的并发区域选择请求数	20
每个账户的DeleteAlternateContact 请求率	每秒 1 个，突发到每秒 6 个
每个账户的DisableRegion 请求率	每秒 1 个，突发到每秒 1 个
每个账户的EnableRegion 请求率	每秒 1 个，突发到每秒 1 个
每个账户的GetAlternateContact 请求率	每秒 10 个，突发到每秒 15 个
每个账户的GetContactInformation 请求率	每秒 10 个，突发到每秒 15 个
每个账户的GetRegionOptStatus 请求率	每秒 5 个，爆发到每秒 5 个
每个账户的ListRegions 请求率	每秒 5 个，爆发到每秒 5 个
每个账户的PutAlternateContact 请求率	每秒 5 个，爆发到每秒 8 个
每个账户的PutContactInformation 请求率	每秒 5 个，爆发到每秒 8 个

为您排查故障 AWS 账户

使用以下主题中的信息来帮助您诊断和修复您的问题AWS 账户。有关根用户的帮助，请参阅 IAM 用户指南中的根用户问题疑难解答。有关登录过程的帮助，请参阅《登录用户指南》AWS中的AWS 账户登录问题疑难解答。

故障排除主题

- 对AWS 账户创建问题进行故障排除
- 对 AWS 账户 关闭问题进行故障排除
- 排查其他相关问题AWS 账户

对AWS 账户创建问题进行故障排除

使用此处的信息有助于排查与创建 AWS 账户 相关的问题。如果您在新账户创建后在登录账户时遇到任何问题，请参阅《登录指南》AWS中的AWS 账户登录问题疑难解答。

问题

- 我没有接到 AWS 验证新账户的电话
- 当我尝试通过电话验证自己的 AWS 账户 时，我收到关于“最大失败尝试次数”的错误
- 已经过去 24 小时，但我的账户还没有激活

我没有接到 AWS 验证新账户的电话

创建时AWS 账户，必须提供一个可以接收 SMS 消息或语音呼叫的电话号码。您可以指定使用哪种方法来验证此电话号码。

如果您没有收到短信或来电，请验证以下内容：

- 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。
- 如果您使用的是手机，请确保您有手机信号可以接收 SMS 消息或电话。
- 您为付款方式输入的信息正确无误。

如果您没有收到短信或电话要求您完成身份验证流程，AWS Support可以帮助您AWS 账户手动激活。使用以下步骤：

1. 请确保可通过您为 AWS 账户 提供的电话号码与您取得联系。
2. 打开 AWS Support 控制台，然后选择创建案例。
   a. 选择账户和账单支持。
   b. 在类型中，选择账户。
   c. 在类别中，选择激活。
   d. 在案例描述部分，提供可以联系您的日期和时间。
   e. 在联系人选项部分，选择聊天以获取联系方式。
   f. 选择提交。

> **Note**
>
> AWS Support即使您的手机AWS 账户尚未激活，您也可以创建案例。

当我尝试通过电话验证自己的 AWS 账户 时，我收到关于“最大失败尝试次数”的错误

AWS Support 可以帮助您手动激活账户。按照以下步骤进行操作：

1. 使用您在创建账户时指定的电子邮件地址和密码登录您的 AWS 账户。
2. 打开 AWS Support 控制台，然后选择创建案例。
3. 选择账户和账单支持。
4. 在类型中，选择账户。
5. 在类别中，选择激活。
6. 在案例描述部分，提供可以联系您的日期和时间。
7. 在联系人选项部分，选择聊天以获取联系方式。
8. 选择提交。

AWS Support 将与您联系并尝试手动激活您的 AWS 账户。

已经过去 24 小时，但我的账户还没有激活

账户激活有时可能会延迟。如果该过程耗时超过 24 小时，请检查以下内容：

- 完成账户激活过程。

  如果您在添加所有必要信息之前关闭注册过程窗口，请打开注册页面。选择登录现有 AWS 账户，然后使用您为账户选择的电子邮件地址和密码登录。

- 查看与您的付款方式关联的信息。

  在 AWS Billing and Cost Management 控制台中，检查付款方式是否有错误。

- 联系您的金融机构。

  有时，金融机构会拒绝来自 AWS 的授权请求。联系与您的付款方式关联的机构，并要求他们批准来自 AWS 的授权请求。 一旦您的金融机构批准授权请求，AWS 就会立即将其取消，因此您无需为授权请求付费。授权请求可能仍会以少量费用（通常为 1 USD）的形式出现在金融机构的对账单上。

- 请检查您的电子邮件和垃圾邮件文件夹，以获取请求的更多信息。
- 尝试使用其他浏览器。
- 联系 AWS Support。

  联系 AWS Support 寻求帮助。提及您已经尝试过的所有问题排查步骤。

> **Note**
>
> 请勿在与 AWS 的任何通信中提供敏感信息，例如信用卡号。

对 AWS 账户 关闭问题进行故障排除

使用以下信息来帮助您诊断和修复账户关闭过程中发现的常见问题。有关账户关闭流程的一般信息，请参阅关闭一个 AWS 账户。

主题

- 我不知道如何删除或取消我的账户
- 我在 “账户” 页面上看不到 “关闭账户” 按钮
- 我关闭了账户，但仍未收到确认电子邮件
- 我在尝试关闭账户时收到 ConstraintViolationException “” 错误
- 我在尝试关闭会员账户时收到 “CLOSE_ACCOUT_QUOTA_UCKEDED” 错误
- 在关闭管理账户之前，我需要删除我的 AWS 组织吗？

我不知道如何删除或取消我的账户

要关闭您的账户，请按照中的说明进行操作关闭一个 AWS 账户。

我在 “账户” 页面上看不到 “关闭账户” 按钮

如果您未以 root 用户身份登录，则账户页面上不会显示关闭账户按钮。您必须以 root 用户身份登录才能关闭您的账户。 AWS Management Console 如果您无法登录，请参阅根用户问题疑难解答。

我关闭了账户，但仍未收到确认电子邮件

此确认电子邮件仅发送到的根用户电子邮件地址 AWS 账户。如果您在几个小时内没有收到此电子邮件，则可以以 root 用户 AWS Management Console 身份登录，以检查您的账户是否已关闭。如果您的账户已成功关闭，您将看到一条消息，表明您的账户已关闭。如果您关闭的账户是成员账户，则可以通过检查已关闭的账户是否在 AWS Organizations 控制台SUSPENDED中标记为来验证成功关闭。有关更多信息，请参阅《AWS Organizations 用户指南》中的关闭组织中的成员账户。

如果您正在尝试关闭管理账户，但没有收到有关账户关闭的确认电子邮件，则您的组织很可能拥有活跃的成员账户。只有当你的组织没有任何活跃的成员账户时，你才能关闭管理账户。要验证您的组织中是否没有活跃的成员账户，请转到 AWS Organizations 控制台，并确保所有成员账户都显示在其账户名称Suspended旁边。之后，您可以关闭管理账户。

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

您正在尝试使用 AWS Organizations 控制台关闭管理账户，但这是不可能的。要关闭管理账户，您需要以管理账户的 root 用户身份登录，然后从 “账户” 页面将其关闭。 AWS Management Console 有关更多信息，请参阅《AWS Organizations 用户指南》中的关闭组织中的管理账户。

我在尝试关闭会员账户时收到 “CLOSE_ACCOUT_QUOTA_UCKEDED” 错误

在连续 30 天的周期内，您只能关闭 10% 的成员账户。此限额不受日历月的限制，而是在您关闭账户时开始。在首次关闭账户后的 30 天内，您不能超过 10% 的账户关闭限额。即使有 10% 的账户超过 1000 个，账户关闭的最低限度为 10 个，最大账户关闭量为 1000 个。有关 Organizations 配额的更多信息，请参阅AWS Organizations 用户指南 AWS Organizations中的配额。

在关闭管理账户之前，我需要删除我的 AWS 组织吗？

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

排查其他相关问题AWS 账户

使用此处的信息可帮助您排查与您的AWS 账户.

问题

- 我需要变更我的信用卡AWS 账户
- 我需要举报账户欺诈活动AWS 账户活动
- 我需要关闭我的AWS 账户

我需要变更我的信用卡AWS 账户

要变更您的信用卡AWS 账户，您必须能够登录。AWS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AWS Billing用户指南.

我需要举报账户欺诈活动AWS 账户活动

如果你怀疑使用你的欺诈活动AWS 账户并且想做一份报告，请参阅我该如何举报滥用AWS资源.

如果您在 Amazon.com 上购买商品时遇到问题，请参阅亚马逊客户服务.

我需要关闭我的AWS 账户

有关帮助解决关闭AWS 账户，请参阅关闭一个 AWS 账户.

账户管理用户指南的文档历史记录

下表描述了AWS账户管理的文档版本。

变更	说明	日期
重写关闭账户的话题	彻底改革了整个关闭账户的主题，包括添加了如何关闭成员和管理账户的步骤。	2024年2月1日
不再支持添加新的安全挑战问题	添加了新内容，指出添加新挑战题的选项已从 “帐户” 页面中删除。	2024 年 1 月 5 日
终止对`aws-portal` 命名空间的支持	AWS Identity and Access Management之前用于管理您的账户的 (IAM) 操作（例如`aws-portal:ModifyAccount` 和`aws-portal:ViewAccount` ）已终止标准支持。	2024 年 1 月 1 日
重写 “区域” 主题	彻底改革了整个 “区域” 主题，包括添加展开和折叠控件。	2023 年 10 月 8 日
将根用户主题重新定位到 IAM 用户指南中	将有关根用户的讨论整合到一个主题中，添加了指向已移至 IAM 用户指南的根用户主题的交叉引用链接。	2023 年 9 月 18 日
主账户联系人主题中添加了新版块	添加了新的电话号码和电子邮件地址要求部分。	2023 年 9 月 12 日
新的联系人信息 API	对新功能`GetContactInformation` 和`PutContactInformation` API 的支持。	2022 年 7 月 22 日

AWS账户管理现在支持通过AWS Organizations控制台更新备用联系人。	现在，您可以使用更新的AWS Organizations托管政策提供的账户 API 权限，通过AWS Organizations控制台更新组织的备用联系人。	2022 年 2 月 8 日
初始版本	《AWS账户管理参考指南》的首次发布	2021 年 9 月 30 日

AWS 术语表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 词汇表。

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。