

Amazon 账户管理



Amazon 账户管理: 用户指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

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

Table of Contents

什么是 Amazon Web Services 账户？	1
的特点 Amazon Web Services 账户	2
你是第一次吗 Amazon 用户？	3
支持和反馈	3
其他 Amazon 资源	4
比较注册选项	5
支持 Amazon Web Services 服务 for 注册 Amazon（新）	5
Amazon Web Services 服务 包含在我们新的免费套餐中 Amazon 经历	5
Amazon Web Services 服务 包含在我们新的付费计划中 Amazon 经历	10
Amazon Web Services 服务 不支持我们的新品 Amazon 经历	12
选择如何注册的注意事项 Amazon	16
比较注册选项的功能	17
比较访问管理	18
管理你的 Amazon Web Services 账户	20
报名参加 Amazon（新）	23
使用注册进行注册 Amazon（新）	25
后续步骤	26
使用 Amazon 设置	26
连接 AI 编码工具	27
将编码工具连接到项目的注意事项	27
将您的 AI 编码工具连接到您的项目	28
处理多个项目	29
Amazon 项目所有者的操作	31
更新你的密码	32
管理多重身份验证（MFA）	33
关键点	33
我们新推出的可用的 MFA 类型 Amazon 经历	33
注册 MFA 设备	35
将安全密钥注册为您的 MFA 设备	36
重命名 MFA 设备	37
删除 MFA 设备	37
删除所有会话	38
管理你的名字或昵称	38
更改您的电子邮件地址	39

编辑您的联系信息	40
选择不使用您的内容来改善服务	40
索取您的 Amazon 建筑商 ID 数据	41
创建项目	42
创建项目的注意事项	42
创建项目	43
Amazon Web Services 区域 为了你的项目	43
找到选定的 Amazon Web Services 区域 为了你的项目	44
在美国东部（俄亥俄州）（us-east - 2）提供区域资源的国家	45
在亚太地区（悉尼）（ap-southeast-2）提供区域资源的国家	47
在欧洲提供区域资源的国家（斯德哥尔摩）（eu-north-1）	51
为您的组织提供托管政策	57
项目的服务控制策略	58
项目免费套餐的服务控制策略	79
项目付费计划的服务控制政策	90
项目的资源控制政策	101
在项目之间切换	104
在项目之间切换以获取活动会话 Amazon Web Services 管理控制台	104
在项目之间切换 Amazon 设置	104
在项目之间切换 Amazon Web Services 管理控制台	104
邀请团队成员	105
团队成员注意事项	105
团队成员如何访问您的 Amazon 资源	106
邀请团队成员	107
邀请团队成员加入项目	107
从项目中移除团队成员	108
移除团队成员	109
撤销邀请	109
重新发送邀请	110
升级您的账户	110
升级账户的注意事项	110
升级您的账户	111
创建支出限额	111
什么是支出限额？	112
设置您的支出限额	112
通知	113

使用可选的早期费用控制来自定义您的支出限额设置	113
如果你达到极限会发生什么	114
其他需要注意的重要事项	114
在中创建支出限额 Amazon 设置	115
更新支出限额	115
在中更新支出限额 Amazon 设置	115
移除支出限额	116
移除中的支出限额 Amazon 设置	116
免费套餐	116
跟踪您的免费套餐使用情况	117
赚取额外积分	118
在中查看您的账单信息 Amazon 设置	119
按项目查看成本	119
在中查看您的账单历史记录 Amazon 设置	120
管理您的付款方式	120
在其中付款 Amazon 设置	121
将您的首选货币更改为 Amazon 设置	121
在中管理税务登记 Amazon 设置	122
更新和删除税务登记号码	122
管理美国免税	123
查看和兑换积分	123
管理印度地区的账户	124
报名参加 Amazon (新) 有 Amazon 印度	125
管理您的客户验证信息	126
设置您的印度账单	129
添加或编辑永久账号	129
编辑多个永久账号	129
编辑多个商品和服务税识别号	130
查看税务发票	130
将登记在册的卖家更改为或更改卖家 Amazon 印度	131
访问 Supp Amazon ort	132
项目支持	132
技术支持	133
如果您的所有项目和组织都已关闭，则为 Support	133
开始试用“商业支持+”	134
监控您的项目	134

使用监控您的项目 Amazon CloudTrail	135
用于 CloudTrail 查看谁修改了您的项目	135
关闭项目	137
在关闭项目之前你需要知道什么	138
关闭项目	138
Post-closure 时期	139
重新打开你的项目	139
激活高级功能	139
激活高级功能后会发生什么	139
怎么会 Amazon 我激活高级功能后设置会发生变化吗？	141
我还能在里面创建一个项目吗 Amazon 激活高级功能后的设置？	142
如何准备激活高级功能	142
如何激活高级功能	143
激活高级功能后	143
设置 root 用户密码	144
管理员工队伍	145
更改身份来源	146
移除组织政策	147
在 Amazon “设置” 中关闭您的账户	149
关闭管理账户之前需要了解的内容	149
关闭项目	150
关闭您的管理账户	150
删除你的 Amazon Builder ID	150
注册 Amazon （高级）	152
步骤 1：创建账户	152
步骤 2：（推荐）安装 Amazon CLI	154
步骤 3：（推荐）设置 Amazon MCP 服务器	155
相关 Amazon 务	155
使用根用户	156
访问您的 账户	157
规划您的 治理结构	158
使用多个的好处 Amazon Web Services 账户	158
何时使用 Amazon Organizations	160
何时使用 Amazon Control Tower	163
了解 API 的操作模式	164
配置您的账户	166

创建或更新您的账户别名	167
启用或禁用 Amazon Web Services 区域 在你的账户中	167
更新您的账单 Amazon Web Services 账户	177
更新Amazon Web Services 电子邮件	177
更新根用户密码	182
更新你的 Amazon Web Services 账户 name	183
更新您的备用联系人 Amazon Web Services 账户	186
更新您的主要联系人 Amazon Web Services 账户	194
查看账户标识符	200
排查账户故障	205
账户创建问题	205
账户关闭问题	206
其它问题	208
管理印度地区的账户	209
创建一个 Amazon Web Services 账户 用 Amazon 印度	209
管理您的客户验证信息	211
关闭您的账户	215
关闭账户前的注意事项	215
如何关闭您的账户	217
账户关闭后会发生什么	220
重新打开您的账户	221
在重新开设账户之前你需要知道什么	221
如何重新开设账户	221
重新开设账户后会发生什么	222
准备好账户以备重新开户后使用	222
区域可用性	222
保护您的账户	223
数据保护	223
Amazon PrivateLink	224
创建端点	225
Amazon VPC 端点策略	225
端点策略	225
身份和访问管理	226
受众	227
使用身份进行身份验证	227
使用策略管理访问	228

Amazon 账户管理和 IAM	229
Identity-based 策略示例	236
使用基于身份的策略	239
问题排查	241
Amazon 托管策略	243
AWSAccountManagementReadOnlyAccess	243
AWSAccountManagementFullAccess	244
策略更新	245
合规性验证	246
恢复能力	246
基础结构安全性	247
监控您的账户	248
CloudTrail 日志	248
中的账户管理信息 CloudTrail	248
了解账户管理日志条目	249
使用以下方式监控账户管理事件 EventBridge	253
账户管理事件	253
配额	256
文档历史记录	258
.....	cclx

什么是 Amazon Web Services 账户？

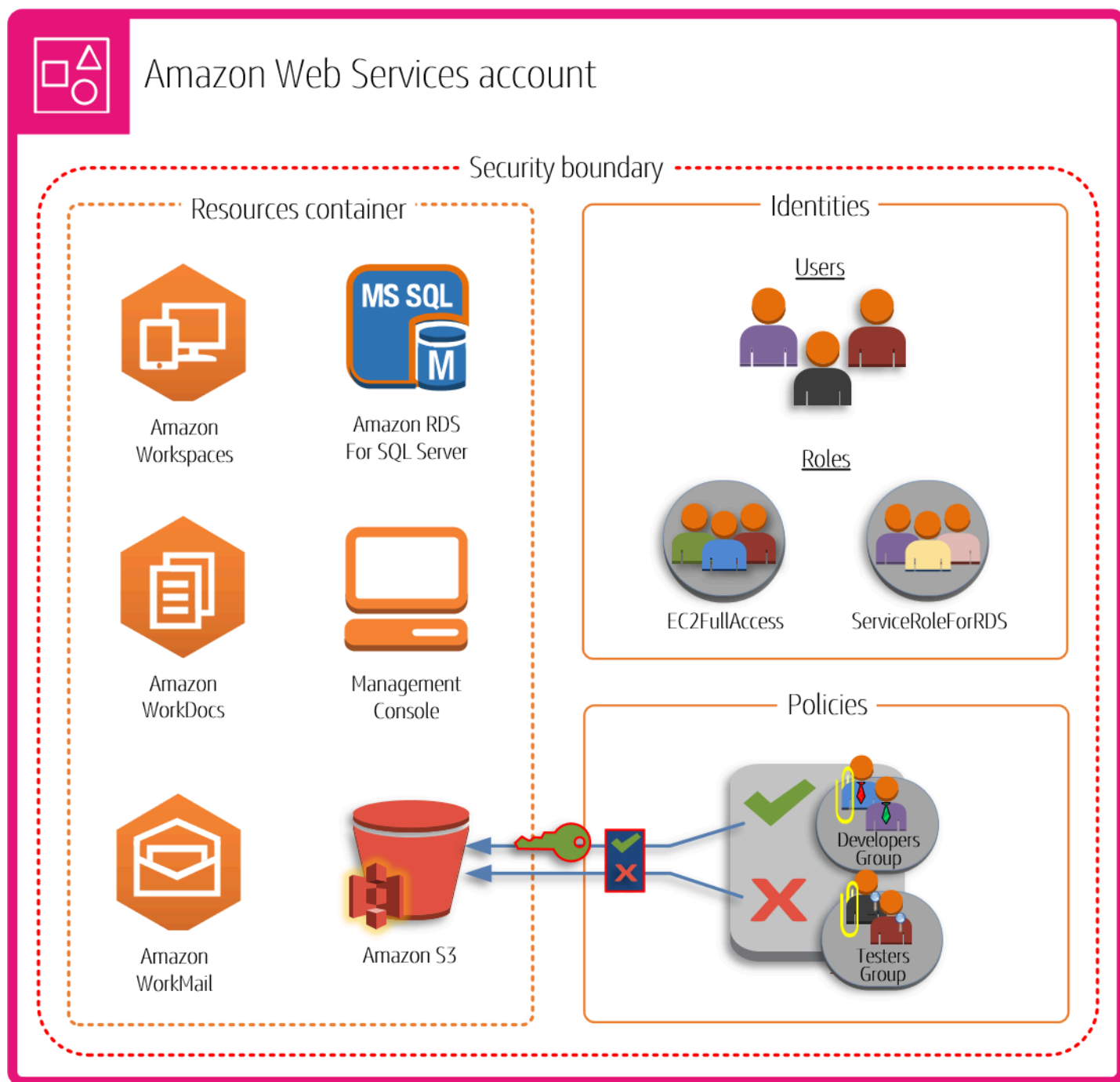
Amazon Web Services 账户 代表您与之建立的正式业务关系 Amazon。您可以在中创建和管理您的 Amazon 资源 Amazon Web Services 账户，并且您的账户提供访问和计费的身份管理功能。每个 Amazon Web Services 账户 都有唯一的 ID，这使它与其他 Amazon Web Services 账户人区分开来。

注册时 Amazon，可以在注册 Amazon（新）和注册（高级）之间进行 Amazon 选择。根据您的选择，您可以访问 Amazon Web Services 账户 或项目。项目包含 Amazon Web Services 账户 与其他合作者共享的设置。有关更多信息，请参阅 [比较注册选项](#)。

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

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

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



使用多重 Amazon Web Services 账户 是扩展环境的最佳做法，因为它为成本提供了自然的计费界限，隔离了资源以保证安全，为个人和团队提供了灵活性，并且可以适应新的业务流程。有关更多信息，请参阅 [使用多个的好处 Amazon Web Services 账户](#)。

的特点 Amazon Web Services 账户

Amazon Web Services 账户 包括以下核心功能：

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

你是第一次吗 Amazon 用户？

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

如果您是的首次用户 Amazon，则第一步是注册。Amazon 您可以创建一个 Amazon Web Services 账户，您可以完全控制账户配置和内容存储位置，这是 HIPAA 或 FedRAMP 等受监管工作负载所必需的，也可以使用预先配置的默认值进行创建 Amazon Web Services 账户。要了解哪种注册最适合您，请参阅[比较注册选项](#)。

有关如何设置一个可以完全控制初始设置的新账户的分步说明，请参阅[报名参加 Amazon（高级）](#)。

有关如何设置新账户并使用预先配置的默认值 Amazon 创建账户的分步说明，请参阅[报名参加 Amazon（新）](#)。

对该项的支持 Amazon 账户管理

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

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

其他 Amazon 资源

- [Amazon 培训和课程](#) — 指向基于角色的课程和专业课程以及自定进度的实验室的链接，可帮助您提高 Amazon 技能并获得实践经验。
- [Amazon 开发者工具](#) — 指向开发者工具和资源的链接，这些工具和资源提供文档、代码示例、发行说明和其他信息，可帮助您构建创新应用程序 Amazon。
- [Amazon Web Services 支持 中心](#) — 用于创建和管理 Support Amazon 案例的中心。还包括指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况和 Amazon Trusted Advisor。
- [Amazon Support](#) — [有关 Amazon Support 信息的主要网页，这是一个一对一的快速响应支持渠道，可帮助您在云中构建和运行应用程序。](#)
- [联系我们](#) — 查询 Amazon 账单、账户、事件、滥用行为和其他问题的中央联络点。
- [Amazon 网站条款](#) — 有关我们的版权和商标、您的帐户、许可证和网站访问权限以及其他主题的详细信息。

比较注册选项

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

注册后 Amazon，即可解锁世界上最全面、采用最广泛的云。我们在最广泛的全球基础设施上提供创新的云和 AI 功能和专业知识的最佳选择，具有行业领先的安全性、可靠性和性能。

有两种注册方式 Amazon。如果您想完全控制账户配置和内容存储位置，或者您有受监管的工作负载（例如 HIPAA、FedRAMP），请使用 [报名参加 Amazon（高级）](#)。如果您是新用户，并且想要使用您已经拥有的登录名登录 Amazon 并在 select 中创建具有预配置默认值的 Amazon 环境 [Amazon Web Services 区域](#)，请使用 [报名参加 Amazon（新）](#)。

支持 Amazon Web Services 服务 for 注册 Amazon（新）

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

当您使用“注册 Amazon（新）”时，您可以访问免费套餐。免费套餐提供对特定 Amazon 服务的访问权限。您可以将您的账户升级到付费套餐以使用其他 Amazon 服务和功能。要了解如何升级您的账户，请参阅[在中升级您的账户 Amazon 设置](#)。

并非所有 Amazon 服务都可用于注册 Amazon（新）。如果某项服务未在以下列表中列出或其功能不受支持，则必须使用[报名参加 Amazon（高级）](#)或[激活高级 Amazon 功能](#)创建帐户。

Amazon Web Services 服务 包含在我们新的免费套餐中 Amazon 经历

免费注册 Amazon（新）套餐中包含以下 Amazon 服务。Multi-Region 或任何服务都不支持跨区域功能。有关更多信息，请参阅 [Amazon Web Services 区域 为了你的项目](#)。

- Amazon API Gateway
- Amazon Athena

- Amazon AppFlow
- Amazon App2Container
- Amazon Augmented AI
- Amazon Bedrock
- Amazon 基岩代理核心
- Amazon CloudFront
 - 不支持 Lambda @Edge。
- Amazon CloudWatch
- Amazon CloudWatch 日志
- Amazon P CodeGuru profiler
- Amazon Cognito
- Amazon Cognito Sync
- Amazon DynamoDB
- Amazon DataZone
- Amazon Elastic Container Registry (ECR)
- EC2 Image Builder
- Amazon EKS Anywhere
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
 - 不支持“购买容量块”和“购买容量区块扩展”。
- Amazon Elastic Container Registry Public
- Amazon Elastic Container Service
- Amazon Elastic Kubernetes Service
- Amazon Elastic File System
- Amazon ElastiCache
- Amazon EventBridge
- Amazon Lex
- Amazon Lightsail
- Amazon Location Service

- Amazon Managed Service for Prometheus
- Amazon Managed Workflows for Apache Airflow
- Amazon MQ
- 亚马逊 OpenSearch 服务
- Amazon Polly
- Amazon Quick
 - 仅支持 Amazon Quick Free 或 Quick Plus。有关更多信息，请参阅 [Amazon 快速定价](#)。
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon Route 53
- Amazon SageMaker
- 亚马逊 SageMaker AI
- 亚马逊 SageMaker 联合工作室
- Amazon Simple Email Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service
 - 不支持 Amazon S3 访问授权。
- Amazon Simple Workflow Service
- Amazon Verified Permissions
- Amazon Virtual Private Cloud
- Amazon Aurora
- Amazon Aurora DSQL
- Amazon Amplify
- Amazon AppConfig
- Amazon AppSync
- Application Auto Scaling
- Amazon Transform MGN
- Amazon Artifact

- 不支持 (HIPAA) Amazon 商业伙伴附录、(HIPAA) Amazon Organizations Business Associate 附录 Amazon 、美国证券交易委员会规则 17a-4 附录 Amazon 和美国证券交易委员会规则 18a-6 附录。
- Amazon B2B Data Interchange
- Amazon Backint 代理
- Amazon Backup
- Amazon Batch
- Amazon 账单与成本管理
 - 使用 Amazon “设置” 设置账单，创建支出限额以控制费用，以及检索和支付发票。您可以使用 Billing and Cost Management 来创建预算、分析和优化成本。如需了解更多信息，请参阅[使用账单和成本管理控制台，体验我们的全新 Amazon 体验](#)。
- Amazon Budgets
- Amazon Certificate Manager
 - Amazon 不支持 [Certific Manager 可导出的公共证书](#)。
- Amazon 云端控制 API
- Amazon Cloud Map
- Amazon Cloud9
- Amazon CloudFormation
- Amazon CloudShell
- Amazon CloudTrail
- Amazon CodeArtifact
- Amazon CodeCommit
- Amazon CodeDeploy
- Amazon CodePipeline
- Amazon Compute Optimizer
- Amazon Config
- Amazon Console Mobile Application
- Amazon Cost Explorer
- Amazon Data Pipeline
- Amazon 数据传输

- Amazon DataSync
- Amazon Directory Service
- Amazon Elastic Beanstalk
- Amazon 终端用户消息收发社交服务
- Amazon Entity Resolution 数据匹配服务
- Amazon Glue
- Amazon Health
- Amazon Identity and Access Management
- Amazon IoT
 - Amazon 不支持 Greengrass。
- Amazon IoT 设备防御者
- Amazon IoT 设备管理
- Amazon IoT SiteWise
- Amazon IoT TwinMaker
- Amazon Key Management Service
- Amazon Lake Formation
- Amazon Lambda
 - 不支持 Lambda @Edge。
- Amazon Launch Wizard
- Amazon License Manager
- Amazon Web Services 管理控制台
- Amazon Web Services Marketplace
 - 仅限 Bedrock 且免费。
- Amazon Network Manager
- Amazon Payment Cryptography
- Amazon PrivateLink
- Amazon Resource Access Manager (内存)
- Amazon 资源探索器
- Amazon Resource Groups
- Route 53 亚马逊应用程序恢复控制器 (ARC)

- Amazon 软件开发工具包和工具
- Amazon Secrets Manager
- Amazon Security Token Service
- Amazon Serverless Application Repository
- 服务配额
- Amazon Signer
- Amazon Step Functions
- Amazon Web Services 支持
- Amazon Systems Manager
- 适用于 SAP 的 Amazon Systems Manager
- Amazon 用户通知服务
 - User-configured 不支持通知和托管通知配置操作。有关更多信息，请参阅[什么是 Amazon 用户通知？](#)
- Amazon WAF
 - Amazon 不支持 Shield。
- Amazon Well-Architected Tool
- Amazon X-Ray
- Amazon CodeBuild
- Elastic Load Balancing
- Amazon SQL Workbench
- 亚马逊 OpenSearch 服务无服务器
- Amazon Timestream

要查看控制免费套餐服务访问权限的政策，请参阅[项目免费套餐的服务控制策略](#)。

Amazon Web Services 服务 包含在我们新的付费计划中 Amazon 经历

如果您有付费计划，则可以使用以下服务进行注册 Amazon（新）。有关更多信息，请参阅[在中升级您的账户 Amazon 设置](#)。Multi-Region 或任何服务都不支持跨区域功能。有关更多信息，请参阅[Amazon Web Services 区域 为了你的项目](#)。

- Amazon DevOps Guru

- Amazon DocumentDB (兼容 MongoDB)
- Amazon EMR
- Amazon Forecast
- Amazon Glacier
- Amazon Kinesis
- Amazon Kinesis Data Streams
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- Amazon Managed Blockchain
- Amazon Managed Streaming for Apache Kafka
- Amazon MemoryDB
- Amazon Neptune
- Amazon Personalize
- Amazon Redshift
- S3 Glacier Deep Archive
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- Amazon AppFabric
- Amazon Web Services Data Exchange
- Amazon End User Messaging SMS
- Amazon Fault Injection Service
- Amazon Firewall Manager
- Amazon Network Firewall
- Amazon 安全代理
- Amazon Storage Gateway
- DevOps 代理人

要查看控制付费套餐服务访问权限的政策，请参阅[项目付费计划的服务控制政策](#)。

Amazon Web Services 服务 不支持我们的新品 Amazon 经历

除非您，否则我们的新 Amazon 体验不支持以下 Amazon 服务[激活高级 Amazon 功能](#)。对于新开发人员或小型团队来说，这些 Amazon 服务不是必需的。其中一些服务会自动为您的账户开启并由管理 Amazon。有关更多信息，请参阅 [比较注册选项的功能](#)。

- Alexa for Business
- Alexa Top Sites
- Alexa Web Information Service
- Amazon Braket
- Amazon Chime
- Amazon Chime Business Calling 一项由 AMCS LLC 出售的服务
- 亚马逊 Chime 给我打电话
- Amazon Chime Call Me 是一项由 AMCS LLC 出售的服务
- 亚马逊 Chime Dial In 一项由 AMCS LLC 出售的服务
- 亚马逊 Chime Dialin
- 亚马逊 Chime 功能
- Amazon Chime SDK
- 亚马逊 Chime 服务
- 亚马逊 CHIME 短信
- Amazon Chime Voice Connector 是一项由 AMCS LLC 出售的服务
- Amazon Cloud Directory
- Amazon CloudSearch
- Amazon CodeWhisperer
- Amazon Connect Customer
- Amazon Connect Customer Profiles
- Amazon Connect Customer Voice ID
- Amazon Deadline Cloud
- Amazon Detective
- Amazon Elastic Inference
- Amazon Elastic Transcoder

- Amazon FinSpace
- Amazon 灵活舰队
- Amazon Fraud Detector
- Amazon FSx
- 亚马逊 GameLift 服务器
- Amazon GameLift 直播
- Amazon GameSparks
- Amazon GuardDuty
- Amazon HealthOmics
- Amazon Inspector Classic
- Amazon Interactive Video Service
- Amazon IVS 聊天功能
- Amazon Kendra
- Amazon Keyspaces (for Apache Cassandra)
- Kiro
- Amazon Macie
- Amazon Managed Grafana
- Amazon Mechanical Turk
- 亚马逊 Mechanical Turk 员工奖励
- Amazon Mobile Analytics
- Amazon Monitron
- Amazon Nimble Studio
- Amazon OpenSearch 服务摄取服务
- Amazon Q
- Amazon Q 企业版
- Amazon Q 开发者版
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon S3 on Outposts
- 亚马逊 G SageMaker round Truth

- Amazon Security Lake
- Amazon Sumerian
- Amazon WorkDocs
- Amazon WorkSpaces
- 亚马逊 WorkSpaces 实例
- 亚马逊 WorkSpaces 应用程序 (亚马逊 WorkSpaces 应用程序)
- Amazon WorkSpaces 瘦客户机
- Amazon WorkSpaces Web
- Amazon WorkLink
- Amazon WorkMail
- Amazon 应用程序成本分析器
- Amazon Clean Rooms
- Amazon 应用程序工作室
- Amazon Application Discovery Service
- Amazon Audit Manager
- Amazon Billing Conductor
- Amazon CloudHSM
- Amazon Client VPN
- Amazon 云广域网
- Amazon Control Tower
- Amazon 数据库迁移服务
- Amazon DeepRacer
- Amazon Device Farm
- Amazon Direct Connect
- Amazon 弹性灾难恢复
- AWS Elemental Live
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive

- AWS Elemental MediaPackage
- AWS Elemental MediaStore
- AWS Elemental MediaTailor
- Amazon Global Accelerator
- Amazon Ground Station
- Amazon HealthImaging
- Amazon IAM Identity Center
- Amazon Identity and Access Management Access Analyzer
- Amazon 互连
- Amazon IoT 活动
- Amazon IoT FleetWise
- Amazon IoT RoboRunner
- Amazon Mainframe Modernization
- Amazon Migration Hub
- Amazon Migration Hub Refactor Spaces
- Amazon Modular Data Center
- Amazon OpsWorks
- Amazon Organizations
- Amazon Outposts
- Amazon 并行计算服务
- Amazon Partner Network
- Amazon 定价计算器
- Amazon 私有证书颁发机构
- Amazon Proton
- Amazon re:Post 私人版
- Amazon Resilience Hub
- Amazon RoboMaker
- Amazon RTB 面料
- Amazon Security Hub

- Amazon 安全事件响应
- Amazon Service Catalog
- Amazon Shield
- Amazon SimSpace Weaver
- Amazon Snowball
- Amazon Supply Chain
- Amazon Web Services 电信网络构建器
- Amazon Transform
- Amazon Transfer Family
- Amazon Transit Gateway
- Amazon Trusted Advisor
- Amazon Verified Access
- Amazon VPN
- Amazon VPC Lattice
- Amazon Wickr
- Amazon CodeCatalyst
- Amazon Comprehend Medical
- 会议电信 (由 AMCS LLC 出售的服务)
- 联络中心电信 (由 AMCS LLC 出售的服务)
- 韩国电信联络中心
- 南非电信联络中心
- DynamoDB Accelerator
- Amazon Elastic VMware Service
- Oracle Database@Amazon
- Amazon 云端 Red Hat OpenShift 服务
- Amazon App Runner

选择如何注册的注意事项 Amazon

在选择注册方式之前，请考虑以下几点。如有必要，您可以激活账户的所有 Amazon 功能。

- 如果您有特定的产品要求，例如包括 HIPAA 或 FedRAMP 在内的受监管工作负载，请不要使用我们的新体验。Amazon
- 您的内容将存储在根据您的联系信息选择的指定区域。
- 新 Amazon 体验使您无需创建 Amazon 权限即可更轻松地开始构建。如果您需要对用户或基于角色的权限进行精细控制，请不要使用 Sign up for Amazon（新增）。
- 如果您需要由 Amazon 设置的特定于账户的付款配置（也称为净条款计费），请不要使用注册 Amazon（新）。
- 如果您需要访问全套 Amazon 服务，请不要使用 Sign up for Amazon（新）。有关更多信息，请参阅 [支持 Amazon Web Services 服务 for 注册 Amazon（新）](#)。

比较注册选项的功能

下表比较了支持注册 Amazon（新）或注册（高级）的 Amazon Amazon 广泛要求。如果某项功能未在此表中列出或未在中描述[比较访问管理](#)，则该功能可用。如果您需要任何不支持的功能，可以为您的帐户激活高级功能。有关更多信息，请参阅 [激活高级 Amazon 功能](#)。

功能	注册 Amazon（新）	注册 Amazon（高级）
加入 Amazon 合作伙伴网络	否	是
创建专业服务合同	否	是
通过以下方式注册企业协议 Amazon	否	是
购买 Amazon 技能生成器团队订阅	否	是
与 Amazon 培训合作伙伴合作	否	是
通过“Amazon 激活”赚取额外积分	否	是
使用 Amazon 市场	否	是
将您的 Amazon 账户指定为符合 HIPAA 或 SEC 标准的账户	否	是
选择特定资源 Amazon Web Services 区域 来创建您的区域资源	不是。有关更多信息，请参阅 Amazon	是

功能	注册 Amazon（新）	注册 Amazon（高级）
	Web Services 区域 为了你的项目。	
访问可选择加入的区域	否	是
IAM Access Analyzer	否	是
Sign-in 访问策略	否	是
为您的账户设置支出限额	是	否
Savings Plans	否	是
自动选择加入付费 计划的成本优化中心	是	否
自动选择加入 Amazon Organizations	是	否
自动选择加入 IAM 身份中心	是	否
自动选择加入 IAM 角色管理器	是	否
主机账号颜色	否	是
使用 Amazon Console Mobile Application	否	是
禁用多会话控制台支持	否	是。如果您使用生成器 ID 再次登录，则会自动启用多会话支持。

比较访问管理

当您使用我们的新 Amazon 体验时，Amazon 会创建预配置的默认值以帮助您开始构建。您的 Amazon 资源按项目进行组织。项目包含以及用于与其他合作者共享的设置。如果您使用付费计划，则您的项目还可以设定每月的税前成本，称为支出限额。您拥有的所有项目都构成了您的组织，您可以通过 Amazon “设置” 中的管理帐户对其进行控制。该组织与 Amazon 组织相同；但是，Amazon 它代表您管理该组织的各个方面。

Amazon 管理您的 Amazon 组织的以下要素：

- 组织管理政策。当您使用我们的新 Amazon 体验时，Amazon 可以管理组织管理策略，包括资源控制策略 (RCP) 和服务控制策略 (SCP)。如果你想自己创建，请使用“注册 Amazon（高级）”。
- 人类访问角色。人类访问角色是授予人类特定权限的任何角色。Amazon 为您和您的团队成员提供项目管理员访问权限。作为项目所有者，您可以添加和移除团队成员。有关更多信息，请参阅[邀请团队成员进行协作 Amazon 设置](#)。您不创建 root 用户。如有必要，您可以创建 IAM 角色和 IAM 用户，但它们只能用于编程访问，不能用于控制台访问。

每个项目都有托管安全实施，因此可以轻松自信地构建。默认情况下，项目中的任何应用程序或代码都可以访问同一项目中的所有 Amazon 资源。您无需执行其他访问配置。

Amazon 除非您为某些资源开启跨项目访问权限，否则不同项目中的资源无法相互访问。例如，您可以在一个项目中创建 Lambda 函数，然后在另一个项目中使用 API 调用该函数。这被描述为跨账户集成。有关更多信息，请参阅[Cross-account Lambda 集成](#)。只要两个项目都由同一个管理账户拥有，就可以支持这个。

默认情况下，您的项目不提供对任何资源的外部访问权限。您必须配置 Amazon 资源以允许公共访问。您可执行以下操作：

- 创建公有 S3 存储桶来托管一个或多个简单的静态网站。有关更多信息，请参阅[Amazon S3 入门](#)。
- 创建一个 API Gateway API 来充当应用程序的前门。有关更多信息，请参阅[构建 HTTP API](#)。
- 使用公有 IP 地址创建一个 EC2 实例，以允许您的实例与互联网进行通信。有关更多信息，请参阅[启动您的第一个 EC2 实例](#)。
- 创建 CloudFront 发行版，向用户提供静态和动态 Web 内容，例如.html、.css、.js 和图像文件。有关更多信息，请参阅[入门 CloudFront](#)。
- 创建 Lambda 函数 URL，为 Lambda 函数提供一个简单、可直接公开访问的 HTTP 终端节点。确保您的 Lambda 函数具有正确的权限。有关更多信息，请参阅[创建函数 URL 和为 Lambda 函数网址创建安全和身份验证模型](#)。
- 使用这些 Amazon 机制或其他机制的组合。

此外，当您激活高级功能时，您可以访问更多机制来提供对资源的外部访问权限。

管理你的 Amazon Web Services 账户

你可以 Amazon Web Services 账户 根据你使用的类型来管理 Amazon 你的。下表显示了在哪里可以找到每项管理任务的文档。

Task	报名参加 Amazon (新)	报名参加 Amazon (高级)
注册	报名参加 Amazon (新)	报名参加 Amazon (高级)
创建 账户	在中创建项目 Amazon 设置	报名参加 Amazon (高级)
关闭账户。	在中关闭项目 Amazon 设置	关闭一个 Amazon Web Services 账户
更新你的密码	在中更新您的密码 Amazon 设置	更新根用户密码
注册 MFA 设备	在中管理多因素身份验证 (MFA) Amazon 设置	步骤 3：(推荐) 设置 Amazon MCP 服务器
更改您的电子邮箱	在中更改您的电子邮件地址 Amazon 设置	更新 亚马逊 Web Services 电子邮件地址
更改你的名字	在中管理您的姓名或昵称 Amazon 设置	更新你的 Amazon Web Services 账户 name
更新联系人信息	在中编辑您的联系信息 Amazon 设置	更新您的主要联系人 Amazon Web Services 账户
更新备用联系人	不适用	更新您的备用联系人 Amazon Web Services 账户

Task	报名参加 Amazon (新)	报名参加 Amazon (高级)
管理账单	在中管理您的付款方式 Amazon 设置	更新您的账单 Amazon Web Services 账户
管理税务信息	在中管理税务登记 Amazon 设置	管理您的付款
启用或禁用 Amazon Web Services 区域	不适用。您无法修改自己的 Amazon Web Services 区域。	启用或禁用 Amazon Web Services 区域 在你的账户中
查看账户标识符	不适用	视图 Amazon Web Services 账户 标识符
创建账户别名	不适用	创建一个 Amazon Web Services 账户 别名
升级您的账户	在中升级您的账户 Amazon 设置	免费套餐计划
创建支出限额	在中创建支出限额 Amazon 设置	不适用
更新支出限额	在中更新支出限额 Amazon 设置	不适用
取消支出限制	移除中的支出限额 Amazon 设置	不适用
邀请团队成员	邀请团队成员进行协作 Amazon 设置	IAM 身份
在项目之间切换	在项目之间切换	Multi-session 支持
连接 AI 编码工具	连接 AI 编码工具	不适用

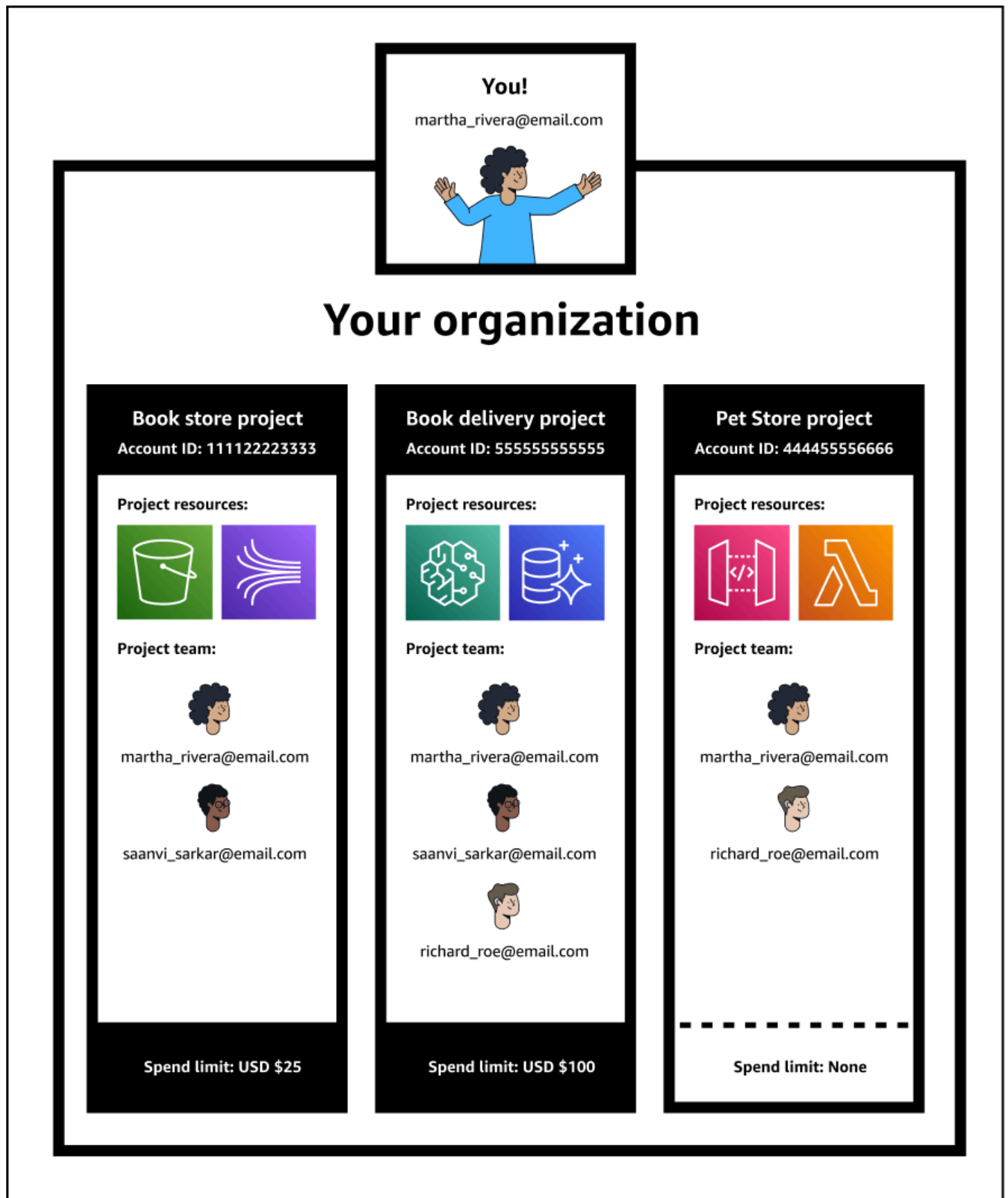
Task	报名参加 Amazon (新)	报名参加 Amazon (高级)
删除所有会话	删除中的所有会话 Amazon 设置	不适用
选择不使用 AI 数据	选择不使用您的内容来改善服务 Amazon 设置	AI 服务选择退出策略
请求您的 数据	申请你的 Amazon 生成器 ID 数据	索取您的数据
删除你的 Amazon 个人资料	关闭您的账户 Amazon 设置	关闭一个 Amazon Web Services 账户
管理印度地区的账户	在印度管理账户 Amazon 设置	管理印度地区的账户
创建管理员用户	不适用	报名参加 Amazon (高级)
规划您的账户治理结构	不适用	规划你的 Amazon Web Services 账户 治理结构

报名参加 Amazon（新）

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

当你使用注册 Amazon（新增）时，你会创建一个预配置的 Amazon 环境，允许你使用像 Google 这样已经拥有的登录名或 GitHub 访问你的 Amazon 资源。您的资源按项目进行组织。项目包含用于与其他合作者共享的 Amazon Web Services 账户 和设置。如果您使用付费计划，则您的项目还可以设定每月的税前成本，称为支出限额。您拥有的所有项目都构成了您的组织。您可以在“Amazon 设置”中管理您的组织、访问您的项目和添加团队成员。



当您注册 Amazon 使用 Sign up for Amazon (新) 时，Amazon 还会创建一个 Amazon 构建者 ID 帐户，该帐户是一个代表您个人的个人资料。每个电子邮件地址只能有一个 Amazon 构建者 ID。如果您已创建 Amazon 构建者 ID 但尚未创建 Amazon Web Services 帐户，则可能已经为您做了一些设置，你必须稍后再修改这些设置。

有关注册 Amazon (新) 的更多信息，请参阅以下文档：

- [比较注册选项](#)
- [支持 Amazon Web Services 服务 for 注册 Amazon \(新\)](#)

使用注册进行注册 Amazon (新)

当您注册时 Amazon，我们可能会要求您提供付款信息。我们的验证流程会在3-5天内扣留1美元（或等值金额），以验证您的账户并防止欺诈。在升级到付费计划之前，您不会产生任何费用。您可以随时通过“Amazon 设置”管理付款方式或关闭账户。此外，当您注册时 Amazon，您可能没有资格获得免费套餐。在这种情况下，您需要提供付款信息，然后您将进入付费计划。使用付费套餐时，您可以设置支出限额，使其在可预测和可控的预算范围内运营。

使用谷歌 GitHub、苹果或亚马逊为您的账户注册 Amazon (新) 支持。如果您已经在浏览器中登录了 Google 帐户，则该帐户将在您注册时使用 Amazon。

要注册 Amazon 使用注册 Amazon (新)

1. 打开[注册 Amazon](#) 页面。
2. 输入您的电子邮件或选择登录方式，例如谷歌 GitHub、苹果或亚马逊。
3. 如果您使用已经拥有的登录名，则系统会将您定向到提供商的登录名。登录后，您将被重定向到 Amazon 注册。
4. 输入您的姓名并选择“继续”。

当您授予团队成员访问您的项目的权限时，该名称将与他们共享。

5. 输入验证码，验证与您的登录相关的电子邮件。验证电子邮件后，选择“继续”。

当您授予团队成员访问您的项目的权限时，将与他们共享此电子邮件。

6. 为您的帐户输入一个强密码，然后选择“继续”。

Amazon 要求您的密码满足以下条件：

- 长度必须至少 8 个字符，最多 128 个字符。

- 必须至少包含以下字符类型中三种的组合：大写字母、小写字母、数字，以及 ! @ # \$ % ^ & * () < > [] { } | _ + - = 符号。
 - 它不得与您的 Amazon Web Services 账户 姓名或电子邮件地址相同。
7. 输入您的联系方式，然后选择“继续”。
 8. Amazon 将为您的三个项目中的一个项目配置 Amazon Web Services 区域 一个新名称。有关更多信息，请参阅 [Amazon Web Services 区域 为了你的项目](#)。您可以随时更改名称。

您现在可以访问 Amazon Web Services 管理控制台。要访问 Amazon 设置，请从中选择管理项目 Amazon Web Services 管理控制台。在 Amazon “设置” 中，您可以邀请团队成员、创建新项目以及修改账单和其他设置。

后续步骤

注册后 Amazon，您可以连接 AI 编码工具，添加团队成员进行协作，如果您有付费套餐，则可以设置支出限额。

- [连接 AI 编码工具](#)
- [邀请团队成员进行协作 Amazon 设置](#)
- [在中创建支出限额 Amazon 设置](#)

使用 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

[Amazon 设置](#)是您管理和访问项目的地方。Amazon 当您使用“注册 Amazon（新）”进行注册时，设置可用。您可以使用 Amazon “设置” 执行以下操作：

- 创建和访问您拥有的项目。有关更多信息，请参阅 [在中创建项目 Amazon 设置](#)。
- 访问已与您共享的项目。
- 邀请团队成员就您的项目进行协作。有关更多信息，请参阅 [邀请团队成员进行协作 Amazon 设置](#)。
- 在项目之间切换。有关更多信息，请参阅 [在项目之间切换](#)。

- 管理您的付款方式。有关更多信息，请参阅 [在中管理您的付款方式 Amazon 设置](#)。
- 从免费套餐升级到付费套餐。有关更多信息，请参阅 [在中升级您的账户 Amazon 设置](#)。
- 管理项目的支出限额。有关更多信息，请参阅 [在中创建支出限额 Amazon 设置](#)。
- 查看您的账单信息。有关更多信息，请参阅 [在中查看您的账单信息 Amazon 设置](#)。
- 管理您的个人资料信息。有关更多信息，请参阅 [在中管理您的姓名或昵称 Amazon 设置](#)、[在中更改您的电子邮件地址 Amazon 设置](#) 和 [在中编辑您的联系信息 Amazon 设置](#)。
- 管理您的安全设置和登录偏好。有关更多信息，请参阅 [在中更新您的密码 Amazon 设置](#) 和 [在中管理多因素身份验证 \(MFA\) Amazon 设置](#)。

当您管理个人资料信息或安全设置时，您将被重定向到 Amazon 构建者 ID 中心。您的 Amazon 构建者 ID 是在您使用“注册 Amazon（新建）”时创建的。有关更多信息，请参阅[什么是 Amazon 构建者 ID？](#)。

连接 AI 编码工具

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以为 AI 编码工具提供项目访问权限并安装代理工具包，该工具包捆绑了 Amazon MCP 服务器配置和一组精选的代理技能。这使您的 AI 编码工具可以代表您创建和管理 Amazon 资源。

将编码工具连接到项目的注意事项

- 您可以将 AI 编码工具连接到您自己的项目或已与您共享的项目。
- 当 AI 编码工具或本地代理创建 Amazon 资源时，您仍需对其负责。这包括[分担责任模型所定义的资源适当安全性](#)，以及这些资源可能产生的任何费用，无论这些费用是在免费计划中计算的，还是根据付费计划收取的。
- 您应对您的 AI 编码工具在您的项目中代表您采取的任何操作负责。
- 要查看您的代理创建的资源，请访问该服务的服务控制台。
- 您生成的证书供 Amazon CLI、Amazon 工具和软件 Amazon 开发工具包使用。PowerShell 可能不支持外部工具。对您的资源的访问有效期为 12 小时。使用以下命令续订您的证书：

```
aws login --profile profile-name
```

profile-name 替换为您在初始设置期间选择的配置文件名称。该命令将自动打开您的默认浏览器。你需要选择你的项目名称来完成登录过程。Amazon 可以将您的凭证续订 90 天。90 天后，您需要再次在浏览器窗口中授予访问权限。

将您的 AI 编码工具连接到您的项目

每个项目都有自己的一组证书，AI 编码工具可以使用这些凭证代表你创建和管理 Amazon 资源。

Amazon Web Services 管理控制台

要将您的 AI 编码工具连接到您的项目，请使用 Amazon 控制台

1. 在浏览器中打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择要访问的项目。
3. 在右上角的导航栏中，选择创建和管理云基础架构。
4. 选择“在 AI 编码工具中使用您的 Amazon 证书”。
5. 选择复制代理提示符并将其输入到您的编码代理中。

这会创建与您的 AI 编码代理共享指导文件的提示。指导文件访问来自的脚本 Amazon，该脚本设置了您的项目凭证和您的 AI 编码代理之间的连接。

您将为您的项目输入配置文件名称。此配置文件名称是您的 AI 编码工具访问资源的方式。

Use your terminal

运行以下命令下载并按照安装说明进行操作：

```
curl -fsSL https://github.com/aws/agent-toolkit-for-aws/blob/main/setup-instructions/setup.md
```

当您使用我们的新 Amazon 体验时，您的代理将安装 Amazon MCP 服务器，您将获得可用于项目的代理技能。您还将获得一份规则文件，其中包含针对此体验调整的指南。规则文件还允许您定义您希望代理提供何种级别的帮助。以下是支持的帮助级别：

- 低：当您建造时，该技能只会标记安全风险。它不会建议对您的架构进行任何改进或替代方案。

- 中等：在你进行构建时，如果该技能检测到潜在问题，它可能会问一些澄清性的问题。它不会建议对您的架构进行任何改进或替代方案。
- 高：当你建造时，该技能将提供高水平的支持。它将建议您的架构的改进或替代方案。

处理多个项目

每个项目都有自己的一组证书，AI 编码工具可以使用这些凭证代表你创建和管理 Amazon 资源。您可以使用配置文件来访问每个项目。配置文件是由维护的配置设置和凭据文件 Amazon CLI，您可以为每个配置文件指定一个唯一的名称。

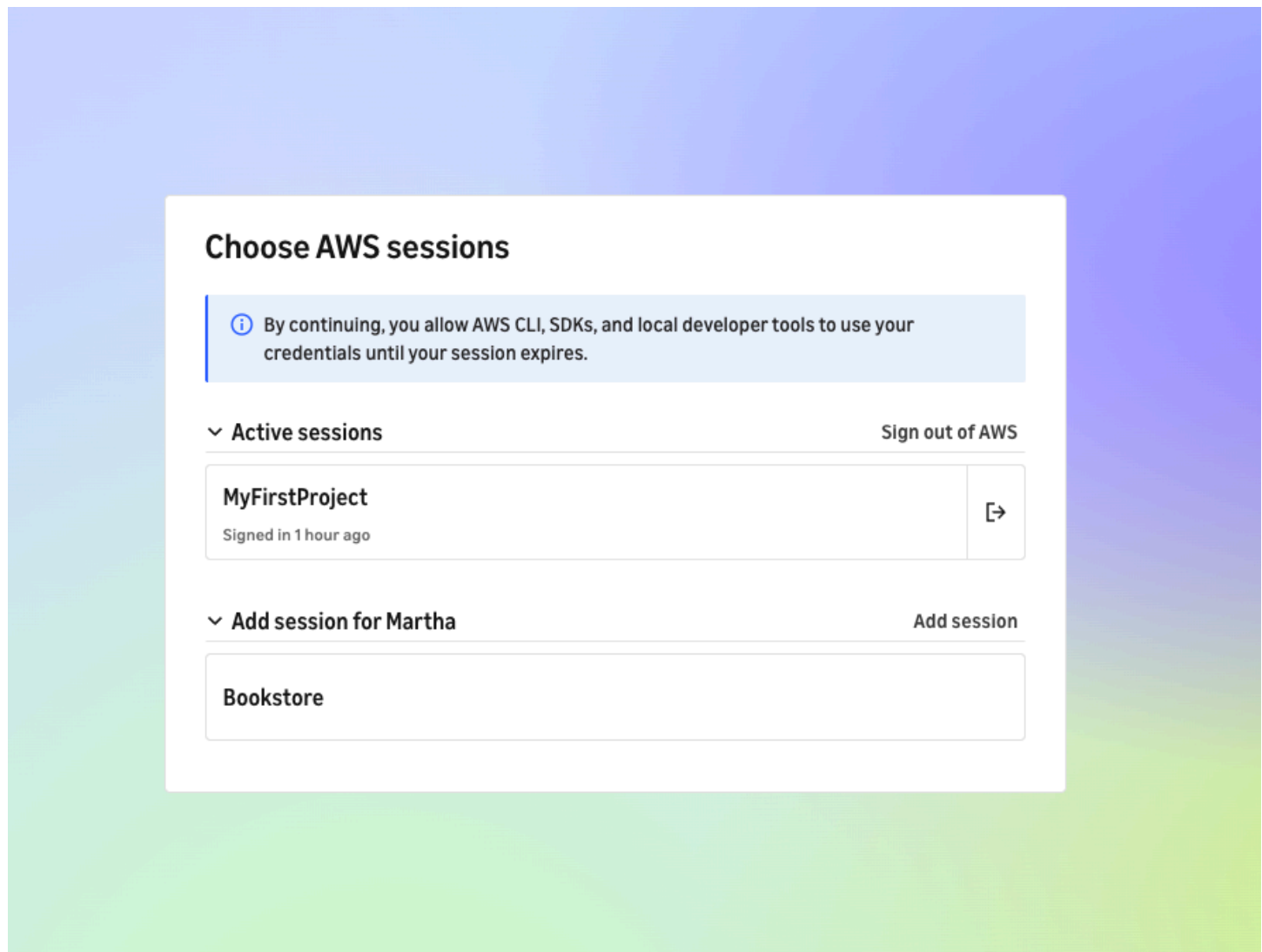
例如，如果您的第一个项目是MyFirstProject并且您在安装MyFirstProjectProfile期间选择了配置文件名称，则可以通过使用以下命令登录来访问该项目：Amazon CLI

```
aws login --profile MyFirstProjectProfile
```

如果您创建了另一个名为的项目Bookstore，则可以使用安装脚本并创建配置文件来访问该项目BookstoreProfile。然后，您可以使用以下命令登录：Amazon CLI

```
aws login --profile BookstoreProfile
```

但是，当你运行这两个命令中的任何一个时，你需要在选择会话页面上为你的 Amazon 证书选择一个 Amazon 会话。



此页面显示活动会话和您可以添加的会话。会话使用您的 Amazon 证书代表您的身份验证状态，它提供的证书与您的 AI 编码代理用于创建和管理资源的证书相同。

在此示例中，您已经登录MyFirstProject但尚未登录Bookstore。在“选择 Amazon 会话”页面上，您可以执行以下操作：

- 要继续使用 Amazon MyFirstProject，请选择MyFirstProject。
- 要访问Bookstore，请选择Bookstore。
- 要删除任何当前会话，请选择退出图标。
- 要 Amazon Web Services 账户 使用 IAM 用户访问，例如您创建的账户[报名参加 Amazon（高级）](#)，请选择添加会话。

您选择的证书将与您的 AI 编码代理用于创建和管理资源的凭证相同。例如，您可以使用以下命令登录：Amazon CLI

```
aws login --profile MyFirstProjectProfile
```

如果您随后选择 Bookstore 会话，您的 AI 编码工具将在 Bookstore 项目中创建 Amazon 资源。

请务必选择与您的个人资料关联的项目相匹配的会话。

Amazon 项目所有者的操作

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

当你拥有自己的项目时，你对项目拥有管理控制权。这包括你可以在其中完成的任务 [使用 Amazon 设置](#)。您还可以执行仅限超级用户的操作。您的团队成员无法完成这些操作。

您当前可以执行的仅限超级用户的操作如下：

- 编辑或删除拒绝所有委托人的 S3 存储桶策略。您可以这样做来使用错误配置的存储桶策略解锁 S3 存储桶。
- 编辑或删除拒绝所有委托人的基于 SQS 资源的策略。你可以这样做，通过错误配置的基于资源的策略解锁 SQS 队列。

执行仅限超级用户的操作

1. 登录您的项目并打开 IAM 控制台，网址为 <https://console.aws.amazon.com/iam/>。
2. 在控制台的导航窗格中，选择根访问管理。
3. 对于权限操作，请选择要在成员账户中执行的特权操作。
 - 选择删除 Amazon S3 存储桶策略，以删除一项配置错误的存储桶策略，此策略将会拒绝所有主体访问 Amazon S3 存储桶策略。
 - a. 输入 S3 URI，或选择 Browse S3 从项目中的存储桶中选择一个名称。
 - b. 选择删除存储桶策略。

- c. 在删除配置错误的策略后，使用 Amazon S3 控制台来纠正存储桶策略。有关更多信息，请参阅《Amazon S3 用户指南》中的[使用 Amazon S3 控制台添加存储桶策略](#)。
- 选择“删除 Amazon SQS 策略”以删除拒绝所有委托人访问 Amazon SQS 队列的基于资源的策略。
 - a. 在 SQS 队列名称中输入队列名称。
 - b. 选择“删除 SQS 策略”。
 - c. 在删除配置错误的策略后，使用 Amazon SQS 控制台来纠正队列策略。有关更多信息，请参阅《Amazon SQS 开发人员指南》中的[Configuring an access policy in Amazon SQS](#)。

在中更新您的密码 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

你可以在 Amazon “设置”中更新你的密码。

要在中更新您的密码 Amazon 设置

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理安全和登录。

您将被重定向到您的 Amazon 建筑商 ID 个人资料。

3. 对于“授权”，选择“更新密码”。
4. 对于 Current password (当前密码)，请键入您的当前密码。
5. 对于“新密码”，输入新密码。

Amazon 要求您的密码满足以下条件：

- 长度必须至少 8 个字符，最多 128 个字符。
 - 必须至少包含以下字符类型中三种的组合：大写字母、小写字母、数字，以及 ! @ # \$ % ^ & * () < > [] { } | _ + = 符号。
6. 在“确认新密码”中，输入您的新密码。

7. 选择更新。

在中管理多因素身份验证 (MFA) Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

Multi-factor 身份验证 (MFA) 是一种增强安全性的简单而有效的机制。第一个因素 (密码) 是您记住的秘密，也称为知识因素。其他因素可以是拥有因素 (您拥有的东西，例如安全密钥) 或固有因素 (您与生俱来的东西，例如生物识别扫描)。我们强烈建议您配置 MFA 以为您的账户添加额外的层。

您可以注册内置身份验证器，也可以注册保存在物理安全位置的安全密钥。如果您无法使用内置身份验证器，则可以使用已注册的安全密钥。对于身份验证器应用程序，您也在这些应用中启用云备份功能或同步功能。这可有助于避免在 MFA 设备丢失或损坏的情况下，失去对配置文件的访问权限。

关键点

注册和管理 MFA 设备时，请记住以下要点：

- 建议注册多个 MFA 设备。如果您无法访问所有已注册的 MFA 设备，则将无法恢复您的账户。
- 我们建议您定期检查已注册的 MFA 设备，确保它们处于最新状态且能正常运行。此外，不使用时，应将这些装置存放在物理安全位置。
- 若您是通过继续使用 Google 创建的账户，那么您可以通过您的 Google 账户启用多重身份验证。有关详细信息，请参阅[开启两步验证](#)。
- 如果您使用“继续使用 Apple”创建帐户，则您的 Apple 帐户中可能已经启用了多重身份验证。如果不是，有关如何启用它的详细信息，请参阅[Apple 帐户 Two-factor 身份验证](#)。
- 如果您使用“继续”创建了账户 GitHub，则可以通过您的 GitHub 账户启用多重身份验证。有关详细信息，请参阅[配置 \(GitHub\) 双因素身份验证](#)。
- 如果您使用“继续使用亚马逊”创建账户，则可以通过您的亚马逊账户启用多重身份验证。有关详细信息，请参阅[什么是 Two-Step 验证？](#)。

我们新推出的可用的 MFA 类型 Amazon 经历

我们的新 Amazon 体验支持以下多因素身份验证 (MFA) 设备类型。

FIDO2 身份验证器

[FIDO2](#) 是一个包含 CTAP2 的标准，[WebAuthn](#) 并且基于公钥加密。FIDO 凭证具有防网络钓鱼功能，因为它们是创建凭证的网站所独有的，例如 Amazon。

Amazon 支持 FIDO 身份验证器的两种最常见外形规格：内置身份验证器和安全密钥。有关最常见的 FIDO 身份验证器类型的更多信息，请参阅下文。

Built-in 身份验证器

某些设备具有内置的身份验证器，例如开启的 TouchID MacBook 或 Windows Hello-compatible 摄像头。如果您的设备兼容 FIDO 协议（包括）WebAuthn，则可以使用指纹或面部作为第二要素。有关更多信息，请参见 [FIDO 身份验证](#)。

安全密钥

您可以购买 FIDO2-compatible 外置 USB、BLE 或 NFC-connected 安全密钥。当系统提示你输入 MFA 设备时，点击按键的传感器。YubiKey 或者飞天制造兼容的设备。有关所有兼容安全密钥的列表，请参阅 [FIDO 认证产品](#)。

密码管理器、密钥提供程序和其他 FIDO 身份验证器

多个第三方提供商支持移动应用程序中的 FIDO 身份验证，例如密码管理器中的功能、带有 FIDO 模式的智能卡以及其他外形规格。这些 FIDO-compatible 设备可以与 IAM Identity Center 配合使用，但我们建议您在为 MFA 启用此选项之前亲自测试 FIDO 身份验证器。

Note

有些 FIDO 身份验证器可以创建可发现的 FIDO 凭证，称为密钥。密钥可以绑定到创建密钥的设备，也可以同步并备份到云端。例如，您可以在支持的 Macbook 上使用 Apple Touch ID 注册密钥，然后按照登录时屏幕上的提示使用 Google Chrome，在 iCloud 中使用密钥从 Windows 笔记本电脑登录网站。有关哪些装置支持可同步密钥以及当前密钥在操作系统和浏览器之间的互操作性的更多信息，请参阅 [passkeys.dev](#) 上的[装置支持](#)（此资源由 FIDO 联盟和万维网联盟 (W3C) 维护）。

身份验证器应用程序

身份验证器应用程序是基于一次性密码（OTP）的第三方身份验证器。您可将安装在移动装置或平板电脑上的身份验证器应用程序用作授权的 MFA 设备。第三方身份验证器应用程序必须符合 RFC 6238，这是一种标准的基于时间的一次性密码（TOTP）算法，且能够生成六位数身份验证码。

提示进行多重身份验证时，务必在显示的输入框中输入来自身份验证器应用程序的有效代码。分配给用户的每台 MFA 设备必须是唯一的。可为任意给定用户注册两个身份验证器应用程序。

您可从以下常见的第三方身份验证器应用程序中进行选择。但是，任何 TOTP-compliant 应用程序都可以使用 Amazon 生成器 ID MFA。

操作系统	经过测试的身份验证器应用程序
Android	1Password 、 Authy 、 Duo Mobile 、 Microsoft 身份验证器 、 Google 身份验证器
iOS	1Password 、 Authy 、 Duo Mobile 、 Microsoft 身份验证器 、 Google 身份验证器

注册 MFA 设备

Note

注册 MFA 后，退出登录，然后在同一装置上重新登录，系统可能不会提示您在受信任的装置上进行 MFA。

使用身份验证器应用程序注册 MFA 设备

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理安全和登录。

您将被重定向到您的 Amazon Builder ID 个人资料。

3. 在 Security (安全性) 页面上，选择 Register device (注册装置) 。
4. 在 Register MFA device (注册 MFA 设备) 页面上，选择 Authenticator app (身份验证器应用程序) 。
5. Amazon Builder ID 操作并显示配置信息，包括二维码图形。此图形是秘密配置密钥的表示形式，适用于不支持 QR 代码的身份验证器应用程序上的手动输入。
6. 打开身份验证器应用程序。如需了解应用程序列表，请参阅 [身份验证器应用程序](#)。

如果身份验证器应用程序支持多个 MFA 设备或账户，请选择相应的选项以创建新的 MFA 设备或账户。

7. 确定 MFA 应用程序是否支持 QR 代码，然后在 Set up your authenticator app (设置身份验证器应用程序) 页面上执行以下操作之一：
 1. 选择 Show QR code (显示 QR 代码)，然后使用该应用程序扫描 QR 代码。例如，您可选择摄像头图标或选择类似于 Scan code (扫描代码) 的选项，然后使用装置的摄像头扫描此代码。
 2. 选择 Show secret key (显示密钥)，然后将该密钥输入到 MFA 应用程序中。

完成输入后，您的身份验证器应用程序将生成并显示一次性密码。

8. 在 Authenticator code (身份验证器代码) 框中，输入当前显示在身份验证器应用程序中的一次性密码。选择分配 MFA。

Important

生成代码之后立即提交您的请求。如果您生成代码后等待时间过长才提交请求，则 MFA 设备已成功与您的 Amazon 生成器 ID 关联，但是 MFA 设备不同步。这是因为基于时间的一次性密码 (TOTP) 很快会过期。这种情况下，您可以重新同步装置。有关更多信息，请参阅 *I get the message 'An unexpected error has occurred' when I try to register or sign in with an authenticator app*。

9. 要在 Amazon Builder ID 中为您的设备起一个友好的名称，请选择“重命名”。此名称可帮助您区分此装置和您注册的其他装置。

MFA 设备现已准备就绪，可以与 Amazon “设置”、“您的项目”和“Amazon 生成器 ID”一起使用。

将安全密钥注册为您的 MFA 设备

使用安全密钥注册 MFA 设备

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理安全和登录。

您将被重定向到您的 Amazon Builder ID 个人资料。

3. 在 Security (安全性) 页面上，选择 Register device (注册装置)。
4. 在 Register MFA device (注册 MFA 设备) 页面上，选择 Security key (安全密钥)。
5. 确保已启用安全密钥。如果您使用单独的物理安全密钥，请将其连接到您的计算机。

6. 按照屏幕上的说明进行操作。您的体验取决于您的操作系统和浏览器。
7. 要在 Amazon Builder ID 中为您的设备起一个友好的名称，请选择“重命名”。此名称可帮助您区分此装置和您注册的其他装置。

MFA 设备现已准备就绪，可以与 Amazon “设置”、“您的项目”和“Amazon 生成器 ID”一起使用。

重命名 MFA 设备

重命名 MFA 设备

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理安全和登录。

您将被重定向到您的 Amazon Builder ID 个人资料。

3. 选择安全性。位于此页面后，可看到 Rename (重命名) 显示为灰色。
4. 选择要更改的 MFA 设备。这将允许您选择 Rename (重命名)。随即显示对话框。
5. 在打开的提示中，在 MFA device name (MFA 设备名称) 中输入新名称，然后选择 Rename (重命名)。重命名的设备显示在 Multi-factor 身份验证 (MFA) 设备下。

删除 MFA 设备

建议保留两个或多个活动 MFA 设备。要禁用多重身份验证，请从您的个人资料中删除所有已注册的 MFA 设备。

删除 MFA 设备

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理安全和登录。

您将被重定向到您的 Amazon Builder ID 个人资料。

3. 在安全页面上，选择要更改的 MFA 设备，然后选择删除。
4. 在 Delete MFA device? (要删除 MFA 设备吗？) 模式窗口中，按照说明删除装置。
5. 选择删除。

已删除的设备不再出现在 Multi-factor 身份验证 (MFA) 设备下。

删除中的所有会话 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以在 Amazon “设置” 中删除跨设备的所有会话。如果您无法识别某台设备，请更改密码并删除所有会话。

删除所有会话

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理安全和登录。

您将被重定向到您的 Amazon 建筑商 ID 个人资料。

3. 对于已登录的设备，选择删除所有会话。
4. 确认您的选择，然后选择“删除所有会话”。

您将退出“Amazon 设置”。

在中管理您的姓名或昵称 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

你可以随时更改你的名字。所有团队成员都可以看到你的名字，如果你已经升级到付费套餐，这个名字就会出现在你的账单信息上。如果您 Amazon 在印度注册，则您的姓名必须与计划用于客户验证的文件上显示的姓名完全一致。

当您更改姓名时，您会更改 Amazon 生成器 ID 中的名称。这将影响您在 Amazon 设置中的姓名、Amazon 生成器 ID 以及您直接通过 Amazon 构建器 ID 访问的任何 Amazon 资源。

你的名字是指在与他人互动时在工具和服务中提及你的名字。你的昵称表示你希望如何被 Amazon 朋友和其他与你密切合作的人所认识。

更改你的名字或昵称

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理个人资料。
3. 要查看个人资料信息，请选择管理个人资料。

您将被重定向到您的 Amazon 建筑商 ID 个人资料。

4. 要查看个人资料信息，请选择“编辑”。
5. （可选）对于“名称”，输入新名称。
6. （可选）在“昵称”中，输入新的昵称。
7. 选择保存更改。

在中更改您的电子邮件地址 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以在 Amazon “设置”中更改您的电子邮件。当您更改电子邮件时，您之前的电子邮件将与您的 Amazon 个人资料和 Amazon 生成器 ID 分开。您将无法使用该电子邮件访问 Amazon “设置”中的任何项目，但您可以使用该电子邮件 Amazon 再次注册。

当您授予团队成员访问您的项目的权限时，您的电子邮件地址将与他们共享。

更改您的电子邮箱

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理个人资料。
3. 要查看个人资料信息，请选择管理个人资料。

您将被重定向到您的 Amazon Builder ID 个人资料。

4. 要获取联系人信息，请选择编辑。
5. 在“电子邮件地址”中，输入新的电子邮件地址，然后选择“验证电子邮件”。我们将向您发送新电子邮件地址的验证码。您将在“验证电子邮件”弹出框中输入。

6. 对于验证码，请输入我们发送到您的新电子邮件的验证码。
7. 选择验证。

在中编辑您的联系信息 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以编辑与“Amazon 设置”关联的电话号码或地址。当您修改这些值时，它们可能会影响纳税义务。

若要编辑您的联系信息

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理个人资料。
3. 要查看联系信息，请选择“编辑”。
4. 输入新的联系人信息。
5. 选择保存。

选择不使用您的内容来改善服务 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

Amazon AI 服务可能会使用和存储客户内容来改进服务，例如修复运营问题、评估服务性能、调试或模型训练。为此，我们可能会将此类内容存储在您使用服务 Amazon Web Services 区域 的地方 Amazon Web Services 区域 以外。您可以通过 Amazon “设置” 选择不使用您的内容以改善服务。选择退出的效果是将 AI 服务选择退出政策 Amazon 附加到您的组织。Amazon 有关选择退出政策的更多信息，请参阅 [AI 服务选择退出政策文档](#)。

选择退出所有服务将使您的所有项目退出服务改进，使用您的内容进行当前和未来支持的 AI 服务，这些服务由 AI 服务选择退出政策支持。

要选择退出亚马逊 Monitron，还需要采取其他步骤。有关更多信息，请参阅 [Amazon 服务条款](#)。只有项目所有者可以选择不让 Amazon 人工智能服务使用数据。

通过以下方式选择不使用数据 Amazon 人工智能服务

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“项目”。
3. 在“概述”中，选择“操作”，然后选择“选择退出 Amazon AI 服务使用数据”。
4. 确认您的选择并选择退出。

申请你的 Amazon 生成器 ID 数据

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以请求和查看与您的 Amazon 构建器 ID 以及使用构建器 ID 访问的 Amazon 应用程序和服务相关的个人信息。Amazon 我们将在 30 天内处理您的请求，并在您的数据准备就绪时通知您。当您的数据请求处于待处理状态时，您无法关闭您的 Amazon 个人资料。您仍然可以关闭项目或拥有所有项目的组织。

有关行使数据主体权利的更多信息，包括提供的与其他 Amazon 网站、应用程序、产品、服务、活动和体验相关的个人信息，请参阅[Amazon 隐私](#)。

请求您的数据

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理个人资料。
3. 选择“管理个人资料”。

您将被重定向到您的 Amazon 建筑商 ID 个人资料。

4. 选择 Privacy & data (隐私与数据)。
5. 选择请求您的建筑商 ID 数据或 Amazon 数据。

页面顶部会显示一条绿色的确认消息，表示我们已收到您的请求并将在 30 天内完成审核。

6. 当您收到我们发送的有关请求已处理的电子邮件时，请返回到您的 Amazon Builder ID 个人资料 的隐私和数据页面。选择最新可用的按钮 Download ZIP archive with your data (下载包含您数据的 ZIP 存档)。

当您的数据请求处于待处理状态时，您将无法删除您的 Amazon 生成器 ID。

在中创建项目 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

一个项目包含一个用于创建 Amazon 资源的单一 Amazon Web Services 账户 项目。项目还包括用于与其他合作者共享的设置。您创建的 Amazon 资源应代表一个应用程序或一组相关的用例。一个项目可以跨越应用程序的开发和生产环境。例如，您可以创建一个名为 Bookstore 的项目，该项目包含书店应用程序的资源，包括数据库、计算资源和存储。

您可以与其他团队成员共享此项目，他们可以为书店应用程序构建和管理资源。

根据账户中的资源，每个项目都有自己的成本控制。如果您使用的是付费套餐，则可以在 Amazon 设置中为每个项目配置支出限制。有关更多信息，请参阅 [在中创建支出限额 Amazon 设置](#)。作为项目所有者，您负责开具每月使用费和经常性费用的发票。

创建项目的注意事项

- 作为团队成员，您可以访问不属于您的项目。
- 每个项目名称对于您的项目都必须是唯一的。其他团队成员拥有的项目可以具有相同的名称。
- 项目名称可以包含以下有效字符：a-z、A-Z、0-9 和句点 (.)。
- 创建项目时，根据联系地址中的国家，将其 Amazon 分配给一个地区——美国东部 (us-east-2 俄亥俄州) (eu-north-1)、欧洲 (斯德哥尔摩) (ap-southeast-2) 或亚太地区 (悉尼) ()，即美国、欧洲或亚太地区。您创建的任何区域资源都将托管在该区域。有关更多信息，请参阅 [Amazon Web Services 区域 为了你的项目](#)。

创建项目

创建项目

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“项目”。
3. 选择创建项目。
4. 在项目名称中，输入项目的描述性名称。

当您邀请团队成员进行协作时，系统会与他们共享此名称。

5. 选择创建。

创建项目需要几秒钟。当您的项目可用时，您可以选择项目并访问 Amazon Web Services 管理控制台以开始构建。

如果您已将 AI 编码工具设置为与您的 Amazon Web Services 账户互连，则可以提示它在新项目中创建资源。

使用 AI 编码工具的示例提示开始使用：

```
What is the Region for my project test project?
```

```
Create a hello world Lambda function in my project test project.
```

```
Create an S3 bucket in my project test project.
```

Amazon Web Services 区域 为了你的项目

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

创建项目时，根据您的联系地址中的国家/地区（美国、欧洲或 Amazon 亚太地区）将其分配到某个区域——美国东部（俄亥俄州 eu-north-1）（ ）、欧洲（斯德哥尔摩 ap-southeast-2）（ ）或亚太地区（悉尼）（ ）。us-east-2 您创建的任何区域资源都将托管在该区域中。

以下是为您的账户选择 Amazon Web Services 区域的注意事项：

- 如果您在 Amazon “设置” 中更改联系信息，则所选区域将不会更改。如果您需要访问特定区域，请使用注册 Amazon（高级）。您还可以为您的账户激活高级功能以选择不同的区域。
- Amazon 可能会引入其他支持的区域，但这些区域仅适用于新注册。要查看截至 2026 年 8 月 18 日的最新支持区域，请参阅下表。如果您已经有项目，则可以在[Amazon 设置中找到所选区域](#)。
- 您的项目提供全球服务。这些服务是通过单一区域访问的，该区域可能与您的家乡地区不同。有关更多信息，请参阅[Amazon 故障隔离边界](#)。此外，还有一些服务可在特定地区使用。在中 Amazon Web Services 管理控制台，您可以在特定区域查看这些服务，但是当您导航到其他服务时，您将返回到所选区域。
- 如果您使用 Amazon Bedrock，则可以使用默认启用的不在所有商业广告中创建资源 Amazon Web Services 区域的 API。
- 如果您使用 CloudFront，则某些会在所选区域之外创建资源的功能不可用。这包括 Amazon WAF 与一起使用 CloudFront。
- 一些涉及全球服务 CloudTrail 的事件记录在全球服务运营的地区中。您可以访问这些活动。
- Amazon WAF 和亚马逊 CloudWatch 日志在美国东部（弗吉尼亚北部）（us-east-1）可用。

您可以使用“Amazon 设置”找到账户中所有项目的选定区域。在中 Amazon Web Services 管理控制台，大多数服务控制台都托管在您所在的区域，包括 Bedrock 和 SageMaker。如果您查看来自全球服务的服务控制台，该控制台会自动将您的所有 API 调用路由到该全球服务的相应区域。

找到选定的 Amazon Web Services 区域 为了你的项目

作为最佳实践，我们建议您在创建任何 Amazon 资源之前务必确认项目的内容。Amazon Web Services 区域

查找选定的 Amazon Web Services 区域 为了你的项目

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“项目”。
3. 在概述部分中，选择其他信息。

在此视图中，您还可以找到与您的项目关联的 Amazon Web Services 账户 ID。

4. 对于区域，您将看到 Amazon Web Services 区域 您的项目已在中进行配置。

当您在任何项目中创建区域 Amazon 资源时，这些资源的亚马逊资源名称将包含这些资源 Amazon Web Services 区域。

在美国东部（俄亥俄州）（us-east - 2）提供区域资源的国家

国家/地区名称	国家/地区代码
安提瓜和巴布达	AG
阿根廷	AR
巴哈马	BS
巴巴多斯	BB
伯利兹	BZ
玻利维亚	BO
巴西	BR
加拿大	CA
智利	CL
哥伦比亚	CO
哥斯达黎加	CR
多米尼加	DM
多米尼加共和国	DO
厄瓜多尔	EC
萨尔瓦多	SV
格林纳达	GD
危地马拉	GT
圭亚那	GY

国家/地区名称	国家/地区代码
海地	HT
洪都拉斯	HN
牙买加	JM
墨西哥	MX
尼加拉瓜	NI
巴拿马	PA
巴拉圭	PY
秘鲁	PE
圣基茨和尼维斯	KN
圣卢西亚岛	LC
圣文森特和格林纳丁斯	VC
苏里南	SR
特立尼达和多巴哥	TT
美国	美国
乌拉圭	UY
委内瑞拉	VE
安圭拉岛	AI
阿鲁巴岛	AW
百慕大	BM
博内尔岛、圣尤斯特歇斯岛和萨巴岛	BQ

国家/地区名称	国家/地区代码
英属维尔京群岛	VG
开曼群岛	KY
库拉索	CW
福克兰群岛	FK
法属圭亚那	GF
瓜德罗普	GP
马提尼克	MQ
Montserrat	MS
波多黎各	PR
圣巴泰勒米	BL
圣马丁	MF
圣皮埃尔和密克隆群岛	PM
荷属圣马丁	SX
特克斯和凯科斯群岛	TC
U.S. 维尔京群岛	VI

在亚太地区（悉尼）（**ap-southeast-2**）提供区域资源的国家

国家/地区名称	国家/地区代码
阿富汗	AF
澳大利亚	AU

国家/地区名称	国家/地区代码
孟加拉国	BD
不丹	BT
文莱	BN
柬埔寨	KH
中国	CN
东帝汶 (Timor-Leste)	TL
斐济	FJ
Hong Kong	HK
印度	IN
印度尼西亚	ID
日本	JP
哈萨克	KZ
基里巴斯	KI
吉尔吉斯斯坦	KG
老挝	LA
澳门	MO
马来西亚	MY
马尔代夫	MV
马绍尔群岛	MH
密克罗尼西亚	FM

国家/地区名称	国家/地区代码
蒙古	MN
缅甸	MM
瑙鲁	NR
尼泊尔	NP
新西兰	NZ
巴基斯坦	PK
帕劳群岛	PW
巴布亚新几内亚	PG
菲律宾	PH
萨摩亚群岛	WS
新加坡	SG
所罗门群岛	SB
韩国	KR
斯里兰卡	LK
中国台北	TW
塔吉克斯坦	TJ
泰国	TH
汤加	TO
土库曼斯坦	TM
图瓦卢	TV

国家/地区名称	国家/地区代码
乌兹别克斯坦	UZ
瓦努阿图	VU
越南	VN
美属萨摩亚	AS
圣诞岛	CX
科科斯（基林）群岛	CC
库克群岛	CK
法属玻里尼西亚	PF
关岛	GU
赫德岛和 McDonald 群岛	HM
新喀里多尼亚	NC
纽埃岛	NU
诺福克岛	NF
北马里亚纳群岛	MP
皮特凯恩群岛	PN
托克劳	TK
U.S. 偏远小岛屿	UM
瓦利斯和富图纳群岛	WF

在欧洲提供区域资源的国家（斯德哥尔摩）（eu-north-1）

国家/地区名称	国家/地区代码
阿尔巴尼亚	AL
阿尔及利亚	DZ
安道尔	AD
安哥拉	AO
亚美尼亚	AM
奥地利	AT
阿塞拜疆	AZ
巴林	BH
白俄罗斯	BY
比利时	BE
贝宁	BJ
波斯尼亚和黑塞哥维那	BA
博茨瓦纳	BW
保加利亚	BG
布基纳法索	BF
布隆迪	BI
佛得角	CV
喀麦隆	CM
中非共和国	CF

国家/地区名称	国家/地区代码
乍得	TD
科摩罗	KM
刚果（布拉柴维尔）	CG
刚果（刚果民主共和国）	CD
科特迪瓦	CI
克罗地亚	HR
塞浦路斯	CY
捷克共和国	CZ
丹麦	DK
吉布提	DJ
埃及	EG
赤道几内亚	GQ
厄立特里亚	ER
爱沙尼亚	EE
史瓦帝尼	SZ
埃塞俄比亚	ET
芬兰	FI
法国	FR
加蓬	GA
冈比亚	GM

国家/地区名称	国家/地区代码
格鲁吉亚	GE
德国	DE
加纳	GH
希腊	GR
几内亚	GN
Guinea-Bissau	GW
匈牙利	HU
Iceland	IS
伊拉克	IQ
爱尔兰	IE
以色列	IL
意大利	IT
约旦	JO
肯尼亚	KE
科索沃	XK
科威特	KW
拉脱维亚	LV
黎巴嫩	LB
莱索托	LS
利比里亚	LR

国家/地区名称	国家/地区代码
利比亚	LY
列支敦士登	LI
立陶宛	LT
卢森堡	LU
马达加斯加	MG
马拉维	MW
Mali	ML
马耳他	MT
毛里塔尼亚	MR
毛里求斯	MU
摩尔多瓦	MD
摩纳哥	MC
黑山共和国	ME
摩洛哥	MA
莫桑比克	MZ
纳米比亚	NA
荷兰	NL
尼日尔	NE
尼日利亚	NG
北马其顿	MK

国家/地区名称	国家/地区代码
挪威	NO
阿曼	OM
巴勒斯坦	PS
波兰	PL
葡萄牙	PT
卡塔尔	QA
罗马尼亚	RO
俄罗斯	RU
卢旺达	RW
圣马力诺	SM
圣多美和普林西比	ST
沙特阿拉伯	SA
塞内加尔	SN
塞尔维亚	RS
塞舌尔	SC
塞拉利昂	SL
斯洛伐克	SK
斯洛文尼亚	SI
索马里	SO
南非	ZA

国家/地区名称	国家/地区代码
南苏丹	SS
西班牙	ES
瑞典	SE
瑞士	CH
坦桑尼亚	TZ
多哥	TG
突尼斯	TN
土耳其	TR
乌干达	UG
乌克兰	UA
阿拉伯联合酋长国	AE
英国	GB
梵蒂冈城	VA
也门	YE
赞比亚	ZM
津巴布韦	ZW
奥兰群岛	AX
南极洲	AQ
布韦岛	BV
英属印度洋领地	IO

国家/地区名称	国家/地区代码
法罗群岛	FO
法属南部领地	TF
直布罗陀	GI
格陵兰	GL
根西岛	GG
马恩岛	IM
Jersey	JE
马约特岛	YT
留尼汪岛	RE
圣赫勒拿岛	SH
南乔治亚岛和南桑威奇群岛	GS
斯瓦尔巴群岛和扬马延岛	SJ
西撒哈拉	EH

为您的组织提供托管政策

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

当您使用我们的新 Amazon 体验时，Amazon 可以管理组织管理策略，包括资源控制策略 (RCP) 和服务控制策略 (SCP)。这些保护性控制措施可防止项目所有者或团队成员执行会限制为帮助您快速构建和开发而定义的预配置默认值 Amazon 的操作。

项目的服务控制策略

以下是适用于项目中所有用户的服务控制策略，不可更改：

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BlockOrgEscape",
      "Effect" : "Deny",
      "Action" : [
        "account:CloseAccount",
        "organizations:AcceptHandshake",
        "organizations:LeaveOrganization",
        "sso:CreateInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProtectManagedRoles",
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam>DeleteRolePermissionsBoundary",
        "iam>DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:TagRole",
        "iam:UntagRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : "arn:*:iam::*:role/managed/*",
      "Condition" : {
        "StringNotLike" : {
          "aws:PrincipalArn" : "arn:*:iam::*:role/managed/
AWSManagedAccountManagementAccessRole"
        }
      }
    }
  ]
}
```

```
]
}
```

激活高级功能时，此政策不会被删除。有关更多信息，请参阅 [激活高级 Amazon 功能](#)。

此外，我们对项目中的所有用户应用以下服务控制政策，以限制对您的项目进行某些不支持或必须在 Amazon “设置” 中完成的修改：

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BlockAccountManagementAPIs",
      "Effect" : "Deny",
      "Action" : [
        "account:AcceptPrimaryEmailUpdate",
        "account:DeleteAlternateContact",
        "account:DisableRegion",
        "account:EnableRegion",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetRegionOptStatus",
        "account:PutAccountName",
        "account:PutAlternateContact",
        "account:PutContactInformation",
        "account:StartPrimaryEmailUpdate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyBillingOperations",
      "Effect" : "Deny",
      "Action" : "billing:*",
      "Resource" : "*"
    },
    {
      "Sid" : "DenyNotificationContactsOperations",
      "Effect" : "Deny",
      "Action" : "notifications-contacts:*",
      "Resource" : "*"
    },
    {
```

```

    "Sid" : "DenyRestrictedNotificationOperations",
    "Effect" : "Deny",
    "Action" : [
        "notifications:AssociateChannel",
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:AssociateManagedNotificationAdditionalChannel",
        "notifications:AssociateOrganizationalUnit",
        "notifications>CreateEventRule",
        "notifications>CreateNotificationConfiguration",
        "notifications>DeleteEventRule",
        "notifications>DeleteNotificationConfiguration",
        "notifications:DeregisterNotificationHub",
        "notifications:DisableNotificationsAccessForOrganization",
        "notifications:DisassociateChannel",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAdditionalChannel",
        "notifications:DisassociateOrganizationalUnit",
        "notifications:EnableNotificationsAccessForOrganization",
        "notifications:GetEventRule",
        "notifications:GetFeatureOptInStatus",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListMemberAccounts",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "notifications:ListTagsForResource",
        "notifications:PutFeatureOptInStatus",
        "notifications:RegisterNotificationHub",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration"
    ],
    "Resource" : "*"
},
{
    "Sid" : "DenyRoleManagerDisablement",
    "Effect" : "Deny",

```

```

    "Action" : "iam:PutAccountProperties",
    "Resource" : "*",
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "iam:AccountPropertyNamespaces" : "RoleManager"
        }
    }
}
]
}

```

当您激活高级功能时，此政策即会被删除。有关更多信息，请参阅 [激活高级 Amazon 功能](#)。

此外，我们还对项目中的所有用户应用以下服务控制政策，Amazon Web Services 区域 以限制为允许支持分区服务，具体取决于您的 *selected-region* 情况：

```

{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partitioal",
      "Effect" : "Deny",
      "NotAction" : [
        "account:*",
        "acm:*",
        "activate:*",
        "artifact:*",
        "aws-marketplace:*",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "budgets:*",

```

```
"ce:*",
"chatbot:*",
"cloudfront-keyvaluestore:*",
"cloudfront:*",
"cloudshell:*",
"cloudtrail:LookupEvents",
"cloudwatch:BatchGet*",
"cloudwatch:Describe*",
"cloudwatch:GenerateQuery",
"cloudwatch:Get*",
"cloudwatch:List*",
"consoleapp:*",
"cost-optimization-hub:*",
"ec2:DescribeRegions",
"ecr-public:*",
"freetier:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"invoicing:*",
"kms:CreateGrant",
"kms:Decrypt",
"kms:DescribeKey",
"kms:ListAliases",
"lightsail:AttachCertificateToDistribution",
"lightsail:CreateCertificate",
"lightsail:CreateContactMethod",
"lightsail:CreateDistribution",
"lightsail:CreateDomain",
"lightsail:CreateDomainEntry",
"lightsail>DeleteAlarm",
"lightsail>DeleteCertificate",
"lightsail>DeleteContactMethod",
"lightsail>DeleteDistribution",
"lightsail>DeleteDomain",
"lightsail>DeleteDomainEntry",
"lightsail:DetachCertificateFromDistribution",
"lightsail:Get*",
"lightsail:IsVpcPeered",
"lightsail:PutAlarm",
"lightsail:ResetDistributionCache",
"lightsail:SendContactMethodVerification",
"lightsail:SetIpAddressType",
```

```

    "lightsail:TagResource",
    "lightsail:TestAlarm",
    "lightsail:UntagResource",
    "lightsail:UpdateDistribution",
    "lightsail:UpdateDistributionBundle",
    "lightsail:UpdateDomainEntry",
    "logs:*",
    "managedblockchain-query:*",
    "managedblockchain:*",
    "mapcredits:*",
    "notifications:GetManagedNotificationConfiguration",
    "notifications:GetManagedNotificationEvent",
    "notifications:ListManagedNotificationChildEvents",
    "notifications:ListManagedNotificationConfigurations",
    "notifications:ListManagedNotificationEvents",
    "organizations:*",
    "pricing:*",
    "q:*",
    "route53:*",
    "route53domains:*",
    "route53globalresolver:*",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "servicequotas:*",
    "signin:*",
    "sso-directory:*",
    "sso-oauth:*",
    "sso:*",
    "sts:*",
    "support:*",
    "tax:*",
    "trustedadvisor:*",
    "uxc:*",
    "waf:*",
    "wafv2:*"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestedRegion" : "us-east-1"
    }
  }
},
{

```

```

    "Sid" : "DenyUsEast1WafResourceAssociation",
    "Effect" : "Deny",
    "Action" : [
        "wafv2:AssociateWebACL",
        "wafv2:DisassociateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:RequestedRegion" : "us-east-1"
        }
    }
},
{
    "Sid" : "UsWest2Partitional",
    "Effect" : "Deny",
    "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "cloudshell:*",
        "cloudtrail:LookupEvents",
        "health:*",
        "identitystore-auth:*",
        "identitystore:*",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:ListAliases",
        "networkmanager-chat:*",
        "networkmanager:*",
        "route53-recovery-cluster:*",

```

```

        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "servicequotas:*",
        "sso-directory:*",
        "sso-oauth:*",
        "sso:*",
        "support:*",
        "trustedadvisor:*",
        "uxc:*"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:RequestedRegion" : "us-west-2"
        }
    }
},
{
    "Sid" : "RegionFloor",
    "Effect" : "Deny",
    "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringNotEquals" : {
            "aws:RequestedRegion" : [
                "unspecified",
                "us-east-1",
                "selected-region",
                "us-west-2"
            ]
        }
    }
}

```

```

    ]
  }
}
]
}

```

激活高级功能后，以下服务控制策略将应用于您的账户：

```

{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partitional",
      "Effect" : "Deny",
      "NotAction" : [
        "a4b:*",
        "access-analyzer:*",
        "account-access:*",
        "account:*",
        "acm:*",
        "activate:*",
        "artifact:*",
        "aws-marketplace-management:*",
        "aws-marketplace:*",
        "aws-portal:*",
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles",
        "billing:*",
        "billingconductor:*",
        "budgets:*",

```

```
"builderid:*",
"ce:*",
"chatbot:*",
"chime:*",
"cloudfront-keyvaluestore:*",
"cloudfront:*",
"cloudshell:*",
"cloudtrail:LookupEvents",
"cloudwatch:BatchGet*",
"cloudwatch:Describe*",
"cloudwatch:GenerateQuery",
"cloudwatch:Get*",
"cloudwatch:List*",
"compute-optimizer:*",
"config:*",
"consoleapp:*",
"consolidatedbilling:*",
"cost-optimization-hub:*",
"cur:*",
"datapipeline:GetAccountLimits",
"devicefarm:*",
"directconnect:*",
"ec2:DescribeRegions",
"ec2:DescribeTransitGateways",
"ec2:DescribeVpnGateways",
"ecr-public:*",
"fms:*",
"freetier:*",
"globalaccelerator:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"importexport:*",
"invoicing:*",
"iq:*",
"kms:*",
"license-manager:ListReceivedLicenses",
"lightsail:AttachCertificateToDistribution",
"lightsail:CreateCertificate",
"lightsail:CreateContactMethod",
"lightsail:CreateDistribution",
"lightsail:CreateDomain",
"lightsail:CreateDomainEntry",
```

```
"lightsail:DeleteAlarm",
"lightsail:DeleteCertificate",
"lightsail:DeleteContactMethod",
"lightsail:DeleteDistribution",
"lightsail:DeleteDomain",
"lightsail:DeleteDomainEntry",
"lightsail:DetachCertificateFromDistribution",
"lightsail:Get*",
"lightsail:IsVpcPeered",
"lightsail:PutAlarm",
"lightsail:ResetDistributionCache",
"lightsail:SendContactMethodVerification",
"lightsail:SetIpAddressType",
"lightsail:TagResource",
"lightsail:TestAlarm",
"lightsail:UntagResource",
"lightsail:UpdateDistribution",
"lightsail:UpdateDistributionBundle",
"lightsail:UpdateDomainEntry",
"logs:*",
"managedblockchain-query:*",
"managedblockchain:*",
"mapcredits:*",
"mobileanalytics:*",
"networkmanager:*",
"notifications-contacts:*",
"notifications:*",
"organizations:*",
"payments:*",
"pricing:*",
"q:*",
"quicksight:DescribeAccountSubscription",
"resource-explorer-2:*",
"route53-recovery-cluster:*",
"route53-recovery-control-config:*",
"route53-recovery-readiness:*",
"route53:*",
"route53domains:*",
"route53globalresolver:*",
"s3:CreateMultiRegionAccessPoint",
"s3:DeleteMultiRegionAccessPoint",
"s3:DescribeMultiRegionAccessPointOperation",
"s3:GetAccountPublicAccessBlock",
"s3:GetBucketLocation",
```

```

    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetMultiRegionAccessPoint",
    "s3:GetMultiRegionAccessPointPolicy",
    "s3:GetMultiRegionAccessPointPolicyStatus",
    "s3:GetStorageLensConfiguration",
    "s3:GetStorageLensDashboard",
    "s3:ListAllMyBuckets",
    "s3:ListMultiRegionAccessPoints",
    "s3:ListStorageLensConfigurations",
    "s3:PutAccountPublicAccessBlock",
    "s3:PutMultiRegionAccessPointPolicy",
    "savingsplans:*",
    "servicequotas:*",
    "shield:*",
    "signin:*",
    "sso-directory:*",
    "sso-oauth:*",
    "sso:*",
    "sts:*",
    "support:*",
    "supportapp:*",
    "supportplans:*",
    "sustainability:*",
    "tag:GetResources",
    "tax:*",
    "trustedadvisor:*",
    "uxc:*",
    "vendor-insights:ListEntitledSecurityProfiles",
    "waf-regional:*",
    "waf:*",
    "wafv2:*"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestedRegion" : "us-east-1"
    }
  }
},
{
  "Sid" : "UsWest2Partitional",
  "Effect" : "Deny",
  "NotAction" : [

```

```

    "bedrock-mantle:CallWithBearerToken",
    "bedrock-mantle:CreateInference",
    "bedrock-mantle:GetInference",
    "bedrock-mantle:GetModel",
    "bedrock-mantle:ListModels",
    "bedrock:ApplyGuardrail",
    "bedrock:CountTokens",
    "bedrock:GetFoundationModel",
    "bedrock:GetFoundationModelAvailability",
    "bedrock:GetInferenceProfile",
    "bedrock:InvokeModel",
    "bedrock:InvokeModelWithResponseStream",
    "bedrock:ListFoundationModels",
    "bedrock:ListInferenceProfiles",
    "cloudshell:*",
    "cloudtrail:LookupEvents",
    "health:*",
    "identitystore-auth:*",
    "identitystore:*",
    "kms:Decrypt",
    "kms:DescribeKey",
    "kms:ListAliases",
    "networkmanager-chat:*",
    "networkmanager:*",
    "route53-recovery-cluster:*",
    "route53-recovery-control-config:*",
    "route53-recovery-readiness:*",
    "servicequotas:*",
    "sso-directory:*",
    "sso-oauth:*",
    "sso:*",
    "support:*",
    "trustedadvisor:*",
    "uxc:*"
  ],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "aws:RequestedRegion" : "us-west-2"
    }
  }
},
{
  "Sid" : "RegionFloor",

```

```

    "Effect" : "Deny",
    "NotAction" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:CreateInference",
        "bedrock-mantle:GetInference",
        "bedrock-mantle:GetModel",
        "bedrock-mantle:ListModels",
        "bedrock:ApplyGuardrail",
        "bedrock:CountTokens",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListFoundationModels",
        "bedrock:ListInferenceProfiles"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringNotEquals" : {
            "aws:RequestedRegion" : [
                "unspecified",
                "us-east-1",
                "selected-region",
                "us-west-2"
            ]
        }
    }
}
]
}

```

支出限制的服务控制策略

如果您使用支出限额，则当您的项目接近支出限制时，以下服务控制策略将应用于该项目。有关支出限额的更多信息，请参阅[在中创建支出限额 Amazon 设置](#)。

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenyBedrockUsage",
    "Effect": "Deny",
    "Action": [

```

```

    "bedrock:ApplyGuardrail",
    "bedrock:CallWithBearerToken",
    "bedrock:InvokeAgent",
    "bedrock:InvokeAutomatedReasoningPolicy",
    "bedrock:InvokeDataAutomation",
    "bedrock:InvokeDataAutomationAsync",
    "bedrock:InvokeFlow",
    "bedrock:InvokeInlineAgent",
    "bedrock:InvokeModel",
    "bedrock:InvokeModelWithResponseStream",
    "bedrock:InvokeTool",
    "bedrock:OptimizePrompt",
    "bedrock:Retrieve",
    "bedrock:RetrieveAndGenerate",
    "bedrock:StartFlowExecution",
    "bedrock-mantle:CallWithBearerToken",
    "bedrock-mantle:CreateInference"
  ],
  "Resource": "*"
}
}

```

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenyLambdaUsage",
    "Effect": "Deny",
    "Action": [
      "lambda:DeleteFunctionConcurrency",
      "lambda:InvokeAsync",
      "lambda:InvokeFunction",
      "lambda:InvokeFunctionUrl",
      "lambda:PutFunctionConcurrency"
    ],
    "Resource": "*"
  }
}

```

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "DenySageMakerInference",
    "Effect": "Deny",

```

```

    "Action": [
      "sagemaker:InvokeEndpoint",
      "sagemaker:InvokeEndpointAsync",
      "sagemaker:InvokeEndpointWithResponseStream"
    ],
    "Resource": "*"
  }
}

```

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCompute",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateNatGateway",
        "ec2:CreateVolume",
        "ec2:CreateVpnConnection",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "elasticloadbalancing:CreateLoadBalancer",
        "autoscaling:CreateAutoScalingGroup",
        "ecs:CreateService",
        "eks:CreateCluster",
        "eks:CreateNodegroup",
        "eks:CreateFargateProfile",
        "elasticbeanstalk:CreateEnvironment",
        "apprunner:CreateService",
        "apprunner:ResumeService",
        "batch:CreateComputeEnvironment",
        "elasticmapreduce:RunJobFlow",
        "appstream:CreateFleet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyLambda",
      "Effect": "Deny",
      "Action": "lambda:CreateFunction",
      "Resource": "*"
    }
  ]
}

```

```

    "Sid": "DenyDatabase",
    "Effect": "Deny",
    "Action": [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance",
        "rds:RestoreDBClusterFromS3",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:RestoreDBInstanceFromS3",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:StartDBCluster",
        "rds:StartDBInstance",
        "dynamodb:CreateTable",
        "dynamodb:CreateGlobalTable",
        "elasticache:CreateCacheCluster",
        "elasticache:CreateReplicationGroup",
        "timestream:CreateDatabase",
        "timestream:CreateTable",
        "memorydb:CreateCluster",
        "es:CreateDomain",
        "aoss:CreateCollection",
        "redshift:CreateCluster",
        "redshift:ResumeCluster",
        "redshift-serverless:CreateWorkgroup",
        "dsq1:CreateCluster"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyStorage",
    "Effect": "Deny",
    "Action": [
        "elasticfilesystem:CreateFileSystem",
        "datasync:CreateTask",
        "storagegateway:ActivateGateway",
        "glacier:CreateVault"
    ],
    "Resource": "*"
},
{
    "Sid": "DenySageMaker",
    "Effect": "Deny",
    "Action": [

```

```

        "sagemaker:CreateApp",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:StartNotebookInstance"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyBedrock",
    "Effect": "Deny",
    "Action": [
        "bedrock:CreateCustomModelDeployment",
        "bedrock:CreateDataAutomationProject",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreateMarketplaceModelEndpoint",
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateModelImportJob",
        "bedrock:CreateModelInvocationJob",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock-mantle:CreateCustomizedModel",
        "bedrock-mantle:CreateFineTuningJob",
        "bedrock-mantle:CreateReservation"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyAIML",
    "Effect": "Deny",
    "Action": [
        "kendra:CreateIndex",
        "personalize:CreateSolution",
        "personalize:CreateCampaign",
        "forecast:CreatePredictor",
        "forecast:CreateForecast",
        "rekognition:CreateProject",
        "lex:CreateBot"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyNetworking",

```

```

    "Effect": "Deny",
    "Action": [
        "cloudfront:CreateDistribution",
        "route53:CreateHostedZone",
        "appmesh:CreateMesh"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyApiGatewayCreate",
    "Effect": "Deny",
    "Action": "apigateway:POST",
    "Resource": [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/apis"
    ]
},
{
    "Sid": "DenyMessaging",
    "Effect": "Deny",
    "Action": [
        "mq:CreateBroker",
        "kafka:CreateCluster",
        "kafka:CreateVpcConnection",
        "kinesis:CreateStream",
        "firehose:CreateDeliveryStream",
        "kinesisanalytics:CreateApplication",
        "kinesisvideo:CreateStream",
        "sns:CreateTopic",
        "sqs:CreateQueue",
        "events:CreateEventBus",
        "pipes:CreatePipe",
        "scheduler:CreateSchedule"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyAnalytics",
    "Effect": "Deny",
    "Action": [
        "states:CreateStateMachine",
        "glue:CreateJob",
        "glue:CreateCrawler",
        "athena:CreateWorkGroup",

```

```

        "appsync:CreateGraphQLApi",
        "appflow:CreateFlow",
        "datazone:CreateDomain",
        "datazone:CreateProject",
        "entityresolution:CreateMatchingWorkflow",
        "datapipeline:CreatePipeline",
        "dataexchange:CreateDataSet"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyDevTools",
    "Effect": "Deny",
    "Action": [
        "amplify:CreateApp",
        "amplify:CreateBranch",
        "cloud9:CreateEnvironmentEC2",
        "codebuild:CreateProject",
        "codepipeline:CreatePipeline",
        "codedeploy:CreateApplication",
        "cloudformation:CreateStack",
        "cloudformation:CreateStackSet",
        "codeartifact:CreateRepository",
        "codeartifact:CreateDomain"
    ],
    "Resource": "*"
},
{
    "Sid": "DenySecurity",
    "Effect": "Deny",
    "Action": [
        "kms:CreateKey",
        "wafv2:CreateWebACL",
        "cloudhsm:CreateCluster",
        "network-firewall:CreateFirewall",
        "secretsmanager:CreateSecret",
        "acm-pca:CreateCertificateAuthority",
        "cognito-idp:CreateUserPool",
        "cognito-identity:CreateIdentityPool",
        "ds:CreateDirectory",
        "ds:CreateMicrosoftAD",
        "fms:PutPolicy",
        "payment-cryptography:CreateKey"
    ],

```

```

    "Resource": "*"
  },
  {
    "Sid": "DenyMedia",
    "Effect": "Deny",
    "Action": [
      "medialive:CreateChannel",
      "mediapackage:CreateChannel",
      "mediaconnect:CreateFlow",
      "mediatailor:CreateChannel"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DenyIoT",
    "Effect": "Deny",
    "Action": [
      "iot:CreateThing",
      "iot:CreateTopicRule",
      "iotevents:CreateDetectorModel",
      "iottwinmaker:CreateWorkspace",
      "iotsitewise:CreateAssetModel",
      "iotsitewise:CreatePortal",
      "iotfleetwise:CreateCampaign"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DenyMisc",
    "Effect": "Deny",
    "Action": [
      "ses:CreateConfigurationSet",
      "ecr:CreateRepository",
      "aps:CreateWorkspace",
      "healthlake:CreateFHIRDatastore",
      "transfer:CreateServer",
      "managedblockchain:CreateNetwork",
      "managedblockchain:CreateMember",
      "route53-recovery-control-config:CreateCluster",
      "fis:CreateExperimentTemplate",
      "appfabric:CreateAppBundle",
      "appfabric:CreateIngestion",
      "b2bi:CreateProfile",
      "b2bi:CreateTransformer",

```

```

        "geo:CreateMap",
        "geo:CreatePlaceIndex",
        "geo:CreateTracker",
        "geo:CreateGeofenceCollection",
        "geo:CreateRouteCalculator"
    ],
    "Resource": "*"
}
]
}

```

项目免费套餐的服务控制策略

以下服务控制策略控制对我们新 Amazon 体验免费套餐中可用 Amazon 服务的访问权限。此策略无法修改。要访问其他服务，请升级您的帐户。有关更多信息，请参阅 [在中升级您的账户 Amazon 设置](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFreeTierServices",
      "Effect": "Deny",
      "NotAction": [
        "a2c:*",
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:ValidatePolicy",
        "account:*",
        "acm:*",
        "aco-automation:*",
        "action-recommendations:*",
        "activate:*",
        "aiops:*",
        "airflow-serverless:*",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "aoss:*",
        "apigateway:*",
        "app-integrations:*",
        "appconfig:*",
        "appflow:*",

```

```
"application-autoscaling:*",
"application-signals-mcp:*",
"application-signals:*",
"application-transformation:*",
"applicationinsights:*",
"appmesh:*",
"appsync:*",
"aps:*",
"arc-zonal-shift:*",
"artifact:*",
"athena:*",
"autoscaling-plans:*",
"autoscaling:*",
"aws-external-anthropic:*",
"aws-marketplace:*",
"b2bi:*",
"backup-gateway:*",
"backup-search:*",
"backup-storage:*",
"backup:*",
"batch:*",
"bcm-pricing-calculator:*",
"bedrock-agentcore:*",
"bedrock-mantle:*",
"bedrock-websearch:*",
"bedrock:*",
"budgets:*",
"ce:*",
"chatbot:*",
"cloud9:*",
"cloudformation:*",
"cloudfront-keyvaluestore:*",
"cloudfront:*",
"cloudshell:*",
"cloudtrail-data:*",
"cloudtrail:*",
"cloudwatch:*",
"codeartifact:*",
"codebuild:*",
"codecommit:*",
"codeconnections:*",
"codedeploy-commands-secure:*",
"codedeploy:*",
"codepipeline:*",
```

```
"codestar-connections:*",
"codestar-notifications:*",
"cognito-identity:*",
"cognito-idp:*",
"cognito-sync:*",
"compute-optimizer:*",
"config:*",
"consoleapp:*",
"consolidatedbilling:*",
"cost-optimization-hub:*",
"customer-verification:*",
"databrew:*",
"datapipeline:*",
"datasync:*",
"datazone:*",
"dbqms:*",
"dlm:*",
"ds-data:*",
"ds:*",
"dsql:*",
"dynamodb:*",
"ebs:*",
"ec2-instance-connect:*",
"ec2:*",
"ec2messages:*",
"ecr-public:*",
"ecr:*",
"ecs-mcp:*",
"ecs:*",
"eks-auth:*",
"eks-mcp:*",
"eks:*",
"elasticache:*",
"elasticbeanstalk:*",
"elasticfilesystem:*",
"elasticloadbalancing:*",
"entityresolution:*",
"es:*",
"events:*",
"evidently:*",
"execute-api:*",
"finops-agent:*",
"freertos:*",
"freetier:*,
```

```
"geo-maps:*",
"geo-places:*",
"geo-routes:*",
"geo:*",
"glue:*",
"groundtruthlabeling:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"imagebuilder:*",
"internetmonitor:*",
"invoicing:*",
"iot-device-tester:*",
"iot:*",
"iotdeviceadvisor:*",
"iotfleethub:*",
"iotjobsdata:*",
"iotmanagedintegrations:*",
"iotsitewise:*",
"iottwinmaker:*",
"iotwireless:*",
"kms:*",
"lakeformation:*",
"lambda:*",
"launchwizard:*",
"lex:*",
"license-manager-linux-subscriptions:*",
"license-manager-user-subscriptions:*",
"license-manager:*",
"logs:*",
"mgn:*",
"migrationhub-orchestrator:*",
"migrationhub-strategy:*",
"mpa:*",
"mq:*",
"networkflowmonitor:*",
"networkmanager-chat:*",
"networkmanager:*",
"networkmonitor:*",
"notifications-contacts:*",
"notifications:*",
"nova-act:*",
"oam:*",
```

```
"observabilityadmin:*",
"opensearch:*",
"organizations:*",
"osis:*",
"payment-cryptography:*",
"pi:*",
"pipes:*",
"polly:*",
"pricing:*",
"q:DeleteConversation",
"q:GenerateCodeFromCommands",
"q:GenerateCodeRecommendations",
"q:GetConversation",
"q:GetIdentityMetadata",
"q:GetTroubleshootingResults",
"q:ListConversations",
"q:PassRequest",
"q:SendEvent",
"q:SendMessage",
"q:StartConversation",
"q:StartTroubleshootingAnalysis",
"q:StartTroubleshootingResolutionExplanation",
"q:UpdateConversation",
"q:UpdateTroubleshootingCommandResult",
"q:UsePlugin",
"ram:*",
"rbin:*",
"rds-data:*",
"rds-db:*",
"rds:*",
"rekognition:*",
"resource-explorer-2:*",
"resource-explorer:*",
"resource-groups:*",
"rhelkb:*",
"route53-recovery-cluster:*",
"route53-recovery-control-config:*",
"route53-recovery-readiness:*",
"route53:*",
"route53domains:*",
"route53globalresolver:*",
"route53profiles:*",
"route53resolver:*",
"rum:*",
```

```
"s3-object-lambda:*",
"s3:*",
"s3express:*",
"s3files:*",
"s3tables:*",
"s3vectors:*",
"sagemaker-data-science-assistant:*",
"sagemaker-geospatial:*",
"sagemaker-mlflow:*",
"sagemaker-unified-studio-mcp:*",
"sagemaker:*",
"scheduler:*",
"schemas:*",
"secretsmanager:*",
"serverlessrepo:*",
"servicecatalog:Describe*",
"servicecatalog:List*",
"servicecatalog:ProvisionProduct",
"servicecatalog:ScanProvisionedProducts",
"servicecatalog:SearchProducts",
"servicecatalog:SearchProvisionedProducts",
"servicecatalog:TerminateProvisionedProduct",
"servicecatalog:UpdateProvisionedProduct",
"servicediscovery:*",
"serviceextract:*",
"servicequotas:*",
"ses:*",
"signer:*",
"signin:*",
"sns:*",
"sqlworkbench:*",
"sqs:*",
"ssm-contacts:*",
"ssm-guiconnect:*",
"ssm-incidents:*",
"ssm-quicksetup:*",
"ssm-sap:*",
"ssm:*",
"ssmmessages:*",
"sso-directory:*",
"sso-oauth:*",
"sso:*",
"states:*",
"sts:*,
```

```

        "support:*",
        "swf:*",
        "synthetics:*",
        "tag:*",
        "tax:*",
        "timestream-influxdb:*",
        "ts:*",
        "uxc:*",
        "verifiedpermissions:*",
        "vpce:*",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "wellarchitected:*",
        "xray:*"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyEC2CapacityBlock",
    "Effect": "Deny",
    "Action": ["ec2:PurchaseCapacityBlock", "ec2:PurchaseCapacityBlockExtension"],
    "Resource": "*"
},
{
    "Sid": "DenyRestrictedAgreements",
    "Effect": "Deny",
    "Action": ["artifact:AcceptAgreement", "artifact:AcceptNdaForAgreement"],
    "Resource": [
        "arn:aws:artifact::agreement/agreement-9c1kBcYznTkcpRIm",
        "arn:aws:artifact::agreement/agreement-y03aUwMAEorHtqjv",
        "arn:aws:artifact::agreement/agreement-bexgr7sjvXAW4Gxu",
        "arn:aws:artifact::agreement/agreement-HZTdNwJuqOKLReXC"
    ]
},
{
    "Sid": "DenyDocDB",
    "Effect": "Deny",
    "Action": ["rds:CreateDBCluster", "rds:CreateDBInstance"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "rds:DatabaseEngine": ["docdb"]
        }
    }
}

```

```

    }
  },
  {
    "Sid": "DenyCloudWAN",
    "Effect": "Deny",
    "Action": [
      "networkmanager:CreateCoreNetwork",
      "networkmanager:CreateConnectAttachment",
      "networkmanager:CreateConnectPeer",
      "networkmanager:CreateVpcAttachment",
      "networkmanager:CreateSiteToSiteVpnAttachment",
      "networkmanager:CreateTransitGatewayPeering",
      "networkmanager:CreateDirectConnectGatewayAttachment",
      "networkmanager:PutCoreNetworkPolicy",
      "networkmanager:ExecuteCoreNetworkChangeSet"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DenyTransitGatewayAndVPN",
    "Effect": "Deny",
    "Action": [
      "ec2:CreateTransitGateway",
      "ec2:CreateTransitGatewayVpcAttachment",
      "ec2:CreateTransitGatewayConnect",
      "ec2:CreateTransitGatewayConnectPeer",
      "ec2:CreateTransitGatewayMulticastDomain",
      "ec2:CreateTransitGatewayPeeringAttachment",
      "ec2:CreateTransitGatewayPolicyTable",
      "ec2:CreateTransitGatewayPrefixListReference",
      "ec2:CreateTransitGatewayRoute",
      "ec2:CreateTransitGatewayRouteTable",
      "ec2:CreateTransitGatewayRouteTableAnnouncement",
      "ec2:CreateClientVpnEndpoint",
      "ec2:CreateClientVpnRoute",
      "ec2:AuthorizeClientVpnIngress",
      "ec2:AssociateClientVpnTargetNetwork",
      "ec2:CreateVpnConnection",
      "ec2:CreateVpnConnectionRoute",
      "ec2:CreateVpnGateway",
      "ec2:CreateCustomerGateway"
    ],
    "Resource": "*"
  },

```

```

{
  "Sid": "DenySageMakerGroundTruth",
  "Effect": "Deny",
  "Action": [
    "sagemaker:CreateLabelingJob",
    "sagemaker:CreateWorkteam",
    "sagemaker:CreateWorkforce",
    "sagemaker:CreateHumanTaskUi"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyGlacierStorageClasses",
  "Effect": "Deny",
  "Action": ["s3:PutObject"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "s3:x-amz-storage-class": ["DEEP_ARCHIVE", "GLACIER"]
    }
  }
},
{
  "Sid": "DenyEC2Fleet",
  "Effect": "Deny",
  "Action": ["ec2:CreateFleet"],
  "Resource": "*"
},
{
  "Sid": "DenyEC2BYOLAndLicenseConfigurations",
  "Effect": "Deny",
  "Action": ["ec2:RunInstances", "ec2:StartInstances"],
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "StringEquals": {
      "ec2:Tenancy": "host"
    }
  }
},
{
  "Sid": "DenyEC2InstanceStoreRootDevice",
  "Effect": "Deny",
  "Action": ["ec2:RunInstances"],
  "Resource": "arn:aws:ec2:*:*:instance/*",

```

```

    "Condition": {
      "StringEquals": {
        "ec2:RootDeviceType": "instance-store"
      }
    },
  },
  {
    "Sid": "DenyLicenseManagerAssociation",
    "Effect": "Deny",
    "Action": ["license-manager:CreateLicenseConfiguration"],
    "Resource": "*"
  },
  {
    "Sid": "DenyIAMRestrictedActions",
    "Effect": "Deny",
    "Action": [
      "iam:*Alias*",
      "iam:*Organizations*",
      "iam:*Provider*",
      "iam:SetSecurityTokenServicePreferences",
      "iam:*LoginProfile*",
      "iam:CreateGroup",
      "iam:AttachGroupPolicy",
      "iam:AddUserToGroup",
      "iam:PutGroupPolicy",
      "iam:UpdateGroup",
      "iam:UpdateServerCertificate",
      "iam:UpdateSigningCertificate",
      "iam:UploadServerCertificate",
      "iam:UploadSigningCertificate",
      "iam:TagServerCertificate",
      "iam:UntagServerCertificate"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DenySSOCreateInstance",
    "Effect": "Deny",
    "Action": ["sso:CreateInstance"],
    "Resource": "*"
  },
  {
    "Sid": "DenyRequestSpotInstances",
    "Effect": "Deny",

```

```

    "Action": ["ec2:RequestSpotInstances"],
    "Resource": "*"
  },
  {
    "Sid": "DenySpotMarketType",
    "Effect": "Deny",
    "Action": ["ec2:RunInstances"],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "ec2:InstanceMarketType": "spot"
      }
    }
  },
  {
    "Sid": "DenyReservedInstanceAndCapacityPurchases",
    "Effect": "Deny",
    "Action": [
      "athena:CreateCapacityReservation",
      "cloudfront:CreateSavingsPlan",
      "dynamodb:PurchaseReservedCapacityOfferings",
      "ec2:AllocateHosts",
      "ec2:CreateCapacityReservation",
      "ec2:CreateCapacityReservationBySplitting",
      "ec2:CreateCapacityReservationCancellationQuote",
      "ec2:CreateCapacityReservationFleet",
      "ec2:PurchaseHostReservation",
      "ec2:PurchaseReservedInstancesOffering",
      "ec2:PurchaseScheduledInstances",
      "elasticache:PurchaseReservedCacheNodesOffering",
      "es:PurchaseReservedElasticsearchInstanceOffering",
      "es:PurchaseReservedInstanceOffering",
      "glacier:PurchaseProvisionedCapacity",
      "memorydb:PurchaseReservedNodesOffering",
      "rds:PurchaseReservedDBInstancesOffering",
      "redshift:AcceptReservedNodeExchange",
      "redshift:PurchaseReservedNodeOffering",
      "sagemaker:CreateReservedCapacity",
      "savingsplans:CreateSavingsPlan"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DenyExportableCertificateRequests",

```

```

    "Effect": "Deny",
    "Action": ["acm:RequestCertificate"],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "acm:AllowExport": "true"
      }
    }
  }
]
}

```

项目付费计划的服务控制政策

以下服务控制政策控制对我们新 Amazon 体验的付费计划中提供的 Amazon 服务的访问权限。此政策无法修改。要访问其他服务，请激活高级功能。有关更多信息，请参阅 [激活高级 Amazon 功能](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPaidTierServices",
      "Effect": "Deny",
      "NotAction": [
        "a2c:*",
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:ValidatePolicy",
        "account:*",
        "acm:*",
        "aco-automation:*",
        "action-recommendations:*",
        "activate:*",
        "aidevops:*",
        "aiops:*",
        "airflow-serverless:*",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "aoss:*",
        "apigateway:*",
        "app-integrations:*",

```

```
"appconfig:*",
"appfabric:*",
"appflow:*",
"application-autoscaling:*",
"application-signals-mcp:*",
"application-signals:*",
"application-transformation:*",
"applicationinsights:*",
"appmesh:*",
"appsync:*",
"aps:*",
"arc-zonal-shift:*",
"artifact:*",
"athena:*",
"autoscaling-plans:*",
"autoscaling:*",
"aws-external-anthropic:*",
"aws-marketplace:*",
"b2bi:*",
"backup-gateway:*",
"backup-search:*",
"backup-storage:*",
"backup:*",
"batch:*",
"bcm-pricing-calculator:*",
"bedrock-agentcore:*",
"bedrock-mantle:*",
"bedrock-websearch:*",
"bedrock:*",
"budgets:*",
"ce:*",
"chatbot:*",
"cloud9:*",
"cloudformation:*",
"cloudfront-keyvaluestore:*",
"cloudfront:*",
"cloudshell:*",
"cloudtrail-data:*",
"cloudtrail:*",
"cloudwatch:*",
"codeartifact:*",
"codebuild:*",
"codecommit:*",
"codeconnections:*",
```

```
"codedeploy-commands-secure:*",
"codedeploy:*",
"codeguru-profiler:*",
"codeguru-reviewer:*",
"codeguru-security:*",
"codepipeline:*",
"codestar-connections:*",
"codestar-notifications:*",
"cognito-identity:*",
"cognito-idp:*",
"cognito-sync:*",
"compute-optimizer:*",
"config:*",
"consoleapp:*",
"consolidatedbilling:*",
"cost-optimization-hub:*",
"customer-verification:*",
"databrew:*",
"dataexchange:*",
"datapipeline:*",
"datasync:*",
"datazone:*",
"dbqms:*",
"devops-guru:*",
"dlm:*",
"docdb-elastic:*",
"ds-data:*",
"ds:*",
"dsql:*",
"dynamodb:*",
"ebs:*",
"ec2-instance-connect:*",
"ec2:*",
"ec2messages:*",
"ecr-public:*",
"ecr:*",
"ecs-mcp:*",
"ecs:*",
"eks-auth:*",
"eks-mcp:*",
"eks:*",
"elasticache:*",
"elasticbeanstalk:*",
"elasticfilesystem:*
```

```
"elasticloadbalancing:*",
"elasticmapreduce:*",
"emr-containers:*",
"emr-serverless:*",
"entityresolution:*",
"es:*",
"events:*",
"evidently:*",
"execute-api:*",
"finops-agent:*",
"firehose:*",
"fis:*",
"fms:*",
"forecast:*",
"freertos:*",
"freetier:*",
"geo-maps:*",
"geo-places:*",
"geo-routes:*",
"geo:*",
"glacier:*",
"glue:*",
"groundtruthlabeling:*",
"health:*",
"iam:*",
"identitystore-auth:*",
"identitystore:*",
"imagebuilder:*",
"internetmonitor:*",
"invoicing:*",
"iot-device-tester:*",
"iot:*",
"iotdeviceadvisor:*",
"iotfleethub:*",
"iotjobsdata:*",
"iotmanagedintegrations:*",
"iotsitewise:*",
"iottwinmaker:*",
"iotwireless:*",
"kafka-cluster:*",
"kafka:*",
"kafkaconnect:*",
"kinesis:*",
"kinesisanalytics:*",
```

```
"kinesisvideo:*",
"kms:*",
"lakeformation:*",
"lambda:*",
"launchwizard:*",
"lex:*",
"license-manager-linux-subscriptions:*",
"license-manager-user-subscriptions:*",
"license-manager:*",
"logs:*",
"managedblockchain-query:*",
"managedblockchain:*",
"mapcredits:*",
"memorydb:*",
"mgn:*",
"migrationhub-orchestrator:*",
"migrationhub-strategy:*",
"mpa:*",
"mq:*",
"neptune-db:*",
"neptune-graph:*",
"network-firewall:*",
"networkflowmonitor:*",
"networkmanager-chat:*",
"networkmanager:*",
"networkmonitor:*",
"notifications-contacts:*",
"notifications:*",
"nova-act:*",
"oam:*",
"observabilityadmin:*",
"opensearch:*",
"organizations:*",
"osis:*",
"payment-cryptography:*",
"personalize:*",
"pi:*",
"pipes:*",
"polly:*",
"pricing:*",
"q:DeleteConversation",
"q:GenerateCodeFromCommands",
"q:GenerateCodeRecommendations",
"q:GetConversation",
```

```
"q:GetIdentityMetadata",
"q:GetTroubleshootingResults",
"q:ListConversations",
"q:PassRequest",
"q:SendEvent",
"q:SendMessage",
"q:StartConversation",
"q:StartTroubleshootingAnalysis",
"q:StartTroubleshootingResolutionExplanation",
"q:UpdateConversation",
"q:UpdateTroubleshootingCommandResult",
"q:UsePlugin",
"ram:*",
"rbin:*",
"rds-data:*",
"rds-db:*",
"rds:*",
"redshift-data:*",
"redshift-serverless:*",
"redshift:*",
"rekognition:*",
"resource-explorer-2:*",
"resource-explorer:*",
"resource-groups:*",
"rhelkb:*",
"route53-recovery-cluster:*",
"route53-recovery-control-config:*",
"route53-recovery-readiness:*",
"route53:*",
"route53domains:*",
"route53globalresolver:*",
"route53profiles:*",
"route53resolver:*",
"rum:*",
"s3-object-lambda:*",
"s3:*",
"s3express:*",
"s3files:*",
"s3tables:*",
"s3vectors:*",
"sagemaker-data-science-assistant:*",
"sagemaker-geospatial:*",
"sagemaker-mlflow:*",
"sagemaker-unified-studio-mcp:*,
```

```
"sagemaker:*",
"scheduler:*",
"schemas:*",
"secretsmanager:*",
"securityagent:*",
"serverlessrepo:*",
"servicecatalog:Describe*",
"servicecatalog:List*",
"servicecatalog:ProvisionProduct",
"servicecatalog:ScanProvisionedProducts",
"servicecatalog:SearchProducts",
"servicecatalog:SearchProvisionedProducts",
"servicecatalog:TerminateProvisionedProduct",
"servicecatalog:UpdateProvisionedProduct",
"servicediscovery:*",
"serviceextract:*",
"servicequotas:*",
"ses:*",
"signer:*",
"signin:*",
"sms-voice:*",
"sns:*",
"social-messaging:*",
"sqlworkbench:*",
"sqs:*",
"ssm-contacts:*",
"ssm-guiconnect:*",
"ssm-incidents:*",
"ssm-quicksetup:*",
"ssm-sap:*",
"ssm:*",
"ssmmessages:*",
"sso-directory:*",
"sso-oauth:*",
"sso:*",
"states:*",
"storagegateway:*",
"sts:*",
"support:*",
"swf:*",
"synthetics:*",
>tag:*",
"tax:*",
"textract:*",
```

```

        "timestream-influxdb:*",
        "timestream:*",
        "transcribe:*",
        "translate:*",
        "ts:*",
        "uxc:*",
        "verifiedpermissions:*",
        "vpce:*",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "wellarchitected:*",
        "xray:*"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyEC2CapacityBlock",
    "Effect": "Deny",
    "Action": ["ec2:PurchaseCapacityBlock", "ec2:PurchaseCapacityBlockExtension"],
    "Resource": "*"
},
{
    "Sid": "DenyRestrictedAgreements",
    "Effect": "Deny",
    "Action": ["artifact:AcceptAgreement", "artifact:AcceptNdaForAgreement"],
    "Resource": [
        "arn:aws:artifact::agreement/agreement-9c1kBcYznTkcpRIIm",
        "arn:aws:artifact::agreement/agreement-y03aUwMAEorHtqjv",
        "arn:aws:artifact::agreement/agreement-bexgr7sjvXAW4Gxu",
        "arn:aws:artifact::agreement/agreement-HZTdNwJuqOKLReXC"
    ]
},
{
    "Sid": "DenyCloudWAN",
    "Effect": "Deny",
    "Action": [
        "networkmanager:CreateCoreNetwork",
        "networkmanager:CreateConnectAttachment",
        "networkmanager:CreateConnectPeer",
        "networkmanager:CreateVpcAttachment",
        "networkmanager:CreateSiteToSiteVpnAttachment",
        "networkmanager:CreateTransitGatewayPeering",
        "networkmanager:CreateDirectConnectGatewayAttachment",
    ]
}

```

```

        "networkmanager:PutCoreNetworkPolicy",
        "networkmanager:ExecuteCoreNetworkChangeSet"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyTransitGatewayAndVPN",
    "Effect": "Deny",
    "Action": [
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayConnect",
        "ec2:CreateTransitGatewayConnectPeer",
        "ec2:CreateTransitGatewayMulticastDomain",
        "ec2:CreateTransitGatewayPeeringAttachment",
        "ec2:CreateTransitGatewayPolicyTable",
        "ec2:CreateTransitGatewayPrefixListReference",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:CreateClientVpnEndpoint",
        "ec2:CreateClientVpnRoute",
        "ec2:AuthorizeClientVpnIngress",
        "ec2:AssociateClientVpnTargetNetwork",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:CreateCustomerGateway"
    ],
    "Resource": "*"
},
{
    "Sid": "DenySageMakerGroundTruth",
    "Effect": "Deny",
    "Action": [
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateWorkteam",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateHumanTaskUi"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyEC2Fleet",

```

```

    "Effect": "Deny",
    "Action": ["ec2:CreateFleet"],
    "Resource": "*"
  },
  {
    "Sid": "DenyEC2BYOLAndLicenseConfigurations",
    "Effect": "Deny",
    "Action": ["ec2:RunInstances", "ec2:StartInstances"],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringEquals": {
        "ec2:Tenancy": "host"
      }
    }
  },
  {
    "Sid": "DenyEC2InstanceStoreRootDevice",
    "Effect": "Deny",
    "Action": ["ec2:RunInstances"],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringEquals": {
        "ec2:RootDeviceType": "instance-store"
      }
    }
  },
  {
    "Sid": "DenyLicenseManagerAssociation",
    "Effect": "Deny",
    "Action": ["license-manager:CreateLicenseConfiguration"],
    "Resource": "*"
  },
  {
    "Sid": "DenyIAMRestrictedActions",
    "Effect": "Deny",
    "Action": [
      "iam:*Alias*",
      "iam:*Organizations*",
      "iam:*Provider*",
      "iam:SetSecurityTokenServicePreferences",
      "iam:*LoginProfile*",
      "iam:CreateGroup",
      "iam:AttachGroupPolicy",
      "iam:AddUserToGroup",

```

```

        "iam:PutGroupPolicy",
        "iam:UpdateGroup",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "iam:UploadServerCertificate",
        "iam:UploadSigningCertificate",
        "iam:TagServerCertificate",
        "iam:UntagServerCertificate"
    ],
    "Resource": "*"
},
{
    "Sid": "DenySSOCreateInstance",
    "Effect": "Deny",
    "Action": ["sso:CreateInstance"],
    "Resource": "*"
},
{
    "Sid": "DenyRequestSpotInstances",
    "Effect": "Deny",
    "Action": ["ec2:RequestSpotInstances"],
    "Resource": "*"
},
{
    "Sid": "DenySpotMarketType",
    "Effect": "Deny",
    "Action": ["ec2:RunInstances"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "ec2:InstanceMarketType": "spot"
        }
    }
},
{
    "Sid": "DenyReservedInstanceAndCapacityPurchases",
    "Effect": "Deny",
    "Action": [
        "athena:CreateCapacityReservation",
        "cloudfront:CreateSavingsPlan",
        "dynamodb:PurchaseReservedCapacityOfferings",
        "ec2:AllocateHosts",
        "ec2:CreateCapacityReservation",
        "ec2:CreateCapacityReservationBySplitting",

```

```

        "ec2:CreateCapacityReservationCancellationQuote",
        "ec2:CreateCapacityReservationFleet",
        "ec2:PurchaseHostReservation",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:PurchaseScheduledInstances",
        "elasticache:PurchaseReservedCacheNodesOffering",
        "es:PurchaseReservedElasticsearchInstanceOffering",
        "es:PurchaseReservedInstanceOffering",
        "glacier:PurchaseProvisionedCapacity",
        "memorydb:PurchaseReservedNodesOffering",
        "rds:PurchaseReservedDBInstancesOffering",
        "redshift:AcceptReservedNodeExchange",
        "redshift:PurchaseReservedNodeOffering",
        "sagemaker:CreateReservedCapacity",
        "savingsplans:CreateSavingsPlan"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyExportableCertificateRequests",
    "Effect": "Deny",
    "Action": ["acm:RequestCertificate"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "acm:AllowExport": "true"
        }
    }
}
]
}

```

项目的资源控制政策

以下是[项目中资源的资源控制策略](#)。此政策无法修改：

```

{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Sid" : "DenyAnyoneOutsideMyOrgAndAWS",
            "Effect" : "Deny",
            "Principal" : "*",

```

```

    "Action" : [
      "aoss:*",
      "appconfig:*",
      "appstream:*",
      "autoscaling:*",
      "codebuild:*",
      "codecommit:*",
      "cognito-identity:*",
      "cognito-idp:*",
      "comprehend:*",
      "comprehendmedical:*",
      "dax:*",
      "dynamodb:*",
      "ecr:*",
      "health:*",
      "kinesisvideo:*",
      "kms:*",
      "logs:*",
      "s3:*",
      "secretsmanager:*",
      "sqs:*",
      "sts:*",
      "support:*",
      "textract:*",
      "transcribe:*",
      "translate:*"
    ],
    "Resource" : "*",
    "Condition" : {
      "BoolIfExists" : {
        "aws:PrincipalIsAWSService" : "false"
      },
      "Null" : {
        "aws:PrincipalARN" : "false"
      },
      "StringNotEqualsIfExists" : {
        "aws:PrincipalOrgID" : "${aws:ResourceOrgID}"
      }
    }
  },
  {
    "Sid" : "DenyAWSWhenItsNotMyOrgsSourceAccount",
    "Effect" : "Deny",
    "Principal" : "*",

```

```

    "Action" : [
      "aoss:*",
      "appconfig:*",
      "appstream:*",
      "autoscaling:*",
      "codebuild:*",
      "codecommit:*",
      "cognito-identity:*",
      "cognito-idp:*",
      "comprehend:*",
      "comprehendmedical:*",
      "dax:*",
      "dynamodb:*",
      "ecr:*",
      "health:*",
      "kinesisvideo:*",
      "kms:*",
      "logs:*",
      "s3:*",
      "secretsmanager:*",
      "sqs:*",
      "sts:*",
      "support:*",
      "textract:*",
      "transcribe:*",
      "translate:*"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "aws:SourceAccount" : "false"
      },
      "StringNotEquals" : {
        "aws:SourceOrgID" : "${aws:ResourceOrgID}"
      }
    }
  }
}
]
}

```

在项目之间切换

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

一次只能管理一个项目的 Amazon 资源。你可以随时根据 Amazon 控制台右上角的名称分辨出你在哪个项目中。

在项目之间切换以获取活动会话 Amazon Web Services 管理控制台

要在项目之间切换活动会话，请从 Amazon Web Services 管理控制台

1. 打开 [Amazon Web Services 管理控制台](#)。
2. 在右上角选择您的项目名称 Amazon Web Services 管理控制台。
3. 选择“切换项目”。
4. 在“活动会话”下，选择一个活动会话。活动会话是指登录时间最长 12 小时的会话。无法更改活动会话时间。
5. 您将被重定向到新项目的 Amazon 控制台主页。

在项目之间切换 Amazon 设置

要在项目之间切换 Amazon 设置

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择要访问的项目。
3. 在右上角的导航栏中，选择创建和管理云基础架构。

您将被重定向回新项目 Amazon Web Services 管理控制台 的。

在项目之间切换 Amazon Web Services 管理控制台

要在项目之间切换 Amazon Web Services 管理控制台

1. 打开 [Amazon Web Services 管理控制台](#)。

2. 选择“管理项目”。
3. 在 Amazon “设置” 中，选择要访问的项目。
4. 在右上角的导航栏中，选择创建和管理云基础架构。

您将被重定向回新项目 Amazon Web Services 管理控制台 的。

邀请团队成员进行协作 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以授予团队成员访问您的项目的权限。当您与团队成员共享项目时，您无法控制他们可以访问哪些 Amazon 服务。你和团队成员都有该项目的管理员权限。这意味着，团队成员有权访问适用于您的项目的所有 Amazon 服务。这包括为服务和应用程序创建访问控制。但是，他们无权执行管理或财务操作，例如删除您的项目或修改支出限额。要查看哪个团队成员修改了 Amazon 服务，请参阅[使用监控您的项目 Amazon CloudTrail](#)。

在 Amazon “设置” 中，您和您的团队成员具有不同的访问权限级别。要查看应用于团队成员的 Amazon 托管策略，请参阅[AWSManagedSettingsReadOnlyAccess](#)。要查看应用于项目所有者的 Amazon 托管策略，请参阅[AWSManagedSettingsAdminAccess](#)。

向项目添加团队成员时，请考虑以下几点。

团队成员注意事项

团队成员可以执行以下操作：

- 查看、创建、编辑、删除和修改项目中的 Amazon 资源。
- 访问 Amazon 设置。
- 查看支出限额。
- 申请增加 Amazon 服务的配额。

团队成员无法执行以下操作：

- 退出项目。

- 执行任何 root 操作。有关更多信息，请参阅 [Amazon 项目所有者的操作](#)。
- 邀请团队成员参与项目。
- 管理任何团队成员的权限。
- 从项目中移除任何团队成员。
- 更改项目的名称。
- 设置或更新付款方式。
- 查看或更新账单详情，包括地址或电话号码。
- 查看或更新税务信息。
- 从免费套餐升级到付费套餐。
- 设置或修改每个项目的支出限额。
- 查看每个项目的成本趋势。
- 查看所有项目的总 Amazon 支出。
- 查看和兑换非免费套餐促销积分。
- 查看所有积分类型的剩余积分和到期日期。
- 查看完整的信用记录，包括已获得、应用和过期的积分。
- 查看积分如何跨项目使用。
- 查看未清余额。
- 向... 执行付款 Amazon。
- 下载发票或查看过去的交易。
- 验证 Amazon 费用是否正确，包括已使用的积分。
- 接收管理账户级别的账单通信。
- 在组织层面获取有关账单问题的帮助。
- 申请增加账户和账单配额的配额。

团队成员如何访问您的 Amazon 资源

我们的新 Amazon 体验为组织创建了一个服务相关角色，其中包含您无法修改的所有项目。该角色会定期验证您的团队成员的内部记录是否与您的实际团队成员保持同步。

AWSServiceRoleForAccountAccessManager 服务相关角色信任以下服务代入该角色：

- `account-access.amazonaws.com`

名为的角色权限策略AccountAccessManagerServiceRolePolicy允许账户访问管理员对指定资源完成以下操作：

- 操作：organizations:ListAccounts , organizations:ListAWSServiceAccessForOrganization
启用 "arn:aws:organizations::*:account/o-*/*"

有关更多信息，请参阅[Amazon 账户访问管理器](#)。

邀请团队成员进行协作 Amazon 设置

要邀请团队成员，您可以从 Amazon “设置” 中的 “团队” 页面向他们发送邀请。团队成员有 14 天的时间接受邀请。团队成员必须创建 Amazon 构建者 ID 才能访问您的项目。他们可以使用 “注册 Amazon (新)” 来完成此操作。

邀请团队成员进行协作 Amazon 设置

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择团队。
3. 选择 “邀请新团队成员”。
4. 对于电子邮件，输入电子邮件地址或电子邮件地址列表。用逗号 (,) 或分号 (;) 分隔电子邮件地址。
5. 选择一个或多个项目与新团队成员共享。
6. 选择 Send invitation (发送邀请)。

如果您的团队成员没有收到邀请，请他们查看垃圾邮件和垃圾文件夹。

邀请团队成员加入中的项目 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以邀请团队成员访问项目。有关团队成员可以在项目中执行哪些操作的信息，请参阅[邀请团队成员进行协作 Amazon 设置](#)。

邀请团队成员加入项目

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择要访问的项目。
3. 对于“成员”，选择“邀请新的团队成员”。
4. 在“电子邮件”中，输入电子邮件地址或电子邮件地址列表。用逗号 (,) 或分号 (;) 分隔电子邮件地址。
5. 选择要与新团队成员共享的项目。
6. 选择 Send invitation (发送邀请)。

如果您的团队成员没有收到邀请，请他们查看垃圾邮件和垃圾文件夹。

从中的项目中移除团队成员 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以随时从项目中移除团队成员。你的团队成员不能自己做这件事。当您移除团队成员时，他们将无法再访问该项目。您的团队成员创建的所有资源都将保留在您的项目中，您必须对其进行管理。

从项目中删除团队成员

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择要访问的项目。
3. 在“成员”选项卡中，选择要从项目中移除的成员，然后选择“移除”。
4. 确认您的选择，然后选择“删除”。

该团队成员仍是您团队的一员，您可以将他们添加到其他项目中。要从 Amazon “设置” 中完全移除团队成员，请参阅[在中移除团队成员 Amazon 设置](#)。

在中移除团队成员 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以使用团队页面从所有项目中移除团队成员。他们将自动失去对任何项目的访问权限。团队成员创建的任何资源都不会被删除。

移除团队成员

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择团队。
3. 选中要移除的团队成员对应的复选框。
4. 选择移除。
5. 确认您的选择，然后选择“移除”。

在中撤消对团队成员的邀请 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以撤消待处理的邀请。邀请将在 Amazon 设置中保留 14 天。当您撤消待处理的邀请时，邀请电子邮件中的访问链接将被禁用。你不能撤消已接受的邀请，而是移除该团队成员。有关更多信息，请参阅 [在中移除团队成员 Amazon 设置](#)。

撤销邀请

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择团队。
3. 选中收到待处理邀请的团队成员对应的复选框。
4. 选择撤销。
5. 确认您的选择，然后选择“撤消邀请”。

向中的团队成员重新发送邀请 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以重新向团队成员发送已撤销、过期或被拒绝的邀请的邀请。当您重新发送邀请时，您的团队成员会收到一封新电子邮件，其有效期自您重新发送邀请之日起 14 天。

重新发送邀请

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择团队。
3. 选中邀请已撤销、过期或被拒绝的团队成员对应的复选框。
4. 选择“重新发送”。
5. 确认您的选择，然后选择“重新发送邀请”。

在中升级您的账户 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

当您使用 Sign up for Amazon（新）注册时，您的账户处于免费套餐中。在免费套餐中，您将获得 100 美元的注册积分，并获得高达 100 美元的额外积分。当您的积分用完或者账户超过 6 个月时，你必须升级到付费套餐。您也可以随时升级到付费计划。当您升级到付费计划时，您可以访问中列出的服务 [Amazon Web Services 服务 包含在我们新的付费计划中 Amazon 经历](#)。

升级账户的注意事项

升级到付费计划时，请考虑以下几点：

- 您无法升级单个项目。当您升级账户时，您的所有项目都将升级。
- 升级后，您将获得永久免费服务和短期试用优惠。

- 您有资格获得其他促销积分和折扣。
- 您必须支付超过积分余额的费用。
- 您可以创建支出限额来设置每月为项目支付的最高金额。有关更多信息，请参阅 [在中创建支出限额 Amazon 设置](#)。
- 您不能将任何项目指定为符合 HIPAA 或 SEC 标准的项目。
- 当积分耗尽时，您的账户不会关闭。
- 这不会将您升级到[报名参加 Amazon（高级）](#)。升级账户时，仅支持使用创建的账户的所有功能都[报名参加 Amazon（高级）](#)将不可用。但是，您可以[激活高级 Amazon 功能](#)为您的账户充值。
- 您无法撤消升级过程。

在中升级您的账户 Amazon 设置

升级您的账户

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择计费。
3. 选择 Upgrade。
4. 选择开始。
5. 添加您的付款方式。

根据您的位置，您可能需要提供一些税务信息。

6. 选择“升级账户”。
7. 选择“继续”返回大楼，或选择“设置支出限额”以设置支出限额。有关支出限额的更多信息，请参阅[在中创建支出限额 Amazon 设置](#)。
8. 选择“转到主机”。

您的升级已完成。

在中创建支出限额 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

什么是支出限额？

支出限制使开发人员能够放心 Amazon 使用，因为他们可以在可预测和可控的预算范围内运营。使用支出限额来设定每月为项目支付的最高金额。支出限额在项目级别设置。您可以对某些项目设置支出限额，而对其它项目则不设置支出限额。

如果您在项目中的使用量达到其上限，则会 Amazon 暂停该项目，该项目将停止其资源，这样您的成本将保持在限制范围内。支出限制专为实验、学习和沙盒工作负载而设计。如果您的应用程序产生意想不到的成本，则可以将它们用于生产环境，前提是可以短暂暂时地暂停资源。

任何拥有项目访问权限的人都可以看到支出限制，但只能由项目所有者管理。您必须使用付费套餐才能设置支出限额。有关更多信息，请参阅 [在中升级您的账户 Amazon 设置](#)。

支出限额是一种预[Amazon 算](#)。

设置您的支出限额

您的支出限额是项目税前成本的上限，而不是费用。设置支出限额时，允许的最低金额为20美元或对可能支出的保守估计，以较高者为准。

为什么存在最低限额：达到支出上限是一种颠覆性的体验。存在最低限额是为了使使用量的正常变化不太可能导致达到支出上限。

保守估计值是如何计算的：该估计值基于您本月迄今为止的活动，但这不是严格的线性外推。Amazon 查看您迄今为止的支出以及您当前正在运行的资源。Amazon 还会使用你前一个月的活动——如果该值很高，则变为最低限度。

如果你有许多资源在运行：对你可能的支出的保守估计会很高。如果要设置较低的支出限额，则需要先停止这些资源。

如果您要重新激活已暂停的项目：对可能支出的保守估计是该月迄今为止的支出加上未收取的任何使用量。

Note

支出限额不包括抵免额，适用于税前费用。

通知

当实际费用达到限额的 50%、75% 和 90% 时，或者您有望在未来 10 天内达到或超过支出限额时，您会收到通知。

使用可选的早期费用控制来自定义您的支出限额设置

您的支出限额可防止您的账单增长超过您设定的金额。如果您的使用量达到该值，则会 Amazon 暂停您的资源以保护您。这些可选控件的作用更早、更温和，因此您可以保持在极限以下。

停止创建新资源

在你达到上限前大约 7 天，新资源就会停止启动。这是通过应用由管理的服务控制策略来实现的 Amazon。服务控制策略取决于服务。要查看可能应用于您的项目的所有服务控制策略，请参阅[支出限制的服务控制政策](#)。

所有已在运行的资源都将保持运行状态。在大多数情况下，您构建的任何内容都不会受到影响。但是，在某些情况下，这可能会导致破坏性体验。例如，如果您启用了自动缩放，并且满足了执行此操作的条件，则不会启动新实例。

暂停闲置资源

在您达到上限前大约 5 天，闲置资源已暂停。您的活动应用程序会继续运行。空闲资源将根据 Comp Amazon ute Optimizer 的建议暂停。有关更多信息，请参阅[查看闲置建议](#)。

您还可以通过登录项目并查看节省机会来查看闲置资源建议。有关更多信息，请参阅[成本优化中心](#)。目前，作为您的支出限制体验的一部分，我们将自动暂停 EC2、RDS 和 SageMaker 终端节点。

为什么我们暂停 EC2 实例：如果过去 14 天内 CPU 利用率峰值低于 5%，并且您的网络每天低 I/O 于 5 MB，我们会暂停 EC2 实例。

如果您有 G 或 P 实例类型，则会有不同的空闲标准。如果过去 14 天内符合以下条件，则 G 或 P 实例类型将被暂停：

- GPU 在 99% 以上的回顾期内没有积极地发挥作用
- GPU 编码器在实例的 99% 或以上的运行时内未得到使用
- 实例级别的 GPU 内存使用率低于 5%
- CPU 最大利用率低于 5%
- 网络利用率低于 5 MB/day

为什么我们暂停 RDS 数据库：如果数据库实例不是只读副本，并且在过去 14 天内有以下情况，我们会暂停适用于 MySQL 的 RDS 和 PostgreSQL 的 RDS：

- 没有数据库连接
- CPU 使用率低
- 低 read/write 活性

为什么我们暂停空闲 SageMaker 端点：如果该端点在过去 14 天内调用次数为零，则会暂停 SageMaker 该终端节点。

暂停成本最高的驱动因素

在您达到上限前大约 4 天，您产生活跃资源的最高费用已暂停。这可能是一种颠覆性的体验。目前，我们从以下五种服务中选择资源：EC2、RDS、Lambda、Bedrock 和 SageMaker。如果您的 Lambda 失控或意外的 Bedrock 峰值，这种选择加入控制可能会防止您产生成本。

如果你达到极限会发生什么

Amazon 暂停您的项目并停止所有资源。将会保留您的数据。

要重新激活您的项目，请从 Amazon “设置” 中提高支出限额。重新激活后，可能需要手动重新启动某些资源。

Important

如果您在项目暂停后的 90 天内未采取任何行动，则会 Amazon 永久删除您的项目数据。

其他需要注意的重要事项

- 如果您使用亚马逊 Route 53，则每 24 小时只能购买一个域名。您必须确保域名费用在支出限额之内，否则，您的域名购买将无法通过。在这种情况下，您必须在购买前提高支出限额。
- 您最多可以将支出限制应用于 10 个项目。

在中创建支出限额 Amazon 设置

要在中创建支出限额 Amazon 设置

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择账单。
3. 在按项目计算的成本中，对于支出限制，选择为项目设置限制。
4. 您可以选择推荐的支出限额或自定义限额。
5. 如果您选择自定义限额，请输入自定义限额。
6. 选择“设置支出限额”。
7. 要通过早期成本控制来自定义支出限额，您可以选择停止新资源启动、暂停闲置资源或暂停最高成本驱动因素。
8. 选择“保存早期成本控制”。

支出限制将立即生效。

在中更新支出限额 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

项目所有者可以随时在 Amazon “设置” 中更新支出限额。您可以增加或减少支出限额，也可以更改可选的早期成本控制。如果由于接近上限而阻止 Amazon 了新资源启动或暂停了资源，则可以提高支出限额。如果您的项目因达到限额而暂停，请提高支出限额以重新激活项目。有关支出限额如何运作的更多信息，请参阅[在中创建支出限额 Amazon 设置](#)。

在中更新支出限额 Amazon 设置

更新支出限额

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择计费。
3. 在按项目划分的成本中，对于支出限额，选择铅笔图标。
4. 对于每月支出限额（美元），输入新的支出限额。

我们会根据您当前的支出提供建议。

5. 要修改要为项目提供哪些保护，请选择“停止新资源启动”、“暂停闲置资源”或“暂停最高成本驱动因素”。
6. 选择保存设置。

支出限额变更将立即生效。

移除中的支出限额 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

项目所有者可以随时在 Amazon “设置” 中删除支出限额。当您取消支出限额后，Amazon 将不再监控您的成本或对项目进行任何早期成本控制。有关支出限额如何运作的更多信息，请参阅[在中创建支出限额 Amazon 设置](#)。

移除中的支出限额 Amazon 设置

移除支出限额

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择计费。
3. 在按项目划分的成本中，对于支出限额，选择铅笔图标。
4. 选择“移除限制”。
5. 确认您的选择，然后选择“移除”。

您的支出限额将立即取消。

我们全新的免费套餐 Amazon 经历

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以使用 Amazon 免费套餐来探索 Amazon 服务，无需承担任何费用。如果您不熟悉 Amazon，无论您的账户计划如何，在创建账户后都将获得 100 美元的信用额度。您还可以通过完成相关活动，在所有项目中额外获得最高 100 美元的服务抵扣金。有关赚取额外服务抵扣金的更多信息，请参阅 [赚取额外积分](#)。此外，您还可以使用 30 多项永久免费 Amazon 服务，这些服务提供每月免费使用限制。

免费账户计划非常适合在长达六个月的时间内免费试用 Amazon 服务和构建概念验证的客户。在此期间，在升级到付费账户计划之前，您不会产生任何费用。您的免费账户计划将在六个月后或您的服务抵扣金用完后（以先到者为准）结束。此外，免费账户计划无法使用某些会迅速消耗全部 Amazon 免费套餐积分金额的 Amazon 服务，也无法使用购买的硬件。有关免费账户计划中符合条件的服务列表，请参阅[注册支持的 Amazon 服务 Amazon（新）](#)。

付费账户计划非常适合构建超出初始服务抵扣金额度的生产应用程序。当您的使用量超过您的积分余额时，或者当您使用不适用积分的服务时，您需要支付标准的即用即付定价。

您拥有的所有项目都属于相同的计划类型。如果您升级到付费账户计划，则您的所有项目都可以使用其他服务，并且您需要为所有项目支付标准的即用即付定价。有关更多信息，请参阅 [Amazon “设置” 中的“升级您的帐户”](#)。

您可以使用成本管理控制台来跟踪您在为项目提供免费套餐的所有 Amazon 服务的使用情况。

跟踪您的免费套餐使用情况

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

Amazon 当您超过每项服务的免费套餐限额的 85% 时，免费套餐使用提醒会自动通过电子邮件通知您。要进行更多跟踪，您可以通过设置零支出预算，将使用量配置为将使用量跟踪到免费套餐限额的 100%。您还可以筛选预算以跟踪每项服务。

您可以通过以下方式跟踪 Amazon 免费套餐的使用情况。

使用 Amazon 设置

您可以在“Amazon 设置”中监控免费账户套餐的到期日期、积分余额和剩余天数。有关更多信息，请参阅 [在中查看和兑换积分 Amazon 设置](#)。您还会定期收到有关您的服务抵扣金余额以及免费账户计划期限即将结束的电子邮件提醒。

如果您有付费套餐，则可以在 Amazon 设置中的积分页面上监控您的积分余额和到期日期。有关升级到付费套餐的更多信息，请参阅[在中升级您的账户 Amazon 设置](#)。

使用账单和成本管理控制台

您可以使用账单和成本管理控制台来跟踪每个项目的免费套餐使用情况。账单和成本管理控制台显示您本月迄今为止的使用情况以及任何达到或高于使用量限制的服务产品的摘要。对于正在使用的每项免费套餐优惠，您可以查看以下内容：

- 该服务
- Amazon 免费套餐的使用限制
- 您当前的使用情况
- 您的预测使用量
- 您的本月至今 (MTD) 实际使用量
- 您的预测月初至今 (MTD) 使用量

以下过程向您展示如何使用账单和成本管理控制台按当月至今的实际使用量对免费套餐使用量进行排序。

对您的免费套餐使用情况进行排序

1. 打开账单与成本管理控制台，网址为 <https://console.aws.amazon.com/cost-management/>。
2. 选择免费套餐。
3. 要按本月至今的实际使用量排序，请选择 MTD 实际使用量百分比。

赚取额外积分

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

如果您是新的 Amazon 客户，通过完成活动，无论您的账户计划如何，您都可以额外获得100美元的积分。这些活动可以帮助您学习 Amazon 服务。您可以在 Amazon Home 控制面板上的“浏览 Amazon”微件中找到这些活动。所有这些活动都将产生 Amazon 服务费，这些费用将从您的 Amazon 免费套餐积分中扣除，但是当您完成每项活动时，您将获得20美元的积分。

待完成的活动

- [使用 Amazon EC2 启动实例](#)

- [在亚马逊基岩游乐场使用基础模型](#)
- [创建预算](#)
- [使用 Lambda 创建 Web 应用程序](#)
- [创建 Amazon RDS 数据库](#)

在中查看您的账单信息 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以使用 Amazon “设置” 查看账单信息。如果您使用的是免费套餐，此页面会显示您有多少天免费套餐以及您的 Amazon 积分。您还可以查看每个项目的成本。如果您使用的是付费计划，则可以查看余额、当前费用和每个项目的成本。如果您使用支出限额，则可以查看与限额相关的信息。你也可以在[在中管理您的付款方式 Amazon 设置](#)和[在中管理税务登记 Amazon 设置](#)。

当您使用免费套餐时，所有使用量均包含在 Amazon 免费套餐积分中。如果您要么耗尽 Amazon 免费套餐积分，要么在 184 天之后（以先发生者为准），则需要升级到付费套餐。有关升级到付费计划的更多信息，请参阅[在中升级您的账户 Amazon 设置](#)。

按项目查看成本

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择计费。
3. 在“按项目划分的成本”下，您将看到本月迄今的费用和预测的本月迄今费用。您将看到项目的所有费用。
4. （可选）要在“检查成本”下查看项目的费用明细，请选择查看。您将被重定向到 Amazon 账单和成本管理控制台。

您在账单和成本管理控制台上看到的 Amazon 账单数据和成本管理器数据每天至少刷新一次。但两者的刷新节奏可能会有所不同，如果您使用支出限额，这可能会导致您在 Amazon 设置和 Amazon 成本管理控制台中本月迄今为止的预估费用出现差异。

在中查看您的账单历史记录 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以在“Amazon 设置”中查看账单历史记录。只有当您有付款方式时，您的账单历史记录才可用。如果您使用免费套餐，则不会看到账单历史记录。

您可以下载在计费期内与您进行交易的每个服务提供商的发票。这包括费用类型、发票日期和以美元计的总额等信息。如果您的账单币种为其他货币，则还会显示该其他货币的总额。发票不分成每个项目。

查看您的账单历史记录

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择计费。
3. 在“余额”旁边，选择“查看账单历史记录”。您将被重定向到账单历史记录。
4. 要下载发票，请选择发票编号。

在中管理您的付款方式 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以在“Amazon 设置”中管理您的付款方式。您的付款方式用于支付所有项目的 Amazon 资源使用量。只有在创建账户时提供了信息或将账户升级到付费套餐时，您才能管理您的付款方式。

管理您的付款方式

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择计费。
3. 在“余额”下，您将看到您的付款信息。选择管理。
4. 对于付款方式，选择更新。

5. 输入新的付款方式，然后选择“保存”。

在其中付款 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以在 Amazon “设置”中支付 Amazon 账单。Amazon 每月初自动向您的默认付款方式收费。如果扣费未成功，您可以使用控制台更新您的付款方式并进行付款。

在付款之前，请确保将来要自动向您收取的付款方式设置为您的默认付款方式。如果您使用的是信用卡，请确认您的信用卡未过期。

进行付款

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择计费。
3. 在“余额”旁边，选择“查看账单历史记录”。您将被重定向到账单历史记录。
4. 在“操作”下，您将看到任何未付发票的支付发票。如果未列出任何发票，则无需执行任何操作。
5. 选择“支付发票”。
6. 确认您的选择，然后选择“付款”。

如果您对从您的银行账户收款或支付逾期余额的问题有疑问，请在[支持中心](#)中创建一个案例。

将您的首选货币更改为 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以在 Amazon “设置”中更改您的首选货币。您的首选货币仅适用于您拥有的项目。某些计费国家/地区限制付款货币。您的发卡机构可能会对使用其他货币的过渡收取费用。

更改您的首选显示货币

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择计费。
3. 在“余额”下，您将看到您的付款信息。选择管理。如果您没有看到余额，则无法更改货币。
4. 选择“设置货币”。
5. 对于“默认付款货币”，选择付款货币。
6. 选择保存。

在中管理税务登记 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以在“Amazon 设置”中管理您的纳税登记号和免税。您的税务信息仅适用于您拥有的项目。

更新和删除税务登记号码

请使用以下步骤更新或删除一个或多个税务登记号。

Note

如果某个国家/地区未在税务设置页面下拉列表中列出，则此时 Amazon 不会收集该国家/地区的税务登记信息。

更新税务登记号

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择计费。
3. 在“余额”下，您将看到您的付款信息。选择管理。
4. 选择税收设置。
5. 修改您的税务登记信息。
6. 选择保存。

管理美国免税

如果您所在的州符合资格，则可以在 Amazon 设置的计划和账单页面上管理您的美国免税。支持部门会在 24 小时内审核您上传的豁免文件。只有当您的账户注册为企业时，您才能管理免税。

上传或添加美国免税

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择计费。
3. 在“余额”下，您将看到您的付款信息。选择管理。
4. 选择 Manage tax exemption (管理免税)，然后选择 Add tax exemption (添加免税)。
5. 指定免税类型和司法管辖区。
6. 上传证明材料文档。
7. 检查您的信息，然后选择 Submit (提交)。

如果他们需要其他信息，或者您的任何文件无效，支持部门将在 24 小时内通过支持案例通知您。

免税获批之后，您可以在免税选项卡下查看其内容及活动有效期。

如果您的免税遭拒，则会通过支持案例联系方式通知您。

在中查看和兑换积分 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

您可以在“Amazon 设置”中查看和兑换您的可用积分。Amazon 抵免额自动应用于账单，以帮助支付与符合条件的服务相关的费用。有关符合条件的服务的更多信息，请参阅[兑换您的 Amazon 促销积分](#)。积分适用于您拥有的所有项目，直到用尽或到期。您无法选择使用您兑换的积分的项目，积分将应用于您拥有的所有项目。

查看您的积分

1. 在处打开 Amazon “设置” <https://settings.aws.com>。

2. 在主导航窗格中，选择计费。
3. 在“当前费用”容器中，您将看到可用的积分。选择您的积分。

根据您的套餐类型，您将被重定向到有效和过期的积分，或者您的积分和最近 6 个月的无效积分视图。

4. 要查看可用积分使用的 Amazon 服务，请选择“查看服务列表”。

兑换您的 Amazon 促销积分

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择计费。
3. 在“当前费用”容器中，您将看到可用的积分。选择您的积分。

根据您的套餐类型，您将被重定向到有效和过期的积分，或者您的积分和最近 6 个月的无效积分视图。

4. 选择兑换积分来兑换您的积分。
5. 对于促销代码，请输入显示的促销代码。兑换积分时，即表示您已阅读并同意[Amazon 促销积分条款和条件](#)。
6. 选择兑换积分。

在印度管理账户 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

如果您注册 Amazon 并选择印度作为联系方式和账单地址，则您的用户协议将与印度本地 Amazon 卖家亚马逊网络服务印度私人有限公司 (Amazon 印度) 签订。Amazon 印度管理您的账单，您的发票总额以印度卢比 (INR) 而不是美元 (USD) 列出。

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

主题

- [报名参加 Amazon \(新\) 有 Amazon 印度](#)

- [管理您的客户验证信息](#)

报名参加 Amazon（新）有 Amazon 印度

Amazon 印度是印度 Amazon 的本地销售商。如果您的联系地址和账单地址在印度，请使用以下步骤进行注册。

要使用“注册”Amazon（新）有 Amazon 印度

1. 前往 aws.amazon.com 并选择创建账户。
2. 在解释注册 Amazon（新）和注册（高级）之间区别的 Amazon 横幅上，选择注册 Amazon。
3. 选择登录方式，例如谷歌 GitHub、苹果或亚马逊。
4. 您将被引导至提供商的登录页面。登录后，您将被重定向到 Amazon 注册。
5. 输入您的姓名并选择“继续”。

当您授予团队成员访问您的项目的权限时，该名称将与他们共享。

6. 输入验证码，验证与您的登录相关的电子邮件。验证电子邮件后，选择“继续”。
7. 为您的帐户输入一个强密码，然后选择“继续”。

Amazon 要求您的密码满足以下条件：

- 长度必须至少 8 个字符，最多 128 个字符。
- 它必须至少包含以下三种字符类型组合：大写、小写、数字和! @ # \$ % ^ 管理门户 * () < > [] { } | _ + - = 符号。
- 它不得与您的 Amazon Web Services 账户 姓名或电子邮件地址相同。

8. 输入您的联系方式，然后选择“继续”。

如果您的联系地址或账单地址位于印度，则根据印度计算机应急响应小组 (CERT-In) 的规定，Amazon 在授予您使用 Amazon 服务的权限之前，必须收集和验证您的身份信息。

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

9. 选择注册账户的主要目的。
10. 选择最能代表账户所有者的所有权类型。如果您选择公司、组织或合作伙伴作为所有权类型，请输入主要管理人员的姓名。关键管理人员可以是董事、运营主管或负责公司运营的人。

11. 根据您选择的所有权类型，请选择一种可接受的印度证件类型进行验证，然后键入您的证件信息。

 Note

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

12. 选择要用于客户验证的姓名。

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

13. 同意提交信息进行验证，然后选择继续。

完成账户注册后，您将收到有关客户验证结果的电子邮件通知。您也可以在“我的 Amazon 设置”中的个人资料页面上查看状态。您必须通过客户验证才能访问 Amazon 服务。

14. Amazon 将配置您的第一个项目。

要访问 Amazon 设置，请从中选择管理项目 Amazon Web Services 管理控制台。在 Amazon “设置”中，您可以邀请团队成员、创建新项目以及修改账单和其他设置。

管理您的客户验证信息

根据印度计算机应急响应小组 (CERT-In) 的规定，Amazon 在授予您新的或持续的 Amazon 服务访问权限之前，必须收集和验证您的身份信息。您的身份必须使用您提供的印度账单或联系地址中的姓名进行验证。在验证过程中，Amazon 将检查证件编号是否有效，以及您提供的姓名是否与您用于客户验证的文件关联的姓名相符。您从联系人或账单信息中选择的姓名必须与证件上显示的姓名完全一致。

要更新您的账单名称、地址和其他联系信息，请参阅[使用 Amazon 设置](#)。如果您编辑之前用于客户验证的任何信息，例如账单中的姓名或 India-based 地址或联系信息，则可能需要更新并重新提交您的客户验证信息。

查看客户验证状态

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

创建您的客户验证信息

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

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理个人资料。
3. 要进行客户验证，请选择创建客户验证。
4. 选择与您计划用于客户验证的证件类型上的姓名完全一致的姓名。例如，如果计划使用公司注册证书验证企业账户，您必须提供证书上显示的公司名称。
5. 提供页面上要求的其余信息。根据选择的证件类型，您可能需要上传证件正面和背面的副本。如果上传了图像文件，请确保证件中的所有信息都清晰可见。
6. 选择提交。

您将通过电子邮件或 Health Amazon Dashboard 收到客户验证结果和任何后续步骤的通知。

编辑您的客户验证信息

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

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

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择管理个人资料。
3. 要进行客户验证，请选择客户验证。
4. 选择编辑，然后更新要更改的信息。

更新信息时，请注意以下指南：

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

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

5. 选择提交。

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

接受的用于客户验证的印度证件

接受印度政府签发的以下证件类型进行客户验证。

Note

政府可能会随时更改以下共享链接。

- PAN 卡 - 永久账号 (PAN) 卡有数字和实体卡两种格式，其中含有印度所得税部门向个人、公司和实体签发的唯一字母数字标识符。PAN 由十个字符组成，包括字母和数字，格式为 **AAAAA1111A**。要使用此证件进行验证，您还必须提供 PAN 证件上显示的出生日期（个人）或注册日期（企业），并上传卡片的正面。请访问[所得税部门的官方网站](#)，查看您的 PAN 的有效性。
- 选民身份证 Card/EPIC —— 选民身份证，也称为选民带照片的身份证（EPIC），包含印度选举委员会向印度符合条件的选民签发的唯一识别码。选民 ID/EPIC 号码由十个字符组成，包括字母和数字。请访问[印度选举委员会](#)的官方网站，检查您的选民 ID 的有效性。要使用此证件进行验证，您必须上传卡片的正面和背面。
- 驾驶执照 - 如果您的驾驶执照不是由印度联邦颁发的，我们建议使用其他证件类型进行验证。驾驶执照号码由 12-16 个字符组成，包括字母、数字、空格和连字符。要使用此证件进行验证，您必须提供出生日期并上传卡片的正面和背面。您可以访问道路运输和公路部的 [Parivahan Sewa 网站](#)，检查您驾驶执照的有效性。
- 公司注册证书 - 公司注册证书是由印度公司事务部（MCA）签发的证件，上面注明了企业注册为法人实体的日期。证书用于唯一标识和跟踪在印度注册的公司。每份证书都包含公司识别号 (CIN)，这是一个由 21 个字符（包括字母和数字）组成的唯一字母数字标识符。要使用此证件进行验证，您必须上传公司注册证书证件。您可以前往[印度公司事务部门门户网站](#)检查您的 CIN 是否有效。

个人和企业账户接受的印度证件类型不同：

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

在中设置您的印度账单 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

如果您注册 Amazon 并选择印度作为联系地址和账单地址，则您的用户协议与印度本地 Amazon 卖家亚马逊网络服务印度私人有限公司 (Amazon 印度) 签订。Amazon 印度管理您的账单，您的发票总额以卢比而不是美元列出。所有税务信息只能由项目所有者创建或修改。

如需其他税收或账单信息，您可以使用每个项目的 Amazon Billing 控制台。

使用“Amazon 设置”的“管理个人资料”页面中的“计划和账单”部分执行以下任务：

- 添加或编辑永久账号
- 编辑多个永久账号
- 编辑多个商品和服务税识别号
- 查看税务发票

添加或编辑永久账号

您可向账户添加永久账号 (PAN) 并对其进行编辑。

添加或编辑 PAN

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“管理个人资料”，然后选择“计划和账单”。
3. 在 Tax Settings 导航栏中，选择 Edit。
4. 对于 Permanent Account Number (PAN)，输入您的 PAN，然后选择 Update。

编辑多个永久账号

您在可以在您的账户中编辑多个永久账号 (PAN)。

编辑多个 PAN 号

1. 在处打开 Amazon “设置” <https://settings.aws.com>。

2. 在主导航窗格中，选择“管理个人资料”，然后选择“计划和账单”。
3. 在 Manage Tax Registration Numbers (管理税务登记号) 下面，选择您要编辑的 PAN 号。
4. 对于 Manage Tax Registration (管理税务登记)，选择 Edit (编辑)。
5. 更新要更改的字段，然后选择 Update (更新)。

编辑多个商品和服务税识别号

您可以在您的账户中编辑多个商品和服务税识别号 (GST)。

编辑多个 GST 号

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“管理个人资料”，然后选择“计划和账单”。
3. 在 Manage Tax Registration Numbers (管理税务登记号) 下面，选择您要编辑的 GST 号，或者选择 Edit all (编辑全部)。
4. 对于 Manage Tax Registration (管理税务登记)，选择 Edit (编辑)。
5. 更新要更改的字段并选择 Update (更新)。

查看税务发票

您可以在“Amazon 设置”中查看您的税务发票。

查看税务发票

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“管理个人资料”，然后选择“计划和账单”。
3. 向下滚动并选择发票选项卡。
4. 在税务发票部分，选择文件编号下方提及的发票链接。

Note

仅当有可用的税务发票时，税务发票部分才显示。

将登记在册的卖家更改为或更改卖家 Amazon 印度

您可以通过更新账单或税务信息将您的登记 Amazon Web Services 账户 卖家 (SOR) 更改为另一个 SOR。如果您的 Amazon 印度账户在功能不可用的旧模式下运营，则这不适用。当您在 账单或税务详细信息中编辑您的国家或地区时，如果新地点的服务提供商与您当前的位置不同，则您账户的 SOR 将自动更改。

如果您将账户更改为往返 Amazon 印度，则无需更新您的默认付款方式（如果将其设置为发票或电汇）。如果您的默认付款方式是信用卡或借记卡，则需要重新确认您的默认支付卡详细信息。这是为了确保付款方式与 Amazon 印度之外的交易分开存储。有关更多信息，请参阅[查看符合条件的 Amazon 印度发票的信用卡或借记卡](#)。

Note

如果您有一个使用信用卡或借记卡作为默认付款方式的 Amazon 印度账户，并且您设置了自动付款的电子授权，则必须先停用电子授权，然后才能编辑您的默认付款首选项。

要更改账户的 SOR，您可以使用以下选项编辑此信息：

使用账单和税务信息更改 SOR

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“管理个人资料”，然后选择“计划和账单”。
3. 在 Default payment preferences（默认付款首选项）部分中，选择 Edit（编辑）。
4. 输入新的账单地址。
5. 在付款货币部分，从您的新 SOR 接受的货币列表中选择一种默认货币。
6. （如果您的默认付款方式是信用卡或借记卡）在确认付款方式部分下，重新输入默认支付卡的详细信息，确认在新服务提供商下使用默认支付卡。

要更改新 SOR 下的默认支付卡，请稍后添加您的支付卡并更改您的默认付款方式设置。

7. 选择保存更改。

几分钟后，您的更改（包括更新的 SOR）将显示在付款首选项页面上。

使用账单和税务信息更改 SOR

要将您的账户转移到其他 SOR，您必须更新与该账户关联的税务登记号（TRN），并提供新的有效 TRN。您也可以删除与账户关联的 TRN。您账户的新 SOR 会根据您的新税务地址所在的国家/地区以及您当前的账单地址，按可用性和优先顺序自动解析。当您账户的 SOR 发生变化时，您将收到一条通知，告知您的账户正在迁入或移出 Amazon 印度。

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“管理个人资料”，然后选择“计划和账单”。
3. 选择您的账户并选择管理税务登记，然后选择编辑、全部编辑或删除 TRN。
4. （如果您的默认付款方式是信用卡或借记卡）在主导航窗格中，选择“管理个人资料”，然后选择“计划和账单”。
5. 选择添加付款方式重新输入默认支付卡的详细信息，或者添加新的支付卡。
6. 保存支付卡后，选择设为默认。

默认付款首选项部分提醒您，您之前的默认付款方式不符合在新 SOR 中使用的条件。添加支付卡后，请刷新页面，此提醒将消失。

访问 Amazon 支持

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

当您注册我们的新 Amazon 体验时，您可以在两个地方与 Support Amazon 合作。

您可以访问基本支持或商业支持+。默认情况下，您已注册 Basic Support。您可以开始试用 Business Support+，最多可免费使用六个月。

项目支持

如果您在项目、团队管理方面遇到问题或与计费有关的问题，可以在“Amazon 设置”中访问 Basic Support 或 Business Support+。您可以为组织申请其他项目，也可以申请增加与账单相关的配额。

创建支持案例

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。

2. 在主导航窗格中，选择 Support。
3. 要获得项目支持，请选择创建案例。
4. 在“主题”中，输入您的支持案例的主题。
5. 对于描述，请描述您的问题。如果可以，请描述重现该问题的步骤。
6. 选择创建工单。

创建支持案例后，您可以查看您的案例信息以继续与支持部门合作。

查看您的案例信息

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择 Support。
3. 选择您的支持案例。在此视图中，您可以看到有关您的案例的所有通信。
4. 要向支持人员发送回复，请在回复中输入您的回复，然后选择发送回复。

问题解决后，您可以将其从 Amazon “设置” 中删除。

为了解决你的问题

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择 Support。
3. 选择解决案例。

问题解决后，您将无法访问案例详情。

技术支持

如果您的 Amazon 资源出现问题，则需要技术支持。要获得技术支持，请在 Support [Amazon Center](#) 中为存在问题的项目提交案例。

如果您的所有项目和组织都已关闭，则为 Support

如果您的所有项目和组织都已关闭，请填写 Support Feedback [表与支持](#) 人员联系。

在“请求信息”部分，在“我们如何为您提供帮助”下，说明您正在使用我们的新 Amazon 体验，并且您的所有项目都已关闭。

开始试用“商业支持+”

您最多可以免费获得六个月的商业支持+。在 2026 年 10 月 31 日之前，免费提供商业支持+。从 2026 年 11 月 1 日起，标准定价开始生效，您将获得 174 美元的商业支持+积分，用于支付长达六个月的每月 29 美元。当免费期结束且积分开始时，您将保持订阅状态，并在您的信用额度余额不足时 Amazon 通知您，然后再开始进行全价计费。

您的商务支持+费用为美元29/month 或 Amazon 支出的一定百分比，以较高者为准。有关更多信息，请参阅[定价详情](#)。您的计划每月续订一次，直到您取消为止。

开始试用 Business Support+

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择 Support。
3. 选择“开始试用”。这将影响您组织中的所有项目。
4. 查看条款，选中“协议”复选框，然后选择“开始试用”。

您可以随时取消，无需承诺，也不会受到任何处罚。取消后，Business Support+ 访问权限将立即终止，所有未使用的积分将被没收。您可以随时以标准价格重新注册，但是商务支持+促销优惠一旦取消，就无法恢复。

取消业务支持+

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择 Support。
3. 选择“取消套餐”。
4. 选中该复选框以确认取消 Business Support+ 会立即返回基础支持，您将无法使用列出的权益，并且您的 174 美元积分将被删除且无法恢复。
5. 选择“取消计划”返回 Basic Support。

使用监控您的项目 Amazon CloudTrail

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

使用监控您的项目 Amazon CloudTrail

您的项目与 Amazon CloudTrail 一项服务集成，该服务可记录团队成员或 Amazon 服务所采取的行动。CloudTrail 将项目的所有 API 调用捕获为事件。捕获的调用包括来自控制台的调用以及所有支持 Amazon 服务的 API 操作。使用收集的信息 CloudTrail，您可以确定向您的项目提出的请求、提出请求的人、何时提出请求以及其他详细信息。

用于 CloudTrail 查看谁修改了您的项目

本教程适用于熟悉的用户 Amazon CLI。如果您与多个团队成员共享项目，则可以使用 CloudTrail 来查看谁修改了项目中的任何资源。onBehalfOf 参数会记录您或团队成员在使用 Amazon “设置” 或 “Amazon Web Services 管理控制台” 访问您的项目时所采取的每项操作。此参数显示用户 ID 和身份存储 ID。这些值共同定义了您已邀请访问您的项目的构建者 ID。

要找到 onBehalfOf 参数并将其连接到团队成员，您需要访问 Amazon CLI 和 Amazon Web Services 管理控制台。如果您没有 Amazon CLI 配置，则可以使用 Amazon CloudShell 访问基于浏览器、经过预先验证的 shell，您可以直接从启动该外壳 Amazon Web Services 管理控制台 并运行命令。Amazon CLI

步骤 1：要找一个 Amazon CloudTrail 事件

1. 登录 Amazon Web Services 管理控制台 并打开 CloudTrail 控制台，网址为 <https://console.aws.amazon.com/cloudtrail/>。
2. 在导航窗格中，选择事件历史记录。您会看到一个筛选的事件列表，最新的事件显示在最前面。选择一个事件。
3. 在事件记录中，您将看到以下内容：

```
"onBehalfOf": {
  "userId": "000000-e00f-000-000-00000000",
  "identityStoreArn":
    "arn:aws:identitystore::111122223333:identitystore/000000-0000-0000-0000-600000007"
}
```

这是定义创建 CloudTrail 事件的团队成员的身份。

步骤 2：将 on BehalfOf 参数连接到团队成员

要使用以下命令将 onBehalfOf 参数连接到团队成员 Amazon CLI：

要再次使用 Amazon CLI 在你的终端里

1. 运行以下命令登录 Amazon CLI。你可以使用找到你所在的地区[Amazon Web Services 区域](#) [为了你的项目](#)。

```
aws login --region project-region
```

2. 运行以下命令以获取您的身份存储的 ID。该 CloudTrail 事件显示身份存储 ARN，但不显示身份存储 ID。在查找身份存储的 ID Amazon Web Services 区域 us-east-1 时，您始终使用。

```
aws sso-admin list-instances --region us-east-1
```

输出将与以下内容类似：

```
{
  "Instances": [
    {
      "InstanceArn": "arn:aws:sso:::instance/ssoins-0000000000",
      "IdentityStoreId": "d-000000",
      "OwnerAccountId": "111122223333",
      "CreateDate": "2025-10-26T23:10:58.529000+00:00",
      "Status": "ACTIVE",
      "PrimaryRegion": "us-east-1",
      "Regions": [
        {
          "RegionName": "us-east-1",
          "Status": "ACTIVE",
          "AddedDate": "2025-10-26T23:10:58.529000+00:00",
          "IsPrimaryRegion": true
        }
      ]
    }
  ]
}
```

您要复制身份存储 ID。在本例中，身份存储 ID 为 d-000000。

3. 运行以下命令来描述与该 onBehalfOf 参数对应的团队成员。

```
aws identitystore describe-user --user-id 00000-e00f-000-000-00000000 --region us-east-1 --identity-store-id d-000000
```

输出将与以下内容类似：

```
{
  "IdentityStoreId": "d-000000",
  "UserId": "00000-e00f-000-000-0000000",
  "UserName": "carlos_salazar",
  "Name": {
    "FamilyName": "Salazar",
    "GivenName": "Carlos"
  },
  "DisplayName": "Carlos",
  "Emails": [
    {
      "Value": "carlos_salazar@example.com",
      "Type": "work",
      "Primary": true
    }
  ],
  "UserStatus": "ENABLED",
  "CreatedAt": "2025-10-26T23:15:27.213000+00:00",
  "CreatedBy": "000000000000",
  "UpdatedAt": "2025-10-26T23:18:55.432000+00:00",
  "UpdatedBy": "000000000000"
}
```

此输出中提供了您的团队成员的显示姓名和电子邮件。

要使用将onBehalfOf参数连接到团队成员 Amazon CloudShell，请登录 Amazon Web Services 管理控制台 并访问 CloudShell。有关更多信息，请参阅[入门 Amazon CloudShell](#)。您将自动拥有正确的 IAM 访问权限 CloudShell。

在中关闭项目 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

如果您不再需要您的项目，可以将其关闭。关闭项目后，可以在关闭项目之日起 90 天内重新打开项目。从您关闭项目之日到 Amazon 永久关闭项目之间的时间是关闭后期。

在关闭项目之前你需要知道什么

在关闭项目之前，请考虑以下几点：

- 如果项目因超过支出限额而暂停，则无法将其关闭。你需要关闭支出限额，然后关闭项目。有关更多信息，请参阅 [在中更新支出限额 Amazon 设置](#)。
- 所有团队成员将自动失去对该项目及其内部所有资源的访问权限。
- 关闭您的项目将作为您终止该项目的 Amazon 客户协议的通知。
- 在关闭项目之前，您无需删除项目中的资源。但是，我们建议备份要所有保留的资源或数据。有关如何备份特定资源的说明，请参阅该服务的相应 Amazon 文档。
- 您可以在关闭后重新打开项目。如果您重新打开项目，则项目中剩余的服务将重新计费。您仍需对任何未付的发票负责。
- 您仍需对项目结束前所用服务的所有未付费用和收费负责。您将在项目结束后的下个月收到 Amazon 账单。例如，如果您在 1 月 15 日关闭了账户，则您将在 2 月初收到 1 月 1 日至 15 日期间所产生使用量的账单。
- 项目关闭后，Amazon 将在我们暂停域名之前的五天内每天发送电子邮件。域名被暂停后，根据域名的注册商，我们将在 30 天内删除该域名或将该域名释放给其注册商。有关更多信息，请参阅“[我的 Amazon Web Services 账户 已关闭或永久关闭，我的域名已在 Route 53 中注册](#)”。这些信息是为项目编写的 Amazon Web Services 账户，但该信息对于项目而言是准确的。
- Amazon CloudTrail 是一项基础安全服务。这意味着，用户创建的跟踪即使在项目关闭后也可以继续存在并交付事件，除非用户在关闭项目之前明确删除了项目中的跟踪。有关如何在关闭后请求删除跟踪的 Amazon Web Services 账户 更多信息，请参阅 CloudTrail 用户指南[中的](#)Amazon Web Services 账户 关闭和跟踪。这些信息是为项目编写的 Amazon Web Services 账户，但信息对于项目是准确的。

关闭项目

关闭项目

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择要访问的项目。
3. 对于“关闭项目”，选择“关闭项目”。

4. 确认您的选择，然后选择关闭项目。

项目页面在 90 天内仍会显示您的项目，直到它被永久删除。

Post-closure 时期

关闭后期是指从您关闭账户之日到 Amazon 永久关闭项目之间的时间长度。后关闭期为 90 天。在关闭后期期间，您只能通过重新打开项目来访问您的内容和 Amazon 服务。关闭后期过后，将 Amazon 永久关闭您的项目，您将无法再重新打开该项目。Amazon 还将删除您账户中的内容和资源（CloudTrail 跟踪除外）。永久关闭项目后，其项目 ID 将无法重复使用。

重新打开你的项目

您的项目将在 90 天后永久关闭，之后您将无法重新打开项目，Amazon 并将删除项目中剩余的内容。要在项目永久关闭之前重新打开项目，(1) 您必须 Amazon Web Services 支持 尽快联系，(2) 我们必须在账户关闭之日起 60 天内收到所有未清余额的全额付款，包括提供发票上注明的所需信息。

Note

如果您重新打开项目，则项目中剩余的服务将重新计费。

激活高级 Amazon 功能

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

激活高级功能后，您可以完全控制用于管理您创建的项目和邀请的团队成员的 Amazon 组织、管理帐户和委派管理员帐户。您将直接管理 Amazon 环境的安全、治理和团队成员资格。您可以访问其他 Amazon 服务、多区域功能以及增强的管理和账单控制。

您必须先升级您的帐户，然后才能激活高级功能。有关更多信息，请参阅 [在中升级您的账户 Amazon 设置](#)。

激活高级功能后会发生什么

激活高级功能后，以下更改将立即应用于您的管理账户和包含您的项目的 Amazon 组织：

- 现在，您是包含您的项目的 Amazon 组织的管理员。
- 您为管理账户设置根电子邮件地址。您还需要设置 root 用户密码。有关更多信息，请参阅 [为您的管理账户设置 root 用户密码](#)。
- 您可以在组织中以成员帐户的身份管理您的项目。作为该组织的管理员，您可以在组织中创建成员帐户。
- 要为受邀加入组织的成员账户提供管理员角色，您必须创建一个 OrganizationAccountAccessRole。有关更多信息，请参阅在[受邀成员账户 OrganizationAccountAccessRole 中创建](#)。
- 您的团队成员被称为员工身份，他们仍然可以访问您的 Amazon 帐户。您也可以选择使用 IAM Identity Center 自定义员工的身份来源。您可以继续使用 Amazon Builder ID 作为身份源，也可以将其更改为外部身份源。如果您将身份源从 Amazon Builder ID 更改为其他身份源，则不可逆转。将来，您无法将 Amazon 生成器 ID 重新启用为身份源。有关更多信息，请参阅 [更改身份来源 Amazon Builder ID](#)。
- 您可以使用账户 Amazon 访问管理器控制用户和群组在 IAM Identity Center 组织实例中的访问权限。您可以使用此功能修改用户访问权限，同时仍允许您的用户使用aws login从浏览器接收其 IAM 角色会话证书进行登录。有关更多信息，请参阅[Amazon 账户访问管理器](#)。
- Amazon 在您的组织中创建一个名为“身份委托管理员”的成员帐户，该帐户具有委派的管理员角色。此角色用于在 IAM 身份中心和账户访问管理器中执行大多数管理任务。在美国东部（弗吉尼亚北部）必须使用委派的管理员角色。有关更多信息，请参阅 [Delegated administration](#)。
- 现在，您可以配置资源控制策略 (RCP) 和服务控制策略 (SCP)，以便在组织中实施自定义护栏。以前，代表您 Amazon 管理 RCP 和 SCP。在激活高级功能后，您可以修改这些策略。有关更多信息，请参阅 [移除组织政策](#)。

激活高级功能时，以下更改也会应用于您的 Amazon 组织：

- 如果您的任何 Amazon 账户都有支出限额，则该限额将被删除。当前暂停的所有项目都将重新激活。如果您激活高级功能，则无法创建支出限额。相反，您可以访问整套账单和成本管理工具。这包括设置预算、下载成本管理器报告以及使用 Amazon 成本异常检测来检测异常支出。您可以使用这些高级工具来分析、组织、计划和优化成本。
- 您可以访问所有 Amazon 服务。中列出了可用的服务[the section called “Amazon Web Services 服务 不支持我们的新品 Amazon 经历”](#)。在启用这些服务之前，您应该规划架构并查阅服务文档。此外，Agent Toolkit 还提供了许多使用这些服务的[技能](#)。
- 您可以访问其他 Amazon Web Services 区域可选区域，也可以访问多区域功能。Multi-Region 架构可提高工作负载的弹性。我们建议您规划如何限制和审计您的区域足迹。请务必确保您创建的资源仅存在于您打算使用的区域。

- 您可以为组织 Amazon Web Services 账户 中的每个人关闭 IAM 角色管理器。IAM 角色管理器是一个可选的账户设置，可自动配置角色，因此您和您的员工无需设置角色。有关更多信息，请参阅[如何启用和禁用角色管理器（控制台）](#)。
- 您可以使用 [IAM 访问分析器](#)。

激活高级功能时，以下更改也会应用于您的用户体验：

- 以前，Amazon Web Services 管理控制台 显示的是一个简化的视图，其中包含一个用于在项目之间切换和访问 Amazon “设置” 的菜单。Amazon Web Services 管理控制台 扩展后包括其他功能，例如区域选择器、其他服务以及为帐户设置颜色，您可以访问这些功能以明显区分它们。有关更多信息，请参阅[控制台功能](#)。
- 现在，您还可以执行以下操作：
 - 禁用多会话控制台支持。
 - 将您的 Amazon 账户指定为符合 HIPAA 或 SEC 标准的账户。
 - 使用 Amazon Marketplace
 - 通过“Amazon 激活”赚取额外积分。
 - 与 Amazon 培训合作伙伴合作。
 - 购买 Amazon 技能生成器团队订阅。
 - 与之签订企业协议 Amazon。
 - 创建专业服务合同。
 - 加入 Amazon 合作伙伴网络。

怎么会 Amazon 我激活高级功能后设置会发生变化吗？

激活高级功能后，只要您使用 Amazon 生成器 ID 作为身份来源，Amazon “设置” 就会可用。Amazon 只能从中访问设置<https://settings.aws.com>。您将无法从中访问它 Amazon Web Services 管理控制台。Amazon “设置” 将提供使用您的管理账户管理账户的链接。使用您的管理账户，您可以从 Amazon “设置” 访问以下 Amazon Web Services 管理控制台 位置。仅使用管理帐户执行管理任务，包括：

- 访问 Billing and Cost Management 控制台以查看您的账单信息。
- 访问 Amazon 组织控制台，修改管理组织的 SCP 和 RCP。
- 访问 Amazon 账户访问管理器控制台，修改员工身份的精细访问权限。
- 访问 IAM 身份中心以更改您的身份来源。

使用管理账户执行这些任务。虽然您还可以访问根用户的电子邮件和密码，但我们建议您仅使用根用户凭证来紧急访问您的账户。

您还可以使用 Amazon “设置” 来访问您在组织中的 Amazon 帐户以及与您共享的任何项目。

如果您想创建自定义角色并通过账户的 Amazon “设置” 访问它们，则必须将会话时长设置为 12 小时。

如果您拥有团队成员访问项目的权限，则可以像激活高级功能之前一样查看和访问该项目。如果您为自己的管理账户和 Amazon 组织激活高级功能，则与您共享的任何项目都不会受到影响。

我还能在里面创建一个项目吗 Amazon 激活高级功能后的设置？

激活高级功能后，您无法在当前 Amazon 组织中创建项目。您必须在组织中创建一个成员帐户。

您可以使用预先配置的默认值创建新的托管 Amazon 组织。为此，请在 Amazon “设置” 中创建一个新项目。然后，您可以创建其他项目并邀请团队成员进行协作。您也可以为此管理账户激活高级功能。

您访问的新预配置环境将与您首次注册时创建的先前 Amazon 组织没有任何连接。Amazon

如何准备激活高级功能

我们建议您在激活高级功能之前执行以下操作：

- 告知所有团队成员您将激活高级功能。除非您修改任何设置，否则您的团队成员将对项目拥有相同的访问权限，但会从简化视图 Amazon Web Services 管理控制台 更改为显示区域并提供对更多服务的访问权限的视图。如果您以后更改身份来源或添加新的 SCP 或 RCP，请通知您的员工，因为这些更改可能会影响他们的登录方式和访问权限。
- 查看您当前所有项目的支出，并注意是否有任何项目的成本波动幅度很大。在没有支出限制的情况下，您将负责您的资源产生的所有费用。我们建议您在激活高级功能之前删除或暂停闲置的资源。
- 规划您将对 Amazon 组织做出的改变，并研究最佳实践。如果您计划在不同的环境中创建资源 Amazon Web Services 区域，请修改适用于所有用户的服务控制策略以进行限制 Amazon Web Services 区域。您需要修改的 StatementID RegionFloor 以包含所有新区域。有关更多信息，请参阅 [项目的服务控制策略](#)。
- 如果您按照中的步骤操作[连接 AI 编码工具](#)，则您的 AI 工具仅包含有关新 Amazon 体验的上下文。在您使用高级功能进行开发时，这可能会导致问题。我们建议执行下列操作：
 - 将aws-starter-rules.md文件从您保存的位置移除。规则文件是否已保存，具体取决于您的代理。有关更多信息，请参阅[将规则文件放在何处](#)。

如何激活高级功能

您可以在 Amazon “设置” 中激活高级功能。无法撤消激活。

激活高级功能

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“项目”。
3. 在“操作”中，选择“浏览高级功能”。

由于激活无法撤销，因此我们将提供更多时间来探索 and 了解激活过程。

4. 准备好激活后，请执行以下操作：
 - a. 在团队名称中，输入团队名称。这是用于存储您的员工身份的 IAM 身份中心实例的名称。您的员工会看到这个名字。
 - b. 在“选择管理账户电子邮件地址”中，选择一个电子邮件地址。此电子邮件地址用于访问管理账户和执行任务。如果您使用其他电子邮件地址，只要您仍使用 Amazon 生成器 ID 作为身份来源，B Amazon uilder ID 电子邮件仍可以从 Amazon “设置” 访问管理账户。
 - c. 完成管理账户电子邮件地址的验证流程。
 - d. 选择“查看”并完成激活。
 - e. 确认您的选择并选择激活。如果您这样做，则无法恢复您的账户。

恭喜，您已经激活了高级 Amazon 功能！

激活高级功能后

激活高级功能后，您可以执行以下操作：

- [管理员工队伍](#)
- [更改身份来源 Amazon Builder ID](#)
- [移除组织政策](#)
- [创建组织单位](#)
- [Amazon Web Services 区域 在您的账户中启用或禁用](#)
- [创建 IAM 角色](#)

为您的管理账户设置 root 用户密码

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

激活高级功能后，您的管理账户现在使用根电子邮件地址进行账户恢复。虽然您仍然可以使用[自助服务选项恢复对 Amazon Builder ID 的访问权限](#)，但现在您可以使用根用户凭据恢复对管理帐户的访问权限。要访问 root 用户，您需要创建 root 用户密码。此外，我们建议您开启多重身份验证 (MFA)，以增强根用户的安全性。

设置 root 用户密码

1. 打开[Amazon 管理控制台](#)并选择使用根用户电子邮件登录。
2. 在“电子邮件地址”中，输入 root 用户的电子邮件地址。

这是您在激活高级功能时为管理账户设置的电子邮件地址。

3. 选择 Forgot your password?。

密码重置过程也是您在激活高级功能后设置 root 用户密码的方式。

4. 输入与该账户关联的电子邮件地址。
5. 提供 CAPTCHA 文本，然后选择“我不是机器人”。
6. 查看与您 Amazon Web Services 账户 关联的电子邮件，查看来自亚马逊 Web Services 的消息。该电子邮件来自以 @verify.signin.aws 结尾的地址。按照电子邮件中的说明设置 root 用户密码。如果您在账户中未看到电子邮件，请检查垃圾邮件文件夹。如果您无法再访问该电子邮件，请参阅《Amazon Sign-In 用户指南》中的[“我无法访问我的 Amazon 账户的电子邮件”](#)。

设置 root 用户密码后，即可恢复对账户的访问权限。接下来，按照[Amazon 账户根用户 Multi-factor 身份验证中的指导为您的根凭证启用 MFA](#)。

仅在必要时使用 root 用户来恢复您的账户，或者在执行[需要根用户凭据的任务时使用 root 用户](#)。对于日常工作，请使用您的身份来源（例如 Amazon Builder ID）登录。

管理员工队伍

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

激活高级功能后，您可以邀请新的员工或删除现有员工。这包括将现有员工添加到新 Amazon 账户。以下信息仅适用于使用 Amazon 生成器 ID 作为身份源的 Amazon 组织。如果您使用外部身份提供商 (IdP)，则可以在这些身份提供商中管理您的员工。如果您使用 Identity Center 目录，请使用[管理身份中心目录中的用户](#)中描述的文档。

邀请新的员工

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“项目”。
3. 访问您的身份委托管理员帐户的 Amazon 控制台。
4. 在 Amazon 主机主页中，搜索 **IAM Identity Center** 并选择它。
5. 在 IAM Identity Center 控制台的用户页面上，选择邀请新的团队成员。
6. 在“电子邮件”中，输入电子邮件地址或电子邮件地址列表。用逗号 (,) 或分号 (;) 分隔电子邮件地址。
7. 选择 Send invitation (发送邀请)。

向新员工授予访问权限 Amazon accounts

员工接受邀请后，您可以配置他们有权访问哪些 Amazon 帐户。

向您在激活高级功能之前创建的账户授予完全权限

1. 确定您要向其授予访问权限的账户的账户 ID。要查找账户 ID，请参阅[查看 Amazon 账户标识符](#)。
2. 在主导航窗格中，选择群组。
3. 选择以您标识的账户 ID 开头的群组名称。
4. 选择“将用户添加到群组”。
5. 选择要添加的用户。

6. 选择添加 1 个用户。

向新用户或现有用户授予自定义权限 Amazon account

您可以在 Amazon 账户访问管理器中配置自定义访问权限。有关更多信息，请参阅[管理 Amazon 账户访问权限](#)。

Note

如果要创建自定义角色并通过 Amazon “设置” 向其授予访问权限，则必须将会话时长设置为 12 小时。

移除员工

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“项目”。
3. 在“操作”中，选择“管理团队”。

这将打开 IAM 身份中心。

4. 在 IAM Identity Center 控制台的用户页面上，选择团队成员，然后选择删除。
5. 确认您的选择并选择“删除”。

该团队成员将立即失去对您的 Amazon 组织的所有访问权限。

这些步骤向您展示了如何通过首先访问 Amazon “设置” 来管理您的员工。但是，您可以使用您的委托管理员账户登录并访问 IAM 身份中心或 IAM 控制台来管理您的员工。Amazon Web Services 管理控制台

更改身份来源 Amazon Builder ID

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

激活高级功能后，您可以从 Amazon Builder ID 更改您的身份来源。如果您从 Amazon 生成器 ID 更改身份来源，则永远无法重复使用 Amazon 构建器 ID 作为 Amazon 组织的身份来源。

要更改您的身份来源，请从 Amazon Builder ID

1. 在以下位置打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“项目”。
3. 在“管理此组织”中，选择“更改身份来源”。

这将打开 IAM 身份中心。

4. 在 IAM Identity Center 控制台的设置页面上，选择操作，然后选择更改身份来源。
5. 对于选择身份来源，将选择 Amazon 生成器 ID。选择一个新来源，然后选择“下一步”。
6. 如果您要更改为 Active Directory，请从下一页的菜单中选择可用目录。如果您要切换到外部身份提供商，我们建议您按照[如何连接到外部身份提供商](#)中的步骤进行操作。
7. 查看并确认您的更改。您需要选中所有复选框以确认您了解组织所做的更改。
8. 确认您的选择并选择更改身份来源。

这些步骤向您展示了如何通过首先访问 Amazon “设置”来更改身份来源。但是，您可以使用委托管理员账户登录并访问 IAM Identity Center 以更改您的身份来源。Amazon Web Services 管理控制台

移除组织政策

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

激活高级功能后，您可以修改资源控制策略 (RCP) 和服务控制策略 (SCP) 以更改组织的治理。Amazon 激活高级功能后，某些 Amazon 托管组织策略将被删除。有关更多信息，请参阅[为您的组织提供托管政策](#)。以下信息仅适用于使用 Amazon 生成器 ID 作为身份源的 Amazon 组织。如果您使用其他来源，请按照[更新政策中的步骤操作](#)。

修改服务控制策略 (SCP)

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“项目”。
3. 在管理此组织中，选择管理策略。

这将打开 Amazon Organizations 控制台。

4. 选择服务控制策略页面。
5. 选择要更新的策略的名称。
6. 在策略的详细信息页面上，选择 Edit policy (编辑策略)。
7. 进行以下任何或全部更改：
 - 您可以通过在 Policy name (策略名称) 中输入新名称来重命名策略。
 - 您可以通过在 Policy description (策略说明) 中输入新文本来更改策略说明。
 - 您可以通过在左窗格中以 JSON 格式编辑策略来编辑策略文本。或者，您可以在右侧的编辑器中选择一个语句，然后使用控件更改其元素。有关每个控件的详细信息，请参阅本主题前面的创建 SCP 过程。
8. 完成后，选择保存更改。

修改资源控制策略 (RCP)

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“项目”。
3. 在管理此组织中，选择管理策略。

这将打开 Amazon Organizations 控制台。

4. 选择资源控制策略页面。
5. 选择要更新的策略的名称。
6. 在策略的详细信息页面上，选择 Edit policy (编辑策略)。
7. 进行以下任何或全部更改：
 - 您可以通过在 Policy name (策略名称) 中输入新名称来重命名策略。
 - 您可以通过在 Policy description (策略说明) 中输入新文本来更改策略说明。
 - 您可以通过在左窗格中以 JSON 格式编辑策略来编辑策略文本。或者，您可以在右侧的编辑器中选择一个语句，然后使用控件更改其元素。有关每个控件的详细信息，请参阅本主题前面的创建 RCP 过程。
8. 完成后，选择保存更改。

这些步骤向您展示如何通过 Amazon “设置” 修改组织政策。但是，您可以使用您的管理账户登录并访问 Amazon Organizations 控制台来修改这些政策。Amazon Web Services 管理控制台

关闭您的账户 Amazon 设置

Warning

我们目前正在向有限数量的客户发布我们的新体验。您可能还无法访问此体验。

如果您不再需要该组织及其中存储的所有项目，则可以关闭项目、关闭管理帐号并删除您的 Amazon Builder ID。

为确保不再向您收取消耗的任何 Amazon 资源的费用，您必须关闭项目并关闭组织的管理账户，但不必关闭个人 Amazon 资料。与之关联的 Amazon 生成器 ID 是免费的。

关闭管理账户后，您可以在关闭账户之日起 90 天内将其重新打开。从您关闭管理账户之日到 Amazon 永久关闭管理账户之间的时间为关闭后期。

关闭管理账户之前需要了解的内容

在关闭您的管理账户之前，您应该考虑以下几点：

- 关闭项目时，请考虑中的注意事项[在关闭项目之前你需要知道什么](#)。
- 必须先关闭所有项目，然后才能关闭您的管理账户。
- 您必须先关闭您的管理账户，然后才能删除您的 Amazon 生成器 ID。
- 关闭管理账户后，您可以在关闭账户之日起 90 天内将其重新打开。从您关闭管理账户之日到 Amazon 永久关闭管理账户之间的时间为关闭后期。
- 您可以在后关闭期重新打开账户。
- 您不能使用关闭组织时在组织中注册的相同电子邮件地址作为其他组织的主电子邮件地址。如果您想在使用 Sign up Amazon（新）时为其他组织使用相同的电子邮件地址，我们建议您在关闭之前对其进行更新。有关更多信息，请参阅 [在中更改您的电子邮件地址 Amazon 设置](#)。
- 如果您已在管理账户上启用多重身份验证 (MFA) 并配置了 MFA 设备，则在您关闭管理账户时，MFA 不会自动删除。如果您选择在后关闭期 90 天内保持 MFA 开启状态，请让 MFA 设备保持活动状态直到后关闭期到期，以防需要在此期间访问该账户。请注意，账户永久关闭后，硬件 TOTP 令牌设备无法与其他用户关联。如果您想稍后与其他用户一起使用硬件 TOTP 令牌，则可以选择在关闭管理账户之前停用硬件 MFA 设备。

关闭项目

要关闭项目，请参阅[在中关闭项目 Amazon 设置](#)。

关闭您的管理账户

关闭您的管理账户

1. 在处打开 Amazon “设置” <https://settings.aws.com>。
2. 在主导航窗格中，选择“项目”。
3. 对于“操作”，选择“关闭管理账户”。
4. 确认您的选择，然后选择关闭管理账户。

删除你的 Amazon Builder ID

删除您的 Amazon 生成器 ID 将导致以下结果：

- 失去访问权限：除了您的项目和组织外，您无法再访问之前通过 Amazon Builder ID 访问的任何 Amazon 工具和服务。
- 内容删除：仅与您的 Amazon Builder ID 相关的任何剩余内容都将被删除，您将无法再使用 Amazon 构建器 ID 访问应用程序中的内容或从应用程序中恢复您的内容。
- 个人信息删除：您提供的与创建和管理您的 Amazon Builder ID 相关的任何个人信息都将被删除，但 Amazon 可能保留法律要求或允许的个人信息除外，例如您的删除请求记录或以无法识别您身份的形式的数据。

您可以在 Amazon 隐私声明中详细了解我们如何处理您的信息。您可以通过访问 Amazon 通信偏好中心来更新您的 Amazon 通讯首选项或取消订阅。

现有登录名保持不变 — 如果您使用谷歌或苹果等登录名，删除您的 Amazon Builder ID 不会删除与您的登录帐户相关的任何内容。

删除你的 Amazon Builder ID

1. 在处打开 Amazon “设置” <https://settings.aws.com>。

即使你已经删除了管理账户，你仍然可以登录。

2. 在主导航窗格中，选择管理个人资料。

3. 要查看个人资料信息，请选择管理个人资料。

您将被重定向到您的 Amazon 建筑商 ID 个人资料。

4. 在主导航窗格中，选择“隐私和数据”。
5. 要删除 Amazon 生成器 ID，请选择删除您的 Amazon 生成器 ID 。
6. 确认选择，然后选择删除。

报名参加 Amazon（高级）

如果您不熟悉 Amazon，第一步是注册 Amazon Web Services 账户。当您按照“注册 Amazon（高级）”的信息进行操作时，Amazon 创建一个帐户，您可以在其中完全控制帐户配置和内容的存储位置。如果您有受监管的工作负载，例如 HIPAA、FedRAMP，请使用此选项。

要将此注册与注册 Amazon（新）进行比较，请参阅[比较注册选项](#)。

要注册 Amazon Web Services 账户，您需要提供以下信息：

- Amazon Web Services 电子邮件地址 – 此电子邮件地址用作[根用户](#)的登录名，也是账户恢复所必需的信息。您必须能够接收发送到此地址的电子邮件消息。在执行某些任务之前，必须验证您是否有权访问发送至此地址的电子邮件。
- Amazon 账户名 — 账户名称显示在多个位置，例如发票上，以及控制台（例如 Billing and Cost Management 控制面板和 Amazon Organizations 控制台）中。我们建议使用标准方法来命名账户，这样就可以为账户指定易于识别的名称。对于公司账户，可以考虑使用命名标准，例如组织-目的-环境（例如，AnyCompany-审计-生产）。对于个人账户，可以考虑使用名字-姓氏-目的之类的命名标准（例如，paulo-santos-testaccount）。
- 地址 — 如果您的联系地址和账单地址在印度，则您的账户的用户协议是与印度本地 Amazon 卖家 Amazon Web Services 印度私人有限公司（Amazon 印度）签订的。您必须在验证过程中提供 CVV。您可能还需要输入一次性密码，具体取决于您的银行。Amazon 在验证过程中，印度会向您收取 2 印度卢比的付款方式。Amazon 验证完成后，印度将退还 2 印度卢比。
- 电话号码 - 此号码用于身份验证及确认您的账户所有权。您必须能够通过此号码接收来电和短信。

Important

如果此账户是为企业开设的，请使用公司电话号码，这样 Amazon Web Services 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。

步骤 1：创建账户

这些说明用于在印度 Amazon Web Services 账户 境外创建。有关在印度创建账户的信息，请参阅[创建一个 Amazon Web Services 账户 用 Amazon 印度](#)。要创建属于由管理的组织的账户 Amazon Organizations，请参阅《Amazon Organizations 用户指南》[中的在组织中创建成员账户](#)。

Amazon Web Services 管理控制台

要创建 Amazon Web Services 账户

1. 打开[注册 Amazon](#) 页面。
2. 输入 root 用户的电子邮件地址和 Amazon Web Services 账户 姓名，然后选择“验证电子邮件地址”。这会向您的电子邮件地址发送验证码。

Important

如果此帐户适用于企业，请使用安全的公司通讯组列表（例如 `it.admins@example.com`），这样 Amazon Web Services 账户 即使员工变更职位或离开公司，您的公司也可以保留访问该列表的权限。由于电子邮件地址可用于重置账户的根用户凭证，因此需要对通讯组列表或地址的访问权限加以保护。

3. 输入您的验证码，然后选择验证。
4. 为 root 用户输入一个强密码，进行确认，然后选择“继续”。Amazon 要求您的密码满足以下条件：
 - 长度必须至少 8 个字符，最多 128 个字符。
 - 必须至少包含以下字符类型中三种的组合：大写字母、小写字母、数字，以及 `!@#$%^&*()<>[]{}|_+~=` 符号。
 - 它不得与您的 Amazon Web Services 账户 姓名或电子邮件地址相同。
5. 选择您的账户计划。有关更多信息，请参阅[免费套餐计划](#)。
6. 输入您的联系信息，然后阅读并接受[Amazon 客户协议](#)。在接受之前，请务必理解条款。

Important

如果此帐户用于企业，则最佳做法是输入公司电话号码，而不是个人电话号码。使用个人电子邮件地址或个人电话号码配置账户的根用户可能会使账户不安全。

7. 输入您的账单信息。如果您想使用不同的账单地址作为 Amazon 单信息，请选择使用新地址。

在添加有效付款方式之前，您无法继续注册流程。

8. 您可能需要确认自己的身份：
 - a. 在国家或地区代码中，输入可在接下来的几分钟内联系到的电话号码。

- b. 在“电话号码”中，输入可在接下来的几分钟内联系到的电话号码。
 - c. 选择“发送短信”。
 - d. 当自动系统与您联系时，输入您收到的验证码，然后选择“继续”。
9. 选择一个可用的 Amazon Web Services 支持计划。有关可用支持计划的描述，请参阅[比较 Amazon Web Services 支持计划](#)。
10. 选择完成注册。此时会显示确认页面，表明您的账户正在激活。
11. 检查您的电子邮件和垃圾邮件文件夹是否有确认账户已激活的电子邮件消息。激活通常需要几分钟，但有时最长需要 24 小时。
12. 收到激活消息后，您可以登录[Amazon Web Services 管理控制台](#)开始使用 Amazon Web Services 服务。有关如何管理账户设置的一般信息，请参阅[配置你的 Amazon Web Services 账户](#)。

对于多个 Amazon Web Services 账户托管方式 Amazon Organizations，请在 IAM Identity Center 中向管理用户分配管理访问权限。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 Amazon Web Services 账户访问权限](#)。

Amazon CLI & SDKs

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

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

步骤 2：（推荐）安装 Amazon CLI

Amazon CLI 按照安装中的说明[进行安装 Amazon CLI](#)。你需要版本 2.32.0 或更高版本。

您可以使用 Amazon CLI 让代理代表您管理 Amazon 资源。

安装后 Amazon CLI，使用以下命令以编程方式登录：

```
aws login
```

这会每 15 分钟自动轮换一次您的证书，使您的会话有效期长达 12 小时，无需人工干预。

使用以下命令验证您的凭证是否有效：

```
aws sts get-caller-identity
```

有关访问您的的更多信息 Amazon Web Services 账户，请参阅[访问您的 Amazon Web Services 账户](#)。

步骤 3：（推荐）设置 Amazon MCP 服务器

Amazon MCP 服务器是一个托管服务器，它允许代理 Amazon 通过模型上下文协议 (MCP) 进行访问。代理无需身份验证即可搜索 Amazon 文档和检索服务信息。要执行 Amazon API 调用、在沙盒环境中运行 Python 脚本或遵循精选技能，代理将通过您的现有 IAM 证书进行身份验证。有关更多信息，请参阅[什么是 Amazon 代理工具包？](#)

完成注册过程后，请参阅以下主题：

- [相关 Amazon 务](#)
- [使用 Amazon Web Services 账户根用户](#)
- [访问您的 Amazon Web Services 账户](#)
- [规划你的 Amazon Web Services 账户 治理结构](#)
- [配置你的 Amazon Web Services 账户](#)
- [排除您的故障 Amazon Web Services 账户](#)
- [管理印度地区的账户](#)
- [关闭一个 Amazon Web Services 账户](#)
- [重新打开 Amazon Web Services 账户](#)

相关 Amazon 务

根据您的注册方式 Amazon，您可以访问 Amazon Web Services 账户 或项目。项目包含 Amazon Web Services 账户 与其他合作者共享的设置。有关更多信息，请参阅[比较注册选项](#)。在本节中，我们将 Amazon Web Services 账户 解释您使用注册 Amazon（高级）创建的内容如何与以下服务无缝协作：

- IAM

您的 Amazon Web Services 账户 与 Amazon Identity and Access Management (IAM) 紧密集成。您可以将 IAM 与您的账户结合使用，以确保使用您的账户工作的其他人只拥有完成其工作所需的访问

权限。您还可以使用 IAM 来控制对所有 Amazon 资源的访问权限，而不仅仅是账户特定信息。在您着手设置 Amazon Web Services 账户账户结构之前，首先熟悉 IAM 的主要概念和最佳实践十分重要。有关更多信息，请参阅《[IAM 用户指南](#)》中的 IAM 安全最佳实践。

- Amazon Organizations

如果您的公司规模庞大或可能增长，则可能需要开设多个反映公司特定结构的 Amazon 账户。Amazon Organizations 为您构建和管理多账户环境提供底层基础设施和功能。您可以将您的现有账户并入组织中，以便集中管理这些账户。您可以创建自动成为组织的一部分的账户，并且您可以邀请其他账户加入您的组织。您也可以附加将影响您的部分或所有账户的策略。有关更多信息，请参阅[何时使用 Amazon Organizations](#)。

以下与账户相关的API操作是API的一部分，而不是 Amazon 账户管理 Amazon Organizations API的一部分。我们之所以将它们包括在这里，是因为客户通常在账户管理文档中查找这些操作，但它们在 Amazon Organizations 命名空间中定义的。

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

- Amazon Control Tower

Amazon Control Tower 为设置和管理安全的多账户 Amazon 环境提供了一种简化的方法。Amazon Control Tower 使用 Amazon Organizations、实例化一组初始账户以及该环境的一些默认护栏和配置，自动创建您的多账户环境。您可以通过几个步骤使用 Amazon Control Tower 来配置新 Amazon Web Services 账户 账户，同时确保账户符合您的组织政策。有关更多信息，请参阅[何时使用 Amazon Control Tower](#)。

使用 Amazon Web Services 账户根用户

根据您的注册方式 Amazon，您可以访问 Amazon Web Services 账户 或项目。项目包含 Amazon Web Services 账户 以及与其他合作者共享的设置。有关更多信息，请参阅[比较注册选项](#)。在本节中，我们将说明如何在您使用 Sign up for Amazon Web Services 账户 或 Amazon (高级) 创建的中使用 root 用户。

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

Important

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

Important

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

您可以[更改或重置根用户密码](#)，[创建或删除根用户的访问密钥](#)（访问密钥 ID 和秘密访问密钥）。有关使用 root 用户[登录的帮助](#)，请参阅《[Amazon Web Services 管理控制台 用户指南](#)》中的以 root 用户[身份](#)登录。Amazon Sign-In

访问您的 Amazon Web Services 账户

此信息是关于 Amazon Web Services 账户 您注册 Amazon 使用注册 Amazon（高级）或激活了帐户的高级功能时访问您的信息。要比较注册选项，请参阅[比较注册选项](#)。

您可以通过以下任一方式访问您 Amazon Web Services 账户 的：

Amazon Web Services 管理控制台

[Amazon Web Services 管理控制台](#)是一个基于浏览器的界面，可用于管理 Amazon Web Services 账户 设置 Amazon 和资源。

Amazon 命令行工具

使用 Amazon 命令行工具，您可以在系统的命令行下发出命令来执行 Amazon Web Services 账户 和执行 Amazon 任务。与使用控制台相比，使用命令行处理更快、更方便。如果你想构建执行 Amazon 任务的脚本，命令行工具也很有用。Amazon 提供两套命令行工具：

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

Amazon 开发工具包

这些 Amazon 软件开发工具包由各种编程语言和平台（例如 Java、Python、Ruby、.NET、iOS 和安卓）的库和示例代码组成。开发工具包执行以下类似任务：加密签署请求、管理错误以及自动重试请求。有关 Amazon 软件开发工具包的更多信息，包括如何下载和安装它们，请参阅亚马逊网络服务<https://www.amazonaws.cn/tools/#sdk>工具。

Amazon 账户管理 HTTPS 查询 API

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

规划你的 Amazon Web Services 账户 治理结构

如果您注册 Amazon 使用注册 Amazon（高级）或激活了账户的高级功能，则此信息是关于规划 Amazon Web Services 账户治理结构的信息。要比较注册选项，请参阅[比较注册选项](#)。

尽管您的 Amazon 旅程可能以一个账户开始，但 Amazon 建议您在工作负载规模和复杂性的增加时设置多个账户。无论是中型企业还是大型企业，都需要制定治理结构计划，以确保数据和工作负载需求都得到满足。

本节介绍中提供的权益和治理服务 Amazon，以帮助实现多账户监管结构。

主题

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

使用多个的好处 Amazon Web Services 账户

此信息介绍 Amazon Web Services 账户 如果您注册 Amazon 使用注册 Amazon（高级）或激活了账户的高级功能，则使用多项的好处。要比较注册选项，请参阅[比较注册选项](#)。

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

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

- 安全控制：不同的应用程序可能具有不同的安全配置文件，这些配置文件需要不同的控制策略和机制。例如，与审计师交谈要容易得多，能够指向 Amazon Web Services 账户 承载受[支付卡行业 \(PCI\) 安全标准约束的所有工作负载要素的审计机构](#)。
 - 隔离 — An Amazon Web Services 账户 是安全保护的单位。应将潜在风险和安全威胁控制在 Amazon Web Services 账户 不影响他人的范围内。由于采用不同的团队或不同的安全配置文件，可能会带来不同的安全需求。
 - 许多团队：不同的团队有不同的职责和资源需求。您可以通过将团队分离来防止他们相互干扰。
- Amazon Web Services 账户
- 数据隔离 – 除了隔离团队之外，将数据存储隔离到一个账户中也很重要。这有助于限制可以访问和管理该数据存储的人数。这有助于遏制高度私有数据的披露，因此有助于遵守[欧盟的《通用数据保护条例》\(GDPR\)](#)。
 - 业务流程 – 不同的业务单位或产品可能有完全不同的目的和流程。使用多个 Amazon Web Services 账户，您可以支持业务部门的特定需求。
 - 账单 – 账户是在账单级别分开项目的唯一真正方式。多个账户有助于在账单级别上分开业务单位、职能团队或个人用户的项目。您仍然可以将所有账单合并到单一付款人（使用 Amazon Organizations 和整合账单），同时将明细项目分 Amazon Web Services 账户为。
 - 配额分配 — 每项 Amazon 服务配额分别执行 Amazon Web Services 账户。将工作负载分成不同的 Amazon Web Services 账户 可以防止它们相互占用配额。

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

管理多个 Amazon Web Services 账户

在开始添加多个账户之前，您需要制定管理这些账户的计划。为此，我们建议您使用 [Amazon Organizations](#)，这是一项免费 Amazon 服务，可以管理组织 Amazon Web Services 账户 中的所有内容。

Amazon 还提供 Amazon Control Tower，它为组织增加了多层 Amazon 托管自动化，并自动将其与其他 Amazon 服务（如 Amazon CloudTrail、Amazon Config CloudWatch Amazon Service Catalog、

亚马逊和其他服务)集成。这些服务可能会产生额外费用。有关更多信息,请参阅[Amazon Control Tower 定价](#)。

另请参阅

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

何时使用 Amazon Organizations

此信息是关于您注册 Amazon 使用 Amazon Organizations 注册 Amazon (高级)或是否激活了帐户的高级功能时应何时使用。要比较注册选项,请参阅[比较注册选项](#)。

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

可信访问权限

当您 Amazon Organizations 使用群组管理账户时,该组织的大多数管理任务只能由组织的管理账户执行。默认情况下,这只包括与组织自身管理相关的操作。通过启用组织与该 Amazon 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 Amazon 服务授予访问有关组织及其所含账户的信息的权限。当启用账户管理可信访问权限时,账户管理服务会授予 Organizations 及其管理账户访问组织所有成员账户的元数据(比如主要或备用联系人信息)的权限。

有关更多信息,请参阅[为以下对象启用可信访问 Amazon 账户管理](#)。

委托管理员

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 Amazon 帐户。这样,委托管理员账户就可以为组织中的成员账户执行账户管理元数据的管理任务,而以前只有管理账户才能执行此种任务。委托管理员账户只能访问账户管理服务的管理任务。委托管理员账户不像管理账户那样拥有对组织的所有管理权限。

有关更多信息,请参阅[为启用委托管理员帐户 Amazon 账户管理](#)。

为以下对象启用可信访问 Amazon 账户管理

这些说明介绍如果您注册 Amazon 使用注册 Amazon (高级)或激活了 Amazon 账户的高级功能,如何为账户管理启用可信访问权限。要比较注册选项,请参阅[比较注册选项](#)。

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

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

请按照以下步骤在组织中启用账户管理的可信访问权限。

最小权限

要执行这些任务，您必须满足以下要求：

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

Amazon Web Services 管理控制台

为启用可信访问 Amazon 账户管理

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

Amazon CLI & SDKs

为启用可信访问 Amazon 账户管理

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

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

以下示例为呼叫账户组织中的 Amazon 账户管理启用可信访问权限。

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

如果成功，此命令不会产生任何输出。

为启用委托管理员帐户 Amazon 账户管理

这些说明介绍如果您注册 Amazon 使用注册 Amazon（高级）或激活了 Amazon 账户的高级功能，如何为账户管理启用委托管理员帐户。要比较注册选项，请参阅[比较注册选项](#)。

您可以为每个组织注册一个委托管理员账户来使用 Amazon 账户管理服务。注册此账户后，该账户中的用户和角色可以通过支持可选AccountId参数来调用account命名空间中的 Amazon CLI 和 Amazon SDK 操作，这些操作可以在组织模式下运行。这使委托管理员可以在中为其他成员 Amazon 账户调用账户管理 API 操作 Amazon Organizations。

要将组织中的成员账户注册为委托管理员账户，请按照以下步骤操作。

Amazon CLI & SDKs

为账户管理服务注册委托管理员账户

您可以使用以下命令，为账户管理服务启用委托管理员。

最小权限

要执行这些任务，您必须满足以下要求：

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

您必须指定以下服务主体：

```
account.amazonaws.com
```

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

以下示例将组织的成员账户注册为适用于账户管理服务的委托管理员。

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

如果成功，此命令不会产生任何输出。

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

Amazon Web Services 管理控制台

Amazon 账户管理管理控制台不支持此任务。您只能使用其中一个 Amazon SDK 中的 Amazon CLI 或 API 操作来执行此任务。

何时使用 Amazon Control Tower

此信息是关于您注册 Amazon 使用 Amazon Control Tower 注册 Amazon（高级）或是否激活了帐户的高级功能时应何时使用。要比较注册选项，请参阅[比较注册选项](#)。

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

提供的这种安全最佳实践方法 Amazon Control Tower 扩展了的核心功能 Amazon Organizations。Amazon Control Tower 应用一套预防和侦探护栏，帮助确保您的组织和账户符合建议的安全和合规标准。

通过使用建立架构良好的 Amazon Organizations 结构 Amazon Control Tower，您可以快速部署可扩展、安全和合规 Amazon 的环境。这种集中化的云管理和治理方法对于希望充分利用云的全部力量 Amazon Web Services 云 同时保持最高安全性和合规性标准的企业至关重要。

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

了解 API 的操作模式

此信息旨在了解您注册 Amazon 使用注册 Amazon（高级）或激活了账户的高级功能后的 API 操作模式。要比较注册选项，请参阅[比较注册选项](#)。

使用 an Amazon Web Services 账户的属性的 API 操作始终采用以下两种操作模式之一：

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

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

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

授予更新账户属性的权限

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

Amazon Web Services 账户在向 IAM 主体（用户或角色）附加 IAM 权限策略时，可以指定主体可以在哪些资源上以及在什么条件下执行哪些操作。

以下是创建权限策略时针对账户管理的一些注意事项。

的亚马逊资源名称格式 Amazon Web Services 账户

- 根据您要引用的账户是独立账户还是组织中的账户，您可以将其包含在政策声明 `resource` 元素中的亚马逊资源名称 (ARN) 的构造方式有所不同。Amazon Web Services 账户 请参阅 [了解 API 的操作模式](#) 中的上一部分。

- 独立账户的账户 ARN :

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

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

- 组织成员账户的账户 ARN :

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

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

IAM 策略的上下文键

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

##:AccountResourceOrgPaths

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

由于 `account:AccountResourceOrgPaths` 是多值字符串类型，因此必须使用 [ForAnyValue 或 ForAllValues 多值字符串](#) 运算符。另请注意，即使您引用的是组织中 OU 的路径 `account`，条件密钥的前缀也是。

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

```
    ]  
  }  
}
```

##:AccountResourceOrgTags

上下文键 `account:AccountResourceOrgTags` 允许您引用可以附加到组织账户的标签。标签是一个 key/value 字符串对，可用于对账户中的资源进行分类和标记。有关更多信息，请参阅《Amazon Resource Groups 用户指南》中的[标签编辑器](#)。有关在基于属性的访问控制策略中使用标签的信息，请参阅《IAM 用户指南》中的[什么是 Amazon 的 ABAC](#)。以下示例片段将策略限制为仅适用于组织中具有键 `project` 和值 `blue` 或 `red` 的标签的账户。

由于 `account:AccountResourceOrgTags` 是多值字符串类型，因此必须使用 [ForAnyValue](#) 或 [ForAllValues](#) 多值字符串运算符。另外，请注意，即使您引用的是组织成员账户上的标签 `account`，条件密钥的前缀也是。

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

Note

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

配置你的 Amazon Web Services 账户

这些说明介绍了如何配置您 Amazon Web Services 账户 是否 Amazon 使用注册 Amazon（高级）或激活了帐户的高级功能。要比较注册选项，请参阅[比较注册选项](#)。

本部分包含描述如何管理您的的主题 Amazon Web Services 账户。

 Note

如果您 Amazon Web Services 账户 是使用亚马逊网络服务印度私人有限公司（印度）在 Amazon 印度创建的，则还有其他注意事项。有关更多信息，请参阅 [管理印度地区的账户](#)。

主题

- [创建一个 Amazon Web Services 账户 别名](#)
- [启用或禁用 Amazon Web Services 区域 在你的账户中](#)
- [更新您的账单 Amazon Web Services 账户](#)
- [更新 亚马逊 Web Services 电子邮件地址](#)
- [更新根用户密码](#)
- [更新你的 Amazon Web Services 账户 name](#)
- [更新您的备用联系人 Amazon Web Services 账户](#)
- [更新您的主要联系人 Amazon Web Services 账户](#)
- [视图 Amazon Web Services 账户 标识符](#)

创建一个 Amazon Web Services 账户 别名

这些说明介绍如果您 Amazon 使用注册 Amazon（高级）注册或激活了账户的高级功能，如何创建 Amazon Web Services 账户 别名。要比较注册选项，请参阅[比较注册选项](#)。

如果您希望 IAM 用户的 URL 包含您的公司名称（或其他易于记住的标识符）而不是 Amazon Web Services 账户 ID，则可以创建账户别名。

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

启用或禁用 Amazon Web Services 区域 在你的账户中

此信息是关于您注册 Amazon 使用注册 Amazon（高级）或激活了账户的高级功能 Amazon Web Services 账户 时 Amazon Web Services 区域 在您的账户中启用或禁用的。要比较注册选项，请参阅[比较注册选项](#)。

An Amazon Web Services 区域 是世界上 Amazon 具有多个可用区的物理位置。可用区由一个或多个离散 Amazon 的数据中心组成，每个数据中心都具有冗余电源、网络 and 连接，位于不同的设施中。这

意味着每个区域在物理上 Amazon Web Services 区域 都是隔离的，独立于其他区域。区域提供容错能力、稳定性和弹性，还可以减少延迟。在离最终用户 Amazon Web Services 区域 更近的地方运行工作负载可以提高性能并降低延迟。有关可用区域和即将推出区域的地图，请参阅 [区域和可用区](#)。要了解有关工作负载在 Amazon Web Services 区域 性架构的更多信息，请访问[Amazon 多区域基础知识](#)。

Amazon Web Services 区域 账户可用性大致分为两类：

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

当您注册时 Amazon Web Services 账户，会根据您的联系地址所在国家/地区为您 Amazon 推荐一个选择加入的地区。拥有 Amazon 选择加入区域的国家/地区的客户将在联系信息页面上看到有关在该国家/地区启用选择加入区域的建议。在同时设有选择加入区域和默认区域的国家/地区（如印度、澳大利亚或加拿大），若选择加入区域距离客户更近，则会显示选择加入区域的推荐提示。激活账户后，您可以在账户中启用其他 Amazon 选择加入区域，也可以选择禁用您在注册期间启用的选择加入区域。

创建时 Amazon Web Services 账户，您的 IAM 数据和证书将自动配置为在所有默认区域中运行，从而允许根用户和具有适当权限的 IAM 身份使用其现有证书访问这些区域中的 Amazon 服务。Amazon 默认情况下，可选区域处于禁用状态，IAM 数据和证书最初在这些区域不可用，这会阻止访问该地区的 Amazon 服务。当您选择启用选择加入区域时，Amazon 会将您的 IAM 数据和凭证传播到该区域。传播完成并启用选择加入区域后，根用户和 IAM 身份就可以使用他们在默认区域中使用的相同的 IAM 证书访问新启用的选择加入区域中的 Amazon 服务。

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

Important

禁用区域将禁用 IAM 对该区域资源的访问。这并不会删除相关资源，这些资源会继续产生费用。在禁用区域之前，请移除所有剩余资源。

Amazon 将区域分组为[分区](#)。每个区域仅属于一个分区，而每个分区包含一个或多个区域。分区具有独立的 Amazon Identity and Access Management (IAM) 实例，并在不同分区中的区域之间提供硬边界。Amazon 商业区域在aws分区中，中国的区域在aws-cn分区中，Amazon GovCloud (US) 区域在aws-us-gov分区中。根据您创建的分区 Amazon Web Services 账户，可以在该分区 Amazon Web Services 区域 中使用。

- aws分区中的账户可让您访问商业分区中的多个区域，这样您就可以在符合要求的位置启动 Amazon 资源。例如，您可能希望在欧洲区域启动 Amazon EC2 实例以更多符合欧洲客户的要求或满足法律要求。
- aws-us-gov分区中的账户可让您访问 Amazon GovCloud (US-West) 区域和 Amazon GovCloud (US-East) 区域。有关更多信息，请参阅 [Amazon GovCloud \(US\)](#)。
- aws-cn 分区中的账户只能让您访问北京和宁夏区域。有关更多信息，请参阅 [中国的 Amazon Web Services](#)。

主题

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

区域可用性参考

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

Opt-in Regions

以下区域为选择加入区域，必须先启用才能使用：

Name	代码	Status
非洲（开普敦）	af-south-1	GA
亚太地区（香港）	ap-east-1	GA

Name	代码	Status
亚太地区（台北）	ap-east-2	GA
亚太地区（海得拉巴）	ap-south-2	GA
亚太地区（雅加达）	ap-southeast-3	GA
亚太地区（墨尔本）	ap-southeast-4	GA
亚太地区（马来西亚）	ap-southeast-5	GA
亚太地区（新西兰）	ap-southeast-6	GA
亚太地区（泰国）	ap-southeast-7	GA
加拿大西部（卡尔加里）	ca-west-1	GA
欧洲（苏黎世）	eu-central-2	GA
欧洲地区（米兰）	eu-south-1	GA
欧洲（西班牙）	eu-south-2	GA
以色列（特拉维夫）	il-central-1	GA
中东（阿联酋）：	me-central-1	GA
中东（巴林）	me-south-1	GA
墨西哥（中部）	mx-central-1	GA

Default Regions

以下区域默认启用且不可禁用：

Name	代码
亚太地区（东京）	ap-northeast-1

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

Important

Amazon 建议您使用区域 Amazon Security Token Service (Amazon STS) 终端节点而不是全局终端节点来减少延迟。来自区域 Amazon STS 终端节点的会话令牌在所有 Amazon 区域都有效。如果您使用区域 Amazon STS 终端节点，则无需进行任何更改。但是，来自全局 Amazon STS 端点 (<https://sts.amazonaws.com>) 的会话令牌仅在 Amazon Web Services 区域

您启用或默认情况下处于启用状态时才有效。如果您打算为账户启用新区域，则可以使用来自区域 Amazon STS 终端节点的会话令牌，也可以激活全球终端 Amazon STS 端节点来发行对所有区域均有效的会话令牌 Amazon Web Services 区域。适用于所有区域的会话令牌较大。如果存储会话令牌，这些较大的令牌可能会影响您的系统。有关 Amazon STS 终端节点如何与 Amazon 区域合作的更多信息，请参阅 Amazon STS 在 Amazon 区域中[管理](#)。

启用和禁用区域之前的注意事项

在启用或禁用区域之前，务必考虑以下几点：

- 无论 Region-opt 状态如何，您都可以在跨区域推理地理区域中使用所有目标区域 - 某些 Amazon 生成式 AI 服务，包括 Amazon Bedrock (参见通过跨区域推理[提高吞吐量](#)) 和 Amazon Q Developer (参见 Amazon Q Developer 中的[Cross-region处理](#)) [使用跨区域推理](#)。如果您使用这些服务，它们会自动在您选定的地理区域内选择最优 Amazon Web Services 区域——包括您尚未为资源和 IAM 数据启用的区域。这会最大限度地提高计算资源和模型的可用性，进而改善客户体验。
- 您可以使用 IAM 权限来控制对区域的访问权限 — Amazon Identity and Access Management (IAM) 包括四种权限，允许您控制哪些用户可以启用、禁用、获取和列出区域。有关更多信息，请参阅《IAM 用户指南》中的 [Amazon：允许启用和禁用 Amazon Web Services 区域](#)。您也可以使用[aws:RequestedRegion](#)条件键来控制对 Amazon Web Services 服务 中的访问权限 Amazon Web Services 区域。
- 启用和禁用区域是免费的 - 启用或禁用区域均不收取任何费用。您只需为在新区域中创建的资源付费。
- 亚马逊 EventBridge 集成 — 您可以在中订阅区域选择状态更新通知。EventBridge 将为每次状态更改创建 EventBridge 通知，允许客户自动化工作流程。
- 表达 Region-opt 状态 — 由于选择加入区域的 enabling/disabling 异步性质，区域选择请求有四种潜在的状态：
 - ENABLING
 - DISABLING
 - ENABLED
 - DISABLED

当选择加入或选择退出处于 ENABLING 或 DISABLING 状态时，无法将其取消。否则将抛出 ConflictException。完成的 (Enabled/Disabled) region-opt 请求取决于关键基础 Amazon 服务的供应。尽管状态为，但可能有些 Amazon 服务无法立即使用 ENABLED。

处理时间和请求限制

启用或禁用区域时，请注意以下时间限制和请求限制：

- 在某些情况下启用一个区域需要几分钟到几小时的时间 - 在启用一个区域时，Amazon 将执行操作以准备您在该区域内的账户，例如将您的 IAM 资源分发给该区域。对大多数账户而言，此过程需要几分钟时间，但有时可能需要几小时。在此过程完成之前，您无法使用区域。
- 禁用区域并非总是立即可见 - 禁用区域后，服务和控制台可能会暂时可见。禁用区域可能需要几分钟到几小时才能生效。
- 一个账户在任何给定时间可以有 6 个处理中的区域选择请求 - 一个请求等于为一个账户启用或禁用一个特定区域。
- 组织可以在给定时间在组织内开启 50 个区域选择请求 — 管理账户可以在任何时间点为其 Amazon 组织提出 50 个待完成的未结请求。一个请求等于为一个账户启用或禁用一个特定区域。

为独立账户启用或禁用区域

要更新您 Amazon Web Services 账户 有权访问的区域，请执行以下过程中的步骤。以下 Amazon Web Services 管理控制台 过程始终仅在独立上下文中起作用。您只能使用 Amazon Web Services 管理控制台 来查看或更新用于调用操作的账户中的可用区域。

Amazon Web Services 管理控制台

为独立服务器启用或禁用区域 Amazon Web Services 账户

最小权限

要执行下列程序中的步骤，IAM 用户或角色必须具有以下权限：

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

1. 以具有最低权限的 Amazon Web Services 账户根用户 IAM 用户或角色或角色身份登录。 [Amazon Web Services 管理控制台](#)
2. 在窗口的右上角，选择您的账户名称，然后选择账户。

3. 在[账户页面](#)，向下滚动至 Amazon Web Services 区域 部分。
4. 选择要启用或禁用的区域，然后选择所需操作：启用或禁用。您将看到确认提示。
5. 如果选择了启用选项，请查看显示的文本，然后选择启用区域。

如果选择了禁用选项，请查看显示的文本，键入 **disable** 进行确认，然后选择禁用区域。

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

Amazon CLI & SDKs

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

- EnableRegion
- DisableRegion
- GetRegionOptStatus
- ListRegions

最小权限

要执行下列步骤，您必须拥有映射到此操作的权限：

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

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

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

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

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

如果成功，此命令不会产生任何输出。

该操作是异步的。以下命令可以使您查看请求的最新状态。

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

在组织中启用或禁用区域

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

Note

Amazon Organizations 托管策略

策略 `AWSOrganizationsReadOnlyAccess` 或 `AWSOrganizationsFullAccess` 已更新为提供访问 Amazon 账户管理 API 的权限，因此您可以从 Amazon Organizations 控制台访问账户数据。要查看更新的托管策略，请参阅组织托管 Amazon 管策略的 [更新](#)。

Note

在通过管理账户或组织中的委托管理员账户为成员账户执行这些操作之前，您必须：

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

Amazon Web Services 管理控制台

在组织中启用或禁用区域

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

Amazon CLI & SDKs

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

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

最小权限

要执行下列步骤，您必须拥有映射到此操作的权限：

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

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

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

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

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

如果成功，此命令不会产生任何输出。

Note

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

该操作是异步的。以下命令可以使您查看请求的最新状态。

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

更新您的账单 Amazon Web Services 账户

Amazon Web Services 账户 如果您注册 Amazon 使用注册 Amazon（高级）或激活了账户的高级功能，这些说明介绍了如何更新账单。要比较注册选项，请参阅[比较注册选项](#)。

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

更新 亚马逊 Web Services 电子邮件地址

这些说明用于如果您 Amazon 使用注册 Amazon（高级）注册或为帐户激活了高级功能，如何更新根用户的电子邮件地址。要比较注册选项，请参阅[比较注册选项](#)。

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

 Note

对的更改 Amazon Web Services 账户 最多可能需要四个小时才能传播到任何地方。

您可以根据账户是独立账户还是组织账户的不同，分别更新Amazon Web Services 电子邮件：

- 独立账户 Amazon Web Services 账户 或管理账户 — 对于 Amazon Web Services 账户 未与组织关联的账户或组织的管理账户，您可以使用 Amazon 管理控制台更新 Amazon Web Services 电子邮件。要了解如何执行此操作，请参阅[更新独立账户 Amazon Web Services 账户 或管理账户的Amazon Web Services 电子邮件](#)。
- Amazon Web Services 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 Amazon Organizations 控制台集中更新成员账户的，也可以通过 Amazon CLI 和 SDK 以编程方式更新成员账户的 Amazon Web Services 电子邮件。Amazon 要了解如何执行此操作，请参阅[更新组织中任何成员的Amazon Web Ser Amazon Web Services 账户 vices 电子邮件](#)。

主题

- [更新 亚马逊 Web Services 电子邮件 对于独立版 Amazon Web Services 账户 或管理账户](#)
- [更新 亚马逊 Web Services 电子邮件 对于任何 Amazon Web Services 账户 在你的组织中](#)

更新 亚马逊 Web Services 电子邮件 对于独立版 Amazon Web Services 账户 或管理账户

要编辑独立账户 Amazon Web Services 账户 或管理账户的 Amazon Web Services 电子邮件地址，请执行以下过程中的步骤。

Amazon Web Services 管理控制台

 Note

您必须以身份登录 Amazon Web Services 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 Amazon Web Services 账户 电子邮件地址和密码以您的[Amazon Web Services 管理控制台](#)身份登录 Amazon Web Services 账户根用户。

2. 在控制台的右上角，选择您的账户名称或账号，然后选择 Account (账户)。
3. 在[账户页面](#)，点击账户详情旁边的操作按钮，然后选择更新电子邮件地址和密码。
4. 在账户详情页面，点击电子邮件地址旁边的编辑按钮。
5. 在编辑账户电子邮件页面，填写新电子邮件地址和确认新电子邮件地址字段，并确认您当前的密码。然后，选择保存并继续。no-reply@verify.signin.aws 将向新的电子邮件地址发送验证码。
6. 在编辑账户电子邮件页面，于验证码栏输入您通过电子邮件收到的验证码，然后选择确认更新。

 Note

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

Amazon CLI & SDKs

其中一个 Amazon 软件开发工具包 Amazon CLI 的 API 操作不支持此任务。您只能使用来执行此任务 Amazon Web Services 管理控制台。

更新 亚马逊 Web Services 电子邮件 对于任何 Amazon Web Services 账户 在你的组织中

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

 Note

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

以 Amazon Web Services 电子邮件地址。如需逐步说明，请遵循 [更新 亚马逊 Web Services 电子邮件 对于独立版 Amazon Web Services 账户 或管理账户](#) 中提供的步骤。

Amazon Management Console

注意

- 要通过管理账户或组织中的委派管理员账户对成员账户执行此过程，必须[为账户管理服务启用可信访问](#)。
- 您不能使用此过程访问与您用于调用操作的组织不同的组织中的帐户。

要更新 亚马逊 Web Services 电子邮件地址 对于使用以下内容的成员账户 Amazon Organizations 控制台

1. 在要注销的管理账户中，以具有所需最低权限 `portal:ModifyAccount` 的用户或角色身份登录。
2. 在 Amazon Web Services 账户 页面上，选择要为其更新 Amazon Web Services 电子邮件地址的成员账户。
3. 在账户详细信息部分中选择操作按钮，然后选择更新电子邮件地址。
4. 在电子邮件下，输入成员账户的新电子邮件地址，然后选择保存。此操作将向新的电子邮件地址发送一次性密码 (OTP)。

Note

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

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

Amazon CLI & SDKs

您可以使用以下 Amazon CLI 命令或其 Amazon 软件开发工具包等效操作来检索或更新 Amazon Web Services 的电子邮件地址：

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

注意

- 要通过管理账户或组织中的委派管理员账户对成员账户执行这些操作，必须[为账户管理服务启用可信访问](#)。
- 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

对于各个操作，您必须具有映射到此操作的权限：

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

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

要完成 Amazon Web Services 电子邮件地址流程，您必须按照以下示例中显示的顺序同时使用主电子邮件 API。

Example `GetPrimaryEmail`

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

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

Example `StartPrimaryEmailUpdate`

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

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

Example AcceptPrimaryEmailUpdate

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

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

更新根用户密码

这些说明介绍如果您注册 Amazon 使用注册 Amazon（高级）或激活了帐户的高级功能，则如何更新根用户密码。要比较注册选项，请参阅[比较注册选项](#)。

要编辑您的 Amazon Web Services 账户根用户密码，请执行以下过程中的步骤。

Amazon Web Services 管理控制台

要编辑您的根用户密码

Note

您必须以的身份登录 Amazon Web Services 账户根用户，这不需要额外的 IAM 权限。您无法以 IAM 用户或角色身份执行这些步骤。

1. 使用您的 Amazon Web Services 账户电子邮件地址和密码以您的[Amazon Web Services 管理控制台](#)身份登录 Amazon Web Services 账户根用户。
2. 在控制台的右上角，选择您的账户名称或账号，然后选择 Account（账户）。
3. 在[账户页面](#)，点击账户详情旁边的操作按钮，然后选择更新电子邮件地址和密码。
4. 在账户详情页面，点击密码旁边的编辑按钮。
5. 在编辑密码页面上，填写当前密码、新密码和确认新密码字段。然后，选择更新密码。有关其他指导，包括设置根用户密码的最佳实践，请参阅《IAM 用户指南》中的[更改 Amazon Web Services 账户根用户的密码](#)。

Amazon CLI & SDKs

其中一个 Amazon SDK 的 API 操作不支持此任务。Amazon CLI 您只能使用来执行此任务 Amazon Web Services 管理控制台。

更新你的 Amazon Web Services 账户 name

这些说明说明了如果您注册 Amazon 使用注册 Amazon（高级）或激活了帐户的高级功能，如何更新您的 Amazon Web Services 账户 姓名。要比较注册选项，请参阅[比较注册选项](#)。

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

账户名称出现在多个地方，例如在您的发票上以及账单和成本管理控制面板和控制台等 Amazon Organizations 控制台中。我们建议您使用标准方法来命名账户，以便您的账户名称易于识别。对于公司账户，请考虑使用组织-目的-环境之类的命名标准（例如，sales-catalog-prod）。出于隐私和安全考虑，请避免使用包含个人身份信息 (PII) 的账户名称。

- 独立账户 Amazon Web Services 账户 或管理账户 - 对于与组织 Amazon Web Services 账户 无关或组织的管理账户，您可以使用 Amazon Web Services 管理控制台、或 Amazon CLI 和 SDK 更新您的账户名称。若要了解如何执行此操作，请参阅[更新您的独立账户名称 Amazon Web Services 账户 或管理账户](#)。
- Amazon Web Services 账户 组织内部 — 对于属于的成员账户，管理账户或委派管理员账户中的用户可以从 Amazon Organizations 控制台集中更新组织中任何成员账户的账户名，也可以通过 Amazon CLI 和软件开发工具包以编程方式更新组织中任何成员账户的账户名。Amazon Organizations 若要了解如何执行此操作，请参阅[为任意账户更新您的账户名 Amazon Web Services 账户 在您的组织中](#)。

Note

对的更改 Amazon Web Services 账户 可能需要长达四个小时才能传播到所有地方。

主题

- [更新您的独立账户名称 Amazon Web Services 账户 或管理账户](#)
- [为任意账户更新您的账户名 Amazon Web Services 账户 在您的组织中](#)

更新您的独立账户名称 Amazon Web Services 账户 或管理账户

要更改独立账户 Amazon Web Services 账户 或管理账户的账户名，请执行以下过程中的步骤。

Amazon Web Services 管理控制台

最小权限

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

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

更新独立账户或管理账户的账户名

1. 使用您的 Amazon Web Services 账户电子邮件地址和密码以您的[Amazon Web Services 管理控制台](#)身份登录 Amazon Web Services 账户根用户。
2. 在控制台的右上角，选择您的账户名称或账号，然后选择 Account (账户)。
3. 在[账户页面](#)，点击账户详情旁边的操作按钮，然后选择更新账户名。
4. 在名称栏，输入您要更新的新账户名称，然后选择保存。

Amazon CLI & SDKs

最小权限

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

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

更新独立账户或管理账户的账户名

您还可以使用以下操作之一：

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

```
$ C:\> aws account put-account-name \
```

```
--account-name "New-Account-Name"
```

- Amazon 软件开发工具包：[PutAccountName](#)

为任意账户更新您的账户名 Amazon Web Services 账户 在您的组织中

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

要为组织中的任何成员账户更改账户名，请执行以下流程中的步骤。

要求

要使用 Amazon Organizations 控制台更新账户名称，您需要进行一些初步设置：

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

Amazon Web Services 管理控制台

最小权限

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

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

要更新成员账户的账户名称

1. 打开组织控制台，网址为<https://console.aws.amazon.com/organizations/>。
2. 在主导航窗格中，选择 Amazon Web Services 账户。
3. 在 Amazon Web Services 账户 页面上，选择要更新的成员账户，选择操作下拉菜单，然后选择更新账户名。

4. 在名称栏中，输入更新的名称，然后选择保存。

Amazon CLI & SDKs

最小权限

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

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

要更新成员账户的账户名称

您还可以使用以下操作之一：

- Amazon CLI：[put-account-name](#)

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

- Amazon 软件开发工具包：[PutAccountName](#)

更新您的备用联系人 Amazon Web Services 账户

Amazon Web Services 账户 如果您 Amazon 使用注册 Amazon (高级) 注册或激活了帐户的高级功能，这些说明介绍了如何更新您的备用联系人。要比较注册选项，请参阅[比较注册选项](#)。

备用联系人 Amazon 允许联系最多三个与该帐户关联的备用联系人。备用联系人不一定是特定人员。如果您拥有负责管理账单、运营和安全相关问题的团队，则可以添加电子邮件分发列表。除此之外，还有与账户的[根用户](#)关联的电子邮件地址。[主账户联系人](#)将继续接收发往根账户电子邮件的所有电子邮件通信。

您只能从与账户关联的以下联系人类型中指定一个类型。

- 账单联系人
- 操作联系人

- 安全联系人

您可以根据账户是独立账户还是组织的一部分，以不同方式添加或编辑备用联系人：

- 独立 Amazon Web Services 账户 — 如果与组织 Amazon Web Services 账户 无关联，您可以使用 Amazon 管理控制台或通过 Amazon CLI 和 SDK 更新自己的备用联系人。要了解如何执行此操作，请参阅[为独立 Amazon Web Services 账户更新备用联系人](#)。
- Amazon Web Services 账户 组织内部 — 对于属于组织的成员账户，管理账户或委派管理员账户中的用户可以从 Amazon Organizations 控制台集中更新 Amazon 组织中的任何成员账户，也可以通过 Amazon CLI 和 SDK 以编程方式更新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 Amazon Web Services 账户 中任何联系人的备用联系人](#)。

主题

- [电话号码和电子邮件地址要求](#)
- [更新独立版的备用联系人 Amazon Web Services 账户](#)
- [更新任何联系人的备用联系人 Amazon Web Services 账户 在您的组织中](#)
- [账户：AlternateContactTypes 上下文密钥](#)

电话号码和电子邮件地址要求

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

- 电话号码只能包含数字、空格和以下字符：“+-()”。
- 电子邮件地址最长可以有 254 个字符，除了标准的字母数字字符外，还可以在电子邮件地址的局部包含以下特殊字符：“+ = . # | ! & - _”。

更新独立版的备用联系人 Amazon Web Services 账户

要为独立用户添加或编辑备用联系人 Amazon Web Services 账户，请执行以下步骤中的步骤。以下 Amazon Web Services 管理控制台 过程始终仅适用于独立上下文。您只能使用 Amazon Web Services 管理控制台 来访问或更改您拨打该操作所用帐户中的备用联系人。

Amazon Web Services 管理控制台

为独立用户添加或编辑备用联系人 Amazon Web Services 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` (查看备用联系人详细信息)
- `account:PutAlternateContact` (设置或更新备用联系人)
- `account>DeleteAlternateContact` (删除备用联系人)

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

Note

如果您没有看到“编辑”选项，则很可能您没有以账户的根用户身份登录，也没有以之前指定的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 Amazon Web Services 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。

Amazon CLI & SDKs

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

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

 注意

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

 最小权限

对于各个操作，您必须具有映射到此操作的权限：

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

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

Example

以下示例检索了调用方账户的当前账单备用联系人。

```
$ aws account get-alternate-contact \
  --alternate-contact-type=BILLING
{
  "AlternateContact": {
    "AlternateContactType": "BILLING",
    "EmailAddress": "saanvi.sarkar@amazon.com",
    "Name": "Saarvi Sarkar",
    "PhoneNumber": "+1(206)555-0123",
    "Title": "CF0"
```

```
}  
}
```

Example

以下示例为调用方账户设置了新的操作备用联系人。

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

如果成功，此命令不会产生任何输出。

Example

Note

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

Example

以下示例删除了调用方账户的安全备用联系人。

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

如果成功，此命令不会产生任何输出。

Note

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

更新任何联系人的备用联系人 Amazon Web Services 账户 在您的组织中

要添加或编辑组织 Amazon Web Services 账户 中任何人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 Amazon Organizations 主机更新备用联系人，您需要进行一些初步设置：

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

Note

Amazon Organizations 托管策

略AWSOrganizationsReadOnlyAccess或AWSOrganizationsFullAccess已更新为提供访问 Amazon 账户管理 API 的权限，因此您可以从 Amazon Organizations 控制台访问账户数据。要查看更新的托管策略，请参阅组织托管 Amazon 管策略的[更新](#)。

Amazon Web Services 管理控制台

为任何人添加或编辑备用联系人 Amazon Web Services 账户 在您的组织中

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

 Important

对于企业而言 Amazon Web Services 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。

Amazon CLI & SDKs

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

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

 注意

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

 最小权限

对于各个操作，您必须具有映射到此操作的权限：

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

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

Example

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

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

Example

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

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

如果成功，此命令不会产生任何输出。

Note

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

Example

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

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

如果成功，此命令不会产生任何输出。

Example**Note**

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

账户：AlternateContactTypes 上下文密钥

您可以使用上下文密钥account:AlternateContactTypes指定 IAM 政策允许（或拒绝）三种联系类型中的哪一种。例如，以下示例 IAM 权限策略使用此条件键，允许附加的主体仅检索组织中特定账户的 BILLING 备用联系人，但不能进行修改。

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

更新您的主要联系人 Amazon Web Services 账户

这些说明用于说明 Amazon Web Services 账户 如果您 Amazon 使用注册 Amazon（高级）注册或为帐户激活了高级功能，如何更新您的主要联系人。要比较注册选项，请参阅[比较注册选项](#)。

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

您可以根据账户是独立账户还是组织的一部分，以不同方式编辑主账户联系人：

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

主题

- [电话号码和电子邮件地址要求](#)
- [更新独立版的主要联系人 Amazon Web Services 账户 或管理账户](#)
- [更新任何联系人的主要联系人 Amazon 您组织中的成员账户](#)

电话号码和电子邮件地址要求

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

- 电话号码只能包含数字。
- 电话号码必须以 + 和国家/地区代码开头，并且国家/地区代码后面不得有任何前导零或多余的空格。例如，+1(US/Canada) 或 +44 (UK)。
- 电话号码在区号、交换代码和本地代码之间不得包含空格。例如，+12025550179。
- 出于安全起见，电话号码必须能够接收来自 Amazon 的短信。不接受免费电话号码，因为大多数免费电话都不支持短信。
- 对于企业而言 Amazon Web Services 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。为账户的 [root 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 Amazon Web Services 账户 或管理账户

要编辑独立账户 Amazon Web Services 账户 或管理账户的主要联系人详细信息，请执行以下过程中的步骤。以下 Amazon Web Services 管理控制台 过程始终仅在独立环境中起作用。可以使用 Amazon Web Services 管理控制台 只访问或更改操作调用账户中的主要联系人信息。

Amazon Web Services 管理控制台

编辑独立版的主要联系人 Amazon Web Services 账户 或管理账户

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

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

Amazon CLI & SDKs

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

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

注意

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

最小权限

对于各个操作，您必须具有映射到此操作的权限：

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

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

Example

以下示例检索了调用方账户的当前主要联系人信息。

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

Example

以下示例为调用方账户设置了新的主要联系人信息。

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

如果成功，此命令不会产生任何输出。

更新任何联系人的主要联系人 Amazon 您组织中的成员账户

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

其他要求

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

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

Amazon Web Services 管理控制台

编辑任何联系人的主要联系人 Amazon Web Services 账户 在你的组织中

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

Amazon CLI & SDKs

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

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

注意

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

最小权限

对于各个操作，您必须具有映射到此操作的权限：

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

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

Example

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

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

```
    "WebsiteUrl": "https://www.examplecorp.com"
  }
}
```

Example

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

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

如果成功，此命令不会产生任何输出。

视图 Amazon Web Services 账户 标识符

此信息是关于您注册 Amazon 使用注册 Amazon（高级）或激活了帐户的高级功能时查看 Amazon Web Services 账户 标识符的信息。要比较注册选项，请参阅[比较注册选项](#)。

Amazon 为每个 Amazon Web Services 账户标识符分配以下唯一标识符：

[Amazon Web Services 账户 ID](#)

一个 12 位数字（如 012345678901）用于唯一标识 Amazon Web Services 账户。许多 Amazon 资源在其[亚马逊资源名称 \(ARN\)](#) 中包含账户 ID。账户 ID 部分将一个账户中的资源与另一个账户中的资源区分开来。如果您是 Amazon Identity and Access Management (IAM) 用户，则可以使用账户 ID 或账户别名登录。Amazon Web Services 管理控制台 虽然应像任何识别信息一样谨慎使用和共享账户 ID，但不应将其视为机密、敏感或保密信息。

[规范用户 ID](#)

字母数字标识符，例

如 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be，它是 ID 的模糊形式。Amazon Web Services 账户 在使用亚马逊简单存储服务 (Amazon S3) 授予对存储桶和对象的跨账户访问权限 Amazon Web Services 账户 时，您可以使用此 ID 进行识别。您可以按[根用户](#)或 IAM 用户的身份检索 Amazon Web Services 账户 的规范用户 ID。

您必须通过身份验证 Amazon 才能查看这些标识符。

Warning

不要将您的 Amazon 证书（包括密码和访问密钥）提供给需要您的 Amazon Web Services 账户标识符才能与您共享 Amazon 资源的第三方。这样做将使他们获得与您相同的访问权限。
Amazon Web Services 账户

找到你的 Amazon Web Services 账户 ID

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

以根用户身份查找您的账户 ID

Amazon Web Services 管理控制台

为了找到你的 Amazon Web Services 账户 以 root 用户身份登录时的 ID

最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当以根用户身份登录时，您不需要任何 IAM 权限。

1. 在右上角的导航栏中，请选择您的账户名称或编号，然后选择安全凭证。

Tip

如果您没有看到安全凭证页面，您可以用 IAM 角色的联合用户身份登录，而非 IAM 用户身份登录。在这种情况下，请查找账户条目及其旁边的账户 ID 号。

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

Amazon CLI & SDKs

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

最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当以根用户身份运行命令时，您不需要任何 IAM 权限。

按如下方式使用 [get-caller-identity](#) 命令。

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

以 IAM 用户身份查找账户 ID

Amazon Web Services 管理控制台

为了找到你的 Amazon Web Services 账户 以 IAM 用户身份登录时的 ID

最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- `account:GetAccountInformation`

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

Tip

如果您没有看到安全凭证页面，您可以用 IAM 角色的联合用户身份登录，而非 IAM 用户身份登录。在这种情况下，请查找账户条目及其旁边的账户 ID 号。

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

Amazon CLI & SDKs

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

最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

- 当以 IAM 用户或角色的身份运行命令时，您必须具有：
 - `sts:GetCallerIdentity`

按如下方式使用 [get-caller-identity](#) 命令。

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

查找您的权威用户 ID Amazon Web Services 账户

您可以使用 Amazon Web Services 管理控制台 或来查找您的 Amazon Web Services 账户 权威用户 ID。Amazon CLI 的权威用户 ID 特定 Amazon Web Services 账户 于该账户。您可以检索您 Amazon Web Services 账户 作为根用户、联合用户或 IAM 用户的权威用户 ID。

以根用户或 IAM 用户的身份查找规范 ID

Amazon Web Services 管理控制台

在您以根用户或 IAM 用户身份登录控制台时查找您的账户的规范用户 ID

最小权限

要执行下列步骤，您必须至少具有以下 IAM 权限：

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

1. 以根用户或 IAM 用户身份登录。Amazon Web Services 管理控制台
2. 在右上角的导航栏中，请选择您的账户名称或编号，然后选择安全凭证。

i Tip

如果您没有看到安全凭证页面，您可以用 IAM 角色的联合用户身份登录，而非 IAM 用户身份登录。在这种情况下，请查找账户条目及其旁边的账户 ID 号。

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

Amazon CLI & SDKs

要查找权威用户 ID，请使用 Amazon CLI

相同的 Amazon CLI 和 API 命令适用于 Amazon Web Services 账户根用户、IAM 用户或 IAM 角色。

按如下方式使用 [list-buckets](#) 命令。

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

以具有 IAM 角色的联合用户身份查找规范 ID

Amazon Web Services 管理控制台

在以具有 IAM 角色的联合用户身份登录控制台时查找账户的规范用户 ID

i 最小权限

- 您必须拥有列出和查看 Amazon S3 存储桶的权限。

1. 使用 IAM 角色以联合用户身份登录。Amazon Web Services 管理控制台
2. 在 Amazon S3 控制台中，请选择存储桶名称，来查看存储桶详细信息。

3. 选择权限选项卡。
4. 在访问控制列表部分的存储桶拥有者下，将显示 Amazon Web Services 账户 的规范 ID。

Amazon CLI & SDKs

要查找权威用户 ID，请使用 Amazon CLI

相同的 Amazon CLI 和 API 命令适用于 Amazon Web Services 账户根用户、IAM 用户或 IAM 角色。

按如下方式使用 [list-buckets](#) 命令。

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

排除您的故障 Amazon Web Services 账户

此信息用于对 Amazon Web Services 账户 您注册 Amazon 使用注册 Amazon（高级）或激活帐户的高级功能进行故障排除。要比较注册选项，请参阅[比较注册选项](#)。

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

故障排除主题

- [对问题进行故障排除 Amazon Web Services 账户 创建](#)
- [对问题进行故障排除 Amazon Web Services 账户 关闭](#)
- [对其他问题进行故障排除 Amazon Web Services 账户](#)

对问题进行故障排除 Amazon Web Services 账户 创建

本信息是关于在注册 Amazon 使用“注册 Amazon（高级）”或激活了帐户的高级功能时对 Amazon Web Services 账户 创建问题进行故障排除。要比较注册选项，请参阅[比较注册选项](#)。

使用下表中的参考链接来帮助您诊断和修复创建新文件时出现的问题 Amazon Web Services 账户。

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

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

对问题进行故障排除 Amazon Web Services 账户 关闭

本信息用于解决在您注册 Amazon 使用“注册 Amazon (高级)”或激活帐户的高级功能时出现的 Amazon Web Services 账户 关闭问题。要比较注册选项，请参阅[比较注册选项](#)。

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

主题

- [我不知道如何删除或取消我的账户](#)
- [我在“账户”页面上看不到“关闭账户”按钮](#)

- [我关闭了账户，但仍未收到确认电子邮件](#)
- [我在尝试关闭账户时收到 ConstraintViolationException “” 错误](#)
- [我在尝试关闭成员账户时收到一条“CLOSE_ACCOUNT_QUOTA_EXCEEDED”错误](#)
- [我需要删除我的 Amazon 关闭管理账户之前的组织？](#)

我不知道如何删除或取消我的账户

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

我在“账户”页面上看不到“关闭账户”按钮

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

我关闭了账户，但仍未收到确认电子邮件

该确认邮件仅发送至 Amazon Web Services 账户的 Amazon Web Services 电子邮件地址。如果您在几个小时内没有收到此电子邮件，则可以以 root 用户 Amazon Web Services 管理控制台 身份[登录](#)以检查您的账户是否已关闭。如果您的账户已成功关闭，您将看到一条显示账户已关闭的信息。如果您关闭的账户是成员账户，则可以通过检查已关闭的账户是否在 Amazon Organizations 控制台CLOSED中标记为一样来验证关闭成功。有关更多信息，请参阅《Amazon Organizations 用户指南》中的[关闭组织中的成员账户](#)。

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

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

你正在尝试使用 Amazon 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根用户 Amazon Web Services 管理控制台 [身份](#)登录，然后从“帐户”页面将其关闭。有关更多信息，请参阅《Amazon Organizations 用户指南》中的[关闭组织中的管理账户](#)。

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

在连续30天内，您只能关闭20%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20%的账户关闭限额。即使20%的账户超过1000个，

最低账户关闭量为250个，最大账户关闭量为1000个。有关 Organizations 配额的更多信息，请参阅《Amazon Organizations 用户指南》中的 [Amazon Organizations 配额](#)。

我需要删除我的 Amazon 关闭管理账户之前的组织？

不，在关闭管理账户之前，您无需删除您的 Amazon 组织。但是只有当组织没有任何活跃的成员账户时，您才能关闭管理账户。要确认您的组织中没有剩余的活跃成员账户，请访问 Amazon Organizations 控制台，确保所有成员账户都显示在其账户名称 Closed 旁边。然后就可以关闭管理账户。

对其他问题进行故障排除 Amazon Web Services 账户

此信息用于解决您在注册 Amazon 使用“注册 Amazon（高级）”或为帐户激活高级功能时遇到的其他问题。Amazon Web Services 账户 要比较注册选项，请参阅[比较注册选项](#)。

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

问题

- [我需要为我的信用卡换一张信用卡 Amazon Web Services 账户](#)
- [我需要举报欺诈行为 Amazon Web Services 账户 活动](#)
- [我需要关闭我的 Amazon Web Services 账户](#)

我需要为我的信用卡换一张信用卡 Amazon Web Services 账户

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

我需要举报欺诈行为 Amazon Web Services 账户 活动

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

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

我需要关闭我的 Amazon Web Services 账户

有关解决关闭时遇到的问题的帮助 Amazon Web Services 账户，请参阅[关闭一个 Amazon Web Services 账户](#)。

管理印度地区的账户

如果您 Amazon 使用注册 Amazon（高级）注册或为帐户激活了高级功能，则此信息是关于在印度管理账户的信息。要比较注册选项，请参阅[比较注册选项](#)。

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

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

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

主题

- [创建一个 Amazon Web Services 账户 用 Amazon 印度](#)
- [管理您的客户验证信息](#)

创建一个 Amazon Web Services 账户 用 Amazon 印度

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

报名参加 Amazon 在印度的账户

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

Note

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

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

5. 输入您的公司或个人联系信息。如果您的联系地址或账单地址位于印度，则根据印度计算机应急响应小组 (CERT-In) 的规定，Amazon 在授予您使用 Amazon 服务的权限之前，必须收集和验证您的身份信息。

您在联系人或账单信息之间选择的姓名必须与您计划用于客户验证的文件上显示的姓名完全一致。例如，如果计划使用公司注册证书验证企业账户，您必须提供证书上显示的公司名称。有关可接受的证件类型列表，请参阅 [the section called “接受的用于客户验证的印度证件”](#)。

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

 Note

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

13. 选择要用于客户验证的姓名。

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

14. 同意提交信息进行验证，然后选择继续。

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

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

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

Note

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

管理您的客户验证信息

根据印度计算机应急响应小组 (CERT-In) 的规定，Amazon 在授予您新的或持续的 Amazon 服务访问权限之前，必须收集和验证您的身份信息。您的身份必须使用您提供的印度账单或联系地址中的姓名进行验证。在验证过程中，Amazon 将检查证件编号是否有效，以及您提供的姓名是否与您用于客户验证的文件关联的姓名相符。您从联系人或账单信息中选择的姓名必须与证件上显示的姓名完全一致。

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

查看客户验证状态

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

如果您的管理账户启用了客户验证继承功能，则您的账户的验证状态将反映该账户的状态。当继承处于活动状态时，您无需采取任何操作。

创建您的客户验证信息

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

1. 登录到 [Amazon Web Services 管理控制台](#)。

2. 在右上角的导航栏中，选择账户名称（或别名），然后选择账户。
3. 在其他设置下，选择客户验证。

如果之前尚未提供客户验证信息，您会看到创建客户验证页面。

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

您将通过电子邮件或 Health Amazon Dashboard 收到客户验证结果和任何后续步骤的通知。

编辑您的客户验证信息

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

如果您编辑用于客户验证的姓名或文件类型，或者更新任何文件信息，则在保存更改时必须再次验证您的身份。

验证继承处于活动状态

如果您的管理账户启用了客户验证继承功能，则无法编辑或提交自己的客户验证信息。您的验证信息以只读模式显示。

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

更新信息时，请注意以下指南：

- 如果选择不同的姓名，则该姓名必须与您计划用于客户验证的证件上的姓名完全一致。例如，如果计划使用公司注册证书验证企业账户，您必须提供证书上显示的公司名称。
- 如果选择其他证件类型，您需要上传证件正面和背面（如果适用）的副本。证件上传中的所有信息都应清晰可见。

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

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

5. 选择提交。

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

管理客户验证继承 Amazon Organizations

使用 [Amazon Org](#) anizations，您可以为组织启用客户验证继承功能。启用继承后，组织中的 India-based 成员账户将继承您的管理账户的验证状态。他们不需要独立完成客户验证。

您的管理账户必须先完成自己的客户验证，然后才能启用继承。启用继承后，您无需重新提交验证文件。

当您的管理账户启用客户验证继承功能时，您的验证状态将延伸到您组织中的 India-based 成员账户。对于这些会员账户，我们可能会根据执法部门或监管部门的要求使用或披露您的验证信息。

启用或禁用客户验证继承

使用以下步骤为组织的 India-based 成员账户开启或关闭客户验证继承功能。

1. 打开 a Amazon Web Services 管理控制台 t [Amazon Web Services 管理控制台](#)。
2. 在导航栏上，选择您的账户名（或别名），然后选择账户。
3. 在其他设置下，选择客户验证。
4. 在“客户验证设置”下，打开继承开关以启用继承，或者关闭以禁用继承。
5. 查看确认对话框，然后确认您的选择。

启用继承后，组织中的所有 India-based 成员账户都将继承您的验证状态。当您禁用继承时，我们会恢复之前完成自己验证的成员账户之前的验证状态。未经事先验证的会员账户必须独立完成客户验证。

的客户验证 Amazon Organiations

如果您的账户有 India-based 联系人或账单地址，则您将继承管理账户的验证状态。这适用于您的管理账户启用了客户验证继承功能。您可以在客户验证页面上看到一条确认这一点的消息。

当继承处于活动状态时，您无法提交或编辑自己的客户验证信息。您无需采取任何行动。

如果您的管理账户禁用继承，则必须拥有自己的客户验证状态。如果您的账户退出组织，或者管理账户将您的账户从组织中移除，则同样适用。如果您之前提交了自己的验证信息，我们会恢复您之前的验证状态。您无需重复该过程。仅当您的姓名和地址自上次验证以来没有更改时，此恢复才适用。

接受的用于客户验证的印度证件

接受印度政府签发的以下证件类型进行客户验证。

Note

以下链接可能会由政府更改。

- **PAN 卡 - 永久账号 (PAN)** 卡有数字和实体卡两种格式，其中含有印度所得税部门向个人、公司和实体签发的唯一字母数字标识符。PAN 由十个字符组成，包括字母和数字，格式为 **AAAAA1111A**。要使用此证件进行验证，您还必须提供 PAN 证件上显示的出生日期（个人）或注册日期（企业），并上传卡片的正面。请访问[所得税部门的官方网站](#)，查看您的 PAN 的有效性。
- **选民身份证 Card/EPIC** —— 选民身份证，也称为选民带照片的身份证（EPIC），包含印度选举委员会向印度符合条件的选民签发的唯一识别码。选民 ID/EPIC 号码由十个字符组成，包括字母和数字。你可以去[印度选举委员会](#)的官方网站查看你的选民身份证的有效性。要使用此证件进行验证，您必须上传卡片的正面和背面。
- **驾驶执照** - 如果您的驾驶执照不是由印度联邦颁发的，我们建议使用其他证件类型进行验证。驾驶执照号码由 12-16 个字符组成，包括字母、数字、空格和连字符。要使用此证件进行验证，您必须提供出生日期并上传卡片的正面和背面。您可以访问道路运输和公路部的[Parivahan Sewa 网站](#)，检查您驾驶执照的有效性。
- **公司注册证书** - 公司注册证书是由印度公司事务部（MCA）签发的证件，上面注明了企业注册为法人实体的日期。证书用于唯一标识和跟踪在印度注册的公司。每份证书都包含公司识别号 (CIN)，这是一个由 21 个字符（包括字母和数字）组成的唯一字母数字标识符。要使用此证件进行验证，您必须上传公司注册证书证件。您可以前往[印度公司事务部门门户网站](#)检查您的 CIN 是否有效。

个人和企业账户接受的印度证件类型不同：

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

管理你的 Amazon 在印度的账户

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

使用 Amazon Web Services 管理控制台 执行以下任务：

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

关闭一个 Amazon Web Services 账户

这些说明用于说明 Amazon Web Services 账户 如果您 Amazon 使用注册 Amazon (高级) 注册或为帐户激活了高级功能，如何关闭您的。要比较注册选项，请参阅[比较注册选项](#)。

如果您不再需要您的 Amazon Web Services 账户，可以按照本节中的说明随时将其关闭。关闭账户后，您可以自账户关闭之日起 90 天内将其重新打开。从您关闭账户之日到 Amazon 永久关闭账户之间的这段时间称为[关闭后期限](#)。

关闭账户前的注意事项

在关闭之前 Amazon Web Services 账户，应考虑以下几点：

- 关闭账户将视作您通知终止该账户的 Amazon 客户协议。
- 在关闭资源 Amazon Web Services 账户 之前，您无需删除其中的资源。但是，我们建议备份要所有保留的资源或数据。有关如何备份特定资源的说明，请参阅该服务的相应 [Amazon 文档](#)。
- 您可以在[后关闭期](#)重新打开账户。如果重新打开账户，则账户中剩余的服务将重新开始收费。您仍需对任何未付的发票以及未结的[预留实例](#)和[节省计划](#)付款。
- 您仍需对账户关闭前所用服务的所有未结费用和收费付款。关闭账户后，您将在下个月收到账 Amazon 单。例如，如果您在 1 月 15 日关闭了账户，则您将在 2 月初收到 1 月 1 日至 15 日期间所产生使用量的账单。关闭账户后，您将继续收到[预留实例](#)和[节省计划](#)的发票，直至发票过期。
- 您将无法再访问您账户中以前提供的 Amazon 服务。但是，在关闭[后 Amazon Web Services 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[Amazon Web Services 支持](#)。

- 您不能在关闭时将注册到 Amazon Web Services 账户 的电子邮件地址用作其他 Amazon Web Services 账户的主要电子邮件。如果想在不同的 Amazon Web Services 账户使用相同的电子邮件地址，我们建议在关闭之前对其进行更新。有关更多信息，请参阅 [更新 亚马逊 Web Services 电子邮件地址](#)。
- 您不能将您在账户关闭时注册的相同账户别名用于其他账户 Amazon Web Services 账户。Amazon Web Services 账户 要为其他账户重复使用别名 Amazon Web Services 账户，请在关闭账户之前删除账户别名。有关更多信息，请参阅 IAM 用户指南中的 [使用别名作为您的 Amazon Web Services 账户 ID](#)。
- 如果已经针对 Amazon Web Services 账户 根用户启用 [多重身份验证 \(MFA\)](#)，或者已配置 [IAM 用户上的 MFA 设备](#)，则在关闭账户时不会自动删除 MFA。如果您选择在 [后关闭期](#) 90 天内保持 MFA 开启状态，请让 MFA 设备保持活动状态直到后关闭期到期，以防需要在此期间访问该账户。请注意，账户永久关闭后，硬件 TOTP 令牌设备无法与其他用户关联。如果随后想将硬件 TOTP 令牌用于其他用户，可以选择在关闭账户之前 [停用硬件 MFA 设备](#)。适用于 [IAM 用户](#) 的 MFA 设备必须由账户管理员删除。

成员账户的其他注意事项

- 当您关闭成员账户时，该账户会在 [后关闭期结束](#) 后从组织中删除。在后关闭期内，已关闭的成员账户仍会计入组织中的账户配额。为了避免将账户计数计入账户限额，请在关闭账户之前，参阅 [从您的组织中删除成员账户](#)。
- 在连续的 30 天内，您只能关闭 20% 或 250 个成员账户，最多可关闭 1,000 个，以较高者为准。此限额不受日历月的限制，而是在您关闭账户时开始。有关 Organizations 限额的更多信息，请参阅 [Amazon Organizations 的限额](#)。
- 如果您使用 Amazon Control Tower，则需要先取消对成员账户的管理，然后再尝试关闭该账户。请参阅《Amazon Control Tower 用户指南》中的 [取消管理成员账户](#)。

特定服务的注意事项

- Amazon Web Services Marketplace 账户关闭后，订阅不会自动取消。如果有任何订阅，首先 [终止订阅中软件的所有实例](#)。然后，前往 Amazon Web Services Marketplace 控制台的“[管理订阅](#)”页面并取消您的订阅。
- 账户关闭后，我们 Amazon 将在最多五天内每天发送电子邮件，然后我们才会暂停该域名。域被暂停后，根据域的注册商，我们将在 30 天内删除域或将其释放给其注册商。有关更多信息，请参阅 [“我的 Amazon Web Services 账户 已关闭或永久关闭”，以及我的域名已在 Route 53 中注册](#)。

如果此账户的 root 用户的电子邮件地址使用通过 Route 53 在同一个账户中注册的域，则在完成以下操作之一之前，请勿关闭此帐户：将该域转移到其他账户 Amazon Web Services 账户，或者更新根用户电子邮件地址以使用未在此账户中注册的域。否则，关闭账户会暂停域名，从而中断向根用户地址发送电子邮件。没有电子邮件，您就无法恢复帐户；如果没有帐户，则无法恢复域名。30 天后，Route 53 将永久删除该域。这也适用于根用户电子邮件地址使用在此账户中注册的域名的成员账户。

- Amazon CloudTrail 是一项基础安全服务。这意味着，用户创建的跟踪即使在关闭后仍可以继续存在并传递事件，除非用户在关闭 Amazon Web Services 账户 之前明确删除了其中的跟踪。Amazon Web Services 账户 有关如何在关闭后请求删除跟踪的更多信息，请参阅《CloudTrail 用户指南》中的[Amazon Web Services 账户 闭包和跟踪](#)。Amazon Web Services 账户

如何关闭您的账户

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

如果在关闭账户的过程中遇到任何问题，请参阅[对问题进行故障排除 Amazon Web Services 账户 关闭](#)。

Standalone account

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

从“账户”页面关闭独立账户

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

Note

其中一个 Amazon 软件开发工具包 Amazon CLI 的 API 操作不支持此任务。您只能使用来执行此任务 Amazon Web Services 管理控制台。

Member account

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

要从中关闭成员帐户 Amazon Organizations 控制台

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

Note

如果您的组织使用[整合账单](#)模式，您将无法在控制台中看到关闭帐户按钮。要在整合账单模式下关闭帐户，请以根用户身份登录要关闭的帐户。在帐户页面上，选择关闭帐户按钮，输入帐户 ID，然后选择关闭帐户按钮。

4. 阅读并确保理解帐户关闭指南。
5. 输入成员帐户 ID，然后选择关闭帐户，启动帐户关闭流程。

Note

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

从“帐户”页面关闭成员帐户

或者，您可以直接从中的[帐户页面](#)关闭 Amazon 成员帐户 Amazon Web Services 管理控制台。有关分步指导，请遵照独立帐户选项卡中的说明。

使用 Amazon CLI 和 SDK 关闭成员账户

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

Management account

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

Note

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

从“账户”页面关闭管理账户

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

Note

其中一个 Amazon 软件开发工具包 Amazon CLI 的 API 操作不支持此任务。您只能使用来执行此任务 Amazon Web Services 管理控制台。

Amazon GovCloud (US) account

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

关闭 Amazon GovCloud (US) 账户

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

账户关闭后会发生什么

在关闭账户后，会立即发生以下情况：

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

并非所有地区和服务都会立即关闭账户，可能需要几个小时才能完成。

Post-closure 时期

关闭后期是指从您关闭账户之日到 Amazon 永久关闭账户 Amazon Web Services 账户之间的时间长度。后关闭期为 90 天。在后关闭期间，您只能通过重新开立账户来访问内容或 Amazon 服务。关闭后期限过后，将 Amazon 永久关闭您的 Amazon Web Services 账户，您将无法再重新开放。Amazon 还将删除您账户中的内容和资源（CloudTrail 路径除外）。账户永久关闭后，其[Amazon Web Services 账户 ID](#) 将永远无法重复使用。

重新打开你的 Amazon Web Services 账户

您的账户将在 90 天后永久关闭，之后您将无法重新打开账户，Amazon 并将删除账户中剩余的内容。要在账户永久关闭之前重新打开账户，请参阅[重新打开 Amazon Web Services 账户](#)。

Note

如果重新打开账户，则账户中剩余的服务将重新开始收费。

重新打开 Amazon Web Services 账户

如果您 Amazon Web Services 账户 已平仓但没有未清余额，则可以在[关闭后](#)期间自行重新开仓。

通过以 root 用户身份登录并从“帐户”页面提交请求，即可重新打开账户。

在重新开设账户之前你需要知道什么

在重新打开之前 Amazon Web Services 账户，请注意以下几点：

- Self-service 要求：只有在您自己关闭账户且账户关闭时您的账户没有未结余额的情况下，您才能使用此自助服务流程。您必须以已关闭账户的根用户身份登录；作为 IAM 用户或角色登录时，您无法重新打开账户。您必须在账户关闭后的 90 天内，即关闭账户后的期限内提交重新开放申请。
- 账户关闭者 Amazon：如果您的账户 Amazon 已关闭，则无法自行重新打开。在账户关闭之日起 30 天内支付所有未清余额，然后联系您[Amazon Web Services 支持](#)重新开设账户。
- 付款和费用：您的账户必须使用有效且未到期的付款方式。由于您上个月的账单将在下个月初完成，因此即使您的账户在关闭时没有余额，也可能在关闭之前有未清余额可供使用。要查看或支付余额，请参阅[付款](#)。当您重新开设账户时，仍在该账户中运行的所有服务将恢复收费。如果您在关闭账户之前没有停止这些服务，则在关闭账户后的期间也可能会产生费用。

如何重新开设账户

请按照以下步骤重新打开已关闭的账户。

Note

其中一个 Amazon 软件开发工具包 Amazon CLI 的 API 操作不支持此任务。只有使用才能执行此任务 Amazon Web Services 管理控制台。

从“帐户”页面重新打开您的账户

1. [以您要重新打开 Amazon Web Services 管理控制台的已关闭 Amazon Web Services 账户的 root 用户身份登录](#)。作为 IAM 用户或角色登录时，您无法重新打开账户。
2. 打开已关闭账户的账户页面，如下所示：在已关闭账户横幅中，选择重新打开账户。
3. 在“重新打开帐户”对话框中，输入对话框中显示的帐户 ID 以确认您要重新打开该帐户。
4. 选择“重新打开账户”以提交您的请求。一条消息确认账户重新开放已启动。

5. 等待重新打开完成。当您的账户再次处于活动状态时，系统会显示一条消息，确认该账户已成功重新开启，并且您的 Amazon 服务和账单已恢复。

如果 Amazon 无法重新打开您的账户，您会收到一条控制台通知，说明原因和解决方法。

重新开设账户后会发生什么

提交重新打开请求后，会发生以下情况：

- 要查看状态，请刷新“帐户”页面。重新开放完成后，账户将显示为活跃，关闭账户的横幅不再出现。
- 账户激活后，Amazon 恢复对其服务和资源的访问权限并恢复计费。

准备好账户以备重新开户后使用

某些资源和订阅不会自动恢复到运行状态。重新开设账户后，您可能需要执行以下操作才能恢复正常操作：

- 启动账户关闭时停止的所有 Amazon EC2 实例。有关更多信息，请参阅 Amazon EC2 用户指南中的[启动实例](#)。
- 从账户关闭时创建的快照中恢复 Amazon RDS 数据库。
- 取消并重新订阅任何 Amazon Web Services Marketplace 订阅。重新开设账户后，订阅不会自动恢复。

区域可用性

Self-service 所有商业区域均可重新开设账户。

中的安全性 Amazon 账户管理

云安全 Amazon 是重中之重。作为 Amazon 客户，您将受益于专为满足大多数安全敏感组织要求而构建的数据中心和网络架构。

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

- 云安全 — 负责保护 Amazon 在云中运行 Amazon 服务的基础架构 Amazon Web Services 云。Amazon 还为您提供可以安全使用的服务。Third-party 作为[Amazon 计划的一部分，审计师定期测试和验证我们的安全措施的有效性](#)。要了解适用于账户管理的合规计划，请参阅[Amazon Web Services 服务 中的合规计划](#)。
- 云端安全 — 您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您的要求以及适用的法律法规。

分担责任模式对所有人强制执行 Amazon Web Services 账户。这包括 Amazon Web Services 账户 您使用我们的新 Amazon 体验创建以及使用我们的高级 Amazon 体验创建的帐户。

本文档可帮助您了解在使用 Amazon 账户管理时如何应用分担责任模型。它说明了如何配置账户管理以实现您的安全性和合规性目标。您还将学习如何使用其他 Amazon 服务来监控和保护您的账户管理资源。其中一些文档仅与凭借我们的高级 Amazon 经验创建的账户相关。我们将确定何时文档仅与凭借我们的高级 Amazon 经验创建的账户相关。

主题

- [中的数据保护 Amazon 账户管理](#)
- [Amazon PrivateLink 适合 Amazon 账户管理](#)
- [Identity and Access Management Amazon 账户管理](#)
- [Amazon 的托管策略 Amazon 账户管理](#)
- [的合规性验证 Amazon 账户管理](#)
- [弹性在 Amazon 账户管理](#)
- [中的基础设施安全 Amazon 账户管理](#)

中的数据保护 Amazon 账户管理

以下信息与所有人相关 Amazon Web Services 账户。

分 Amazon [担责任模型](#)适用于 Amazon 账户管理中的数据保护。如本模型所述 Amazon，负责保护运行所有网络的全球基础设施 Amazon Web Services 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 Amazon Web Services 服务的安全配置和管理任务。有关数据隐私的更多信息，请参阅[Amazon 中国地区法律条款](#)。

出于数据保护的目的，我们建议您保护 Amazon Web Services 账户证书并使用 Amazon IAM Identity Center 或 Amazon Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 用于 SSL/TLS 与 Amazon 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 Amazon CloudTrail。有关使用 CloudTrail 跟踪捕获 Amazon 活动的信息，请参阅[Amazon CloudTrail 用户指南中的使用跟 CloudTrail 踪](#)。
- 使用 Amazon 加密解决方案以及其中的所有默认安全控件 Amazon Web Services 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果在 Amazon 通过命令行接口或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 终端节点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-3 版》<https://www.amazonaws.cn/compliance/fips/>。

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

Amazon PrivateLink 适合 Amazon 账户管理

以下信息与所有人相关 Amazon Web Services 账户。

如果您使用亚马逊虚拟私有云 (Amazon VPC) 托管 Amazon 资源，则无需通过公共互联网即可从 VPC 内部访问 Amazon 账户管理服务。

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

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

创建端点

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

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

Note

在创建端点时，请使用以下格式将账户管理指定为您希望 VPC 连接到的服务：

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

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

有关使用创建和配置终端节点的信息 Amazon CloudFormation，请参阅《用户指南》中的 [AWS::EC2::vpcEndPoint](#) 资源。Amazon CloudFormation

Amazon VPC 端点策略

通过在创建 Amazon VPC 终端节点时附加终端节点策略，您可以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端点策略来创建复杂的 IAM 规则。有关更多信息，请参阅：

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

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

以下信息与所有人相关 Amazon Web Services 账户。

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

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

以下示例显示了亚马逊 VPC 终端节点策略，该策略允许账户 123456789012 中一个名为 Alice 的 IAM 用户检索和更改任何人的备用联系信息 Amazon Web Services 账户，但拒绝所有 IAM 用户删除任何账户上的任何备用联系信息。

如果您想将属于某个 Amazon 组织的账户的访问权限授予该组织成员账户中的委托人，则该 Resource 元素必须使用以下格式：

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

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

Identity and Access Management Amazon 账户管理

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

以下信息与用于 Amazon 账户管理的 Identity and Access Management 有关。这些信息与您在我们的[高级 Amazon 体验](#)或为 Amazon Web Services 账户 账户激活高级功能时创建的信息最为相关。要了解访问控制如何为我们的新 Amazon 体验起作用，请参阅[比较访问管理](#)。

主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [操作方法 Amazon 账户管理与 IAM 配合使用](#)
- [Identity-based 的策略示例 Amazon 账户管理](#)
- [使用基于身份的策略（IAM 策略）Amazon 账户管理](#)
- [问题排查 Amazon 账户管理身份和访问权限](#)

受众

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

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅[问题排查 Amazon 账户管理身份和访问权限](#)）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅[操作方法 Amazon 账户管理与 IAM 配合使用](#)）
- IAM 管理员：编写用于管理访问权限的策略（请参阅[Identity-based 的策略示例 Amazon 账户管理](#)）

使用身份进行身份验证

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

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

Amazon Web Services 账户 根用户

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

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 Amazon Web Services 服务 使用临时证书进行访问。

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

IAM 用户和群组

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

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

IAM 角色

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

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

使用策略管理访问

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

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

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

Identity-based 政策

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

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

Resource-based 政策

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

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

其他策略类型

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

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《IAM 用户指南》中的 [IAM 实体的权限边界](#)。
- 服务控制策略 (SCP) – 指定 Amazon Organizations 中组织或组织单元的最大权限。有关更多信息，请参阅《Amazon Organizations 用户指南》中的 [服务控制策略](#)。
- 资源控制策略 (RCP) – 设置对账户中资源的最大可用权限。有关更多信息，请参阅《Amazon Organizations 用户指南》中的 [资源控制策略 \(RCP \)](#)。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的 [会话策略](#)。

多个策略类型

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

操作方法 Amazon 账户管理与 IAM 配合使用

这些信息与您在使用我们的高级 Amazon 体验时创建的信息最为 Amazon Web Services 账户 相关。要了解访问控制如何为我们的新 Amazon 体验起作用，请参阅[比较访问管理](#)。

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

您可以搭配使用的 IAM 功能 Amazon 账户管理

IAM 功能	账户管理支持
Identity-based 政策	是
Resource-based 政策	否
策略操作	是

IAM 功能	账户管理支持
策略资源	是
策略条件键	是
ACL	否
ABAC (策略中的标签)	否
临时凭证	是
主体权限	是
服务角色	否
Service-linked 角色	否

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

Identity-based 账户管理政策

支持基于身份的策略：是

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

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

Identity-based 账户管理的政策示例

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

Resource-based 账户管理中的政策

支持基于资源的策略：否

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

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

账户管理的策略操作

支持策略操作：是

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

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

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

账户管理中的策略操作在操作前使用以下前缀：

```
account
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

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

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

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

账户管理的策略资源

支持策略资源：是

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

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

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

账户管理服务在 IAM 策略的 Resource 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 Amazon Web Services 账户：

- account

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

- accountInOrganization

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

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

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

账户管理的策略条件键

支持特定于服务的策略条件键：是

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

Condition 元素根据定义的条件指定语句何时执行。您可以创建使用[条件运算符](#)（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 Amazon 全局条件键，请参阅 IAM 用户指南中的[Amazon 全局条件上下文密钥](#)。

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

- 账户:TargetRegion

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

- 账户:AlternateContactTypes

此条件键采用备用联系人类型的列表：

- BILLING
- OPERATIONS
- SECURITY

使用此键，您可以将请求筛选为仅针对指定备用联系人类型的操作。

- 账户:AccountResourceOrgPaths

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

```
o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
```

- 账户:AccountResourceOrgTags

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

- 账户:EmailTargetDomain

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowConditionKey",
      "Effect": "Allow",
```

```
    "Action": [
      "account:StartPrimaryEmailUpdate"
    ],
    "Resource": "*",
    "Condition": {
      "StringEqualsIgnoreCase": {
        "account:EmailTargetDomain": [
          "example.com",
          "company.org"
        ]
      }
    }
  }
}
```

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

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

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，但它们不使用 JSON 策略文档格式。

Attribute-based 使用账户管理进行访问控制

支持 ABAC（策略中的标签）：否

Attribute-based 访问控制 (ABAC) 是一种基于属性定义权限的授权策略。在 Amazon，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）和许多 Amazon 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

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

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

使用受支持条件密钥的示例 JSON 策略

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

JSON

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

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

将临时凭证用于账户管理

支持临时凭证：是

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

Cross-service 账户管理的委托人权限

支持转发访问会话 (FAS) : 是

转发访问会话 (FAS) 使用调用主体的权限 Amazon Web Services 服务，再加上 Amazon Web Services 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅[转发访问会话](#)。

账户管理的角色

支持服务角色 : 否

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

Service-linked 账户管理的角色

支持服务相关角色 : 否

服务相关角色是一种与服务相关联的 Amazon Web Services 服务角色。该服务可以代替您执行操作。Service-linked 角色出现在您的，Amazon Web Services 账户 并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

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

Identity-based 的策略示例 Amazon 账户管理

这些信息与您在使用我们的高级 Amazon 体验时创建的信息最为 Amazon Web Services 账户 相关。要了解访问控制如何为我们的新 Amazon 体验起作用，请参阅[比较访问管理](#)。

默认情况下，用户和角色没有创建或修改账户管理资源的权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

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

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

主题

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

策略最佳实践

Identity-based 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 Amazon Web Services 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 Amazon 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的 Amazon 托管策略。它们在你的版本中可用 Amazon Web Services 账户。我们建议您通过定义针对您的用例的 Amazon 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 [Amazon 托管策略](#) 或 [工作职能的 Amazon 托管策略](#)。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的策略和权限](#)。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 Amazon Web Services 服务，例如 Amazon CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 [使用 IAM Access Analyzer 验证策略](#)。
- 需要多重身份验证 (MFA)-如果 Amazon Web Services 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 [使用 MFA 保护 API 访问](#)。

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

使用中的“账户”页面 Amazon Web Services 管理控制台

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

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

对于仅调用 Amazon CLI 或 Amazon API 的用户，您无需为其设置最低控制台权限。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 Amazon Web Services 管理控制台

在以下示例中，您想要为 Amazon Web Services 账户 中的 IAM 用户授予对 Amazon Web Services 管理控制台中“账户”页面的只读访问权限。附加此策略的用户无法进行任何更改。

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

JSON

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

提供对“账户”页面的完全访问权限 Amazon Web Services 管理控制台

在以下示例中，您想要为 Amazon Web Services 账户 中的 IAM 用户授予对 Amazon Web Services 管理控制台中“账户”页面的完全访问权限。附加了此策略的用户可以修改账户的设置。

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

JSON

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

使用基于身份的策略（IAM 策略）Amazon 账户管理

这些信息与您在使用我们的高级 Amazon 体验时创建的信息最为 Amazon Web Services 账户 相关。要了解访问控制如何为我们的新 Amazon 体验起作用，请参阅[比较访问管理](#)。

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

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

Amazon 账户管理操作政策

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

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 Amazon Web Services 管理控制台，除了要用于修改该设置的权限（或许可）之外，您还必须允许该权限。

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

Note

此权限仅适用于控制台。此权限不支持 API 访问。

权限名称	访问级别	说明
account:DeleteAlternateContact	写入	授予权限以删除账户的备用联系人。
account:DisableRegion	写入	授予权限以禁用使用区域。
account:EnableRegion	写入	授予权限以启用使用区域。
account:PutAccountName	写入	授予权限以更新账户的名称。
account:PutAlternateContact	写入	授予权限以修改账户的备用联系人。
account:PutContactInformation	写入	授予权限以更新账户的主要联系人信息。
account:StartPrimaryEmailUpdate	写入	授予启动 Amazon 组织中成员账户主电子邮件地址更新的权限。

问题排查 Amazon 账户管理身份和访问权限

这些信息与您在使用我们的高级 Amazon 体验时创建的信息最为 Amazon Web Services 账户 相关。要了解访问控制如何为我们的新 Amazon 体验起作用，请参阅[比较访问管理](#)。

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

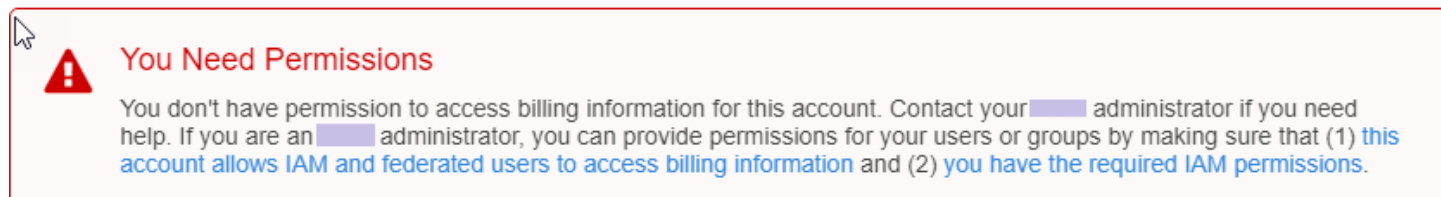
主题

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

我没有在“账户”页面中执行操作的权限

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

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



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

我无权执行 `iam:PassRole`

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

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

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

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

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

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

我想允许我以外的人进入 Amazon Web Services 账户 访问我的账户详情

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

Amazon 的托管策略 Amazon 账户管理

这些信息与您在使用我们的高级 Amazon 体验或为 Amazon Web Services 账户 账户激活高级功能时创建的信息最为相关。要了解访问控制如何适用于我们的新 Amazon 体验，请参阅[比较访问管理](#)。

Amazon 账户管理目前提供两种可供您使用的 Amazon 托管策略：

- [Amazon 管理策略：AWSAccountManagementReadOnlyAccess](#)
- [Amazon 管理策略：AWSAccountManagementFullAccess](#)
- [账户管理更新至 Amazon 托管策略](#)

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

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

您无法更改 Amazon 托管策略中定义的权限。如果 Amazon 更新 Amazon 托管策略中定义的权限，则更新会影响该策略所关联的所有主体身份（用户、组和角色）。Amazon 当新的 Amazon 托管策略启动或新 Amazon Web Services 服务的 API 操作可用于现有服务时，最有可能更新托管策略。

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

Amazon 管理策略：AWSAccountManagementReadOnlyAccess

您可以将 AWSAccountManagementReadOnlyAccess 策略附加到 IAM 身份。

该策略提供了仅查看以下内容的只读权限：

- 有关您的元数据 Amazon Web Services 账户
- 已启用或禁用的 Amazon Web Services 账户（您只能使用 Amazon 控制台查看账户中的区域状态）Amazon Web Services 区域

方法为：授予运行任何 Get* 或 List* 操作的权限。它不提供任何修改账户元数据或启用或禁用 Amazon Web Services 区域 用账户的功能。

权限详细信息

该策略包含以下权限。

- account— 允许委托人检索有关的元数据信息。Amazon Web Services 账户它还允许主体列出为 Amazon Web Services 管理控制台中的账户启用的 Amazon Web Services 区域。

JSON

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

Amazon 管理策略：AWSAccountManagementFullAccess

您可以将 AWSAccountManagementFullAccess 策略附加到 IAM 身份。

该策略提供查看或修改以下内容的完全管理权限：

- 有关您的元数据 Amazon Web Services 账户

- 已启用或禁用的 Amazon Web Services 账户（您只能使用 Amazon 控制台查看账户的状态或启用或禁用区域）Amazon Web Services 区域

方法为：授予运行任何 account 操作的权限。

权限详细信息

该策略包含以下权限。

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

JSON

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

账户管理更新至 Amazon 托管策略

查看自该服务开始跟踪这些变化以来账户 Amazon 管理政策更新的详细信息。有关此页面更改的自动提示，请订阅账户管理文档历史记录页面上的 RSS 源。

更改	描述	日期
Amazon 账户管理推出了新的 Amazon 托管政策，并开始跟踪变更	账户管理最初采用以下 Amazon 托管政策： <ul style="list-style-type: none">• AWSAccountManagementReadOnlyAccess	2021 年 9 月 30 日

更改	描述	日期
	<ul style="list-style-type: none"> AWSAccountManagementFullAccess 	

的合规性验证 Amazon 账户管理

我们的新 Amazon 体验不能用于任何受监管的工作负载。以下信息仅与您使用注册 Amazon（高级）时创建的帐户相关。

Third-party 审计师评估可 Amazon Web Services 账户 作为多个合规计划的一部分在您中运行的 Amazon 服务的安全性及 Amazon 合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规计划范围内的 Amazon 服务清单，请参阅[Amazon Web Services 服务 中的合规计划范围](#)。有关一般信息，请参阅[Amazon 合规计划](#)。

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

您在使用您的服务时的合规责任 Amazon Web Services 账户 由数据的敏感性、贵公司的合规目标以及适用的法律法规决定。Amazon 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，并提供了部署以安全性和合规性为重点 Amazon 的基准环境的步骤。
- [Amazon 规资源合规资源](#) — 这套工作手册和指南可能适用于您的行业和地点。
- [根据Amazon Config 开发人员指南](#)中的规则评估资源 — 该 Amazon Config 服务评估您的资源配置是否符合内部惯例、行业准则和法规。
- [Amazon Security Hub CSPM](#)— 这 Amazon Web Services 服务 可以全面了解您的安全状态 Amazon ，帮助您检查是否符合安全行业标准和最佳实践。

弹性在 Amazon 账户管理

以下信息与所有人相关 Amazon Web Services 账户。如果您使用我们的新 Amazon 体验，则需要考虑其他地区因素。有关更多信息，请参阅[Amazon Web Services 区域 为了你的项目](#)。

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

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

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

中的基础设施安全 Amazon 账户管理

以下信息与所有人相关 Amazon Web Services 账户。

作为托管 Amazon 服务，在您 Amazon Web Services 账户 中运行的服务受 Amazon 全球网络安全的保护。有关 Amazon 安全服务以及如何 Amazon 保护基础设施的信息，请参阅[Amazon 云安全](#)。要使用基础设施安全的最佳实践来设计您的 Amazon 环境，请参阅安全支柱架 Amazon 构完善框架[中的](#)基础设施保护。

您可以使用 Amazon 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。
- 具有完美向前保密 (PFS) 的密码套件，例如 DHE (短暂的) 或 ECDHE (椭圆曲线短暂的 Diffie-Hellman)。Diffie-Hellman 大多数现代系统 (如 Java 7 及更高版本) 都支持这些模式。

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

监视你的 Amazon Web Services 账户

这包括 Amazon Web Services 账户 您使用我们的新 Amazon 体验创建以及使用我们的高级 Amazon 体验创建的帐户。要比较注册选项，请参阅[比较注册选项](#)。

监控是维护 Amazon 账户管理和您的其他 Amazon 解决方案的可靠性、可用性和绩效的重要组成部分。Amazon 提供以下监控工具来监视账户管理，报告出现问题，并在适当时自动采取措施：

- Amazon CloudTrail捕获（日志）由您或代表您发起的 API 调用 Amazon Web Services 账户 和相关事件，并将日志文件写入您指定的亚马逊简单存储服务 (Amazon S3) 存储桶。这可以让您标识哪些用户和账户调用了 Amazon、发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅[Amazon CloudTrail 《用户指南》](#)。
- 亚马逊 EventBridge通过自动响应系统事件（例如应用程序可用性問題或资源更改）来进一步提高您的 Amazon 服务自动化程度。来自 Amazon 服务的事件几乎是实时传送到 EventBridge 的。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](#)。

日志记录 Amazon 使用账户管理 API 调用 Amazon CloudTrail

这包括 Amazon Web Services 账户 您使用我们的新 Amazon 体验创建以及使用我们的高级 Amazon 体验创建的帐户。要比较注册选项，请参阅[比较注册选项](#)。

Amazon 账户管理 API 与一项提供用户 Amazon CloudTrail、角色所采取操作记录的服务或调用账户管理操作的 Amazon 服务相集成。CloudTrail将所有账户管理 API 调用捕获为事件。捕获的调用包括对账户管理操作的所有调用。如果您创建跟踪，则可以开启向 Amazon S3 存储桶持续交付事件，包括账户管理操作的事件。CloudTrail 如果您未配置跟踪，仍可以在 CloudTrail 控制台的事件历史记录中查看最新事件。使用收集的信息 CloudTrail，您可以确定调用账户管理操作的请求、用于提出请求的 IP 地址、谁提出请求以及何时提出请求以及其他详细信息。

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

中的账户管理信息 CloudTrail

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

要持续记录您的事件 Amazon Web Services 账户，包括账户管理操作的事件，请创建跟踪。跟踪可以 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在中创建跟踪时 Amazon Web Services 管理控制台，该跟踪适用于所有人 Amazon Web Services 区域。此跟踪记录在 Amazon 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Amazon S3 存储桶。您可以配置其他 Amazon 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- [创建跟踪记录概述](#)
- [CloudTrail 支持的服务和集成](#)
- [为以下对象配置 Amazon SNS 通知 CloudTrail](#)
- [接收来自多个区域的 CloudTrail 日志文件](#)
- [接收来自多个账户的 CloudTrail 日志文件](#)

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

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

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

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

了解账户管理日志条目

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

示例 1：以下示例显示了调用操作的 CloudTrail 日志条目，该 GetAlternateContact 操作旨在检索帐户的当前 OPERATIONS 备用联系人。该记录信息不含此操作返回的值。

Example 示例 1

```
{
```

```

"eventVersion": "1.08",
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "ARO1234567890EXAMPLE:AccountAPITests",
  "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
  "accountId": "123456789012",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "ARO1234567890EXAMPLE",
      "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
      "accountId": "123456789012",
      "userName": "ServiceTestRole"
    },
    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-04-30T19:25:53Z"
    }
  },
},
"eventTime": "2021-04-30T19:26:15Z",
"eventSource": "account.amazonaws.com",
"eventName": "GetAlternateContact",
"awsRegion": "us-east-1",
"sourceIPAddress": "10.24.34.250",
"userAgent": "Mozilla/5.0",
"requestParameters": {
  "alternateContactType": "SECURITY"
},
"responseElements": null,
"requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
"eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012"
}

```

示例 2：以下示例显示了呼叫该操作的 CloudTrail 日志条目，该PutAlternateContact操作旨在向帐户添加新的BILLING备用联系人。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "PutAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "name": "*Alejandro Rosalez*",
    "emailAddress": "alrosalez@example.com",
    "title": "CFO",
    "alternateContactType": "BILLING"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

}

示例 3：以下示例显示了调用删除当前OPERATIONS备用联系人的DeleteAlternateContact操作的 CloudTrail 日志条目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    },
    "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"
}
```

使用以下方式监控账户管理事件 EventBridge

这包括 Amazon Web Services 账户 您使用我们的新 Amazon 体验创建以及使用我们的高级 Amazon 体验创建的帐户。要比较注册选项，请参阅[比较注册选项](#)。

亚马逊 EventBridge（以前称为 CloudWatch 事件）可帮助您监控特定事件并启动使用其他的目标操作 Amazon Web Services 服务。来自 Amazon Web Services 服务的事件近乎实时 EventBridge 地传送到。

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

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

账户管理事件

以下示例显示了账户管理的事件。事件会尽可能生成。

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

事件类型

- [启用和禁用区域的事件](#)

启用和禁用区域的事件

当通过控制台或 API 启用或禁用账户中的区域时，会启动异步任务。初始请求将作为 CloudTrail 事件记录在目标账户中。此外，当启用或禁用过程启动时，EventBridge 事件将发送到调用帐户，并在任一进程完成后再次发送事件。

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

```
{
  "version": "0",
  "id": "11112222-3333-4444-5555-666677778888",
  "detail-type": "Region Opt-In Status Change",
  "source": "aws.account",
```

```
{
  "account": "123456789012",
  "time": "2020-09-30T06:51:08Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:account::123456789012:account"
  ],
  "detail": {
    "accountId": "123456789012",
    "regionName": "ap-east-1",
    "status": "ENABLED"
  }
}
```

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

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

以下示例事件模式创建了一条捕获所有区域事件的规则。

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

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

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

```
    "status":[
      "DISABLED",
      "ENABLED"
    ]
  }
}
```

的配额 Amazon 账户管理

您的每项 Amazon 服务 Amazon Web Services 账户 都有默认配额，以前称为限制。

以下配额信息适用于您创建的项目（如果您使用）[报名参加 Amazon（新）](#)。要调整配额，请创建支持票证。有关更多信息，请参阅 [项目支持](#)。

资源	限额	可调整
您在免费计划中拥有的项目数量	29	否
您在付费计划中可以拥有的项目数量	299	否
您可以与之共享项目的人数	500	否
您可以接受的项目邀请数量	100	否

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

资源	限额
每个账户的 GetContactInformation 请求速率	每秒 3 个，突增到每秒 5 个
每个调用方账户的 GetPrimaryEmail 请求速率	每秒 3 个，突增到每秒 3 个
每个账户的 PutAlternateContact 请求速率	每秒 1 个，突增到每秒 6 个
每个账户的 PutContactInformation 请求速率	每秒 1 个，突增到每秒 2 个
每个调用方账户的 StartPrimaryEmailUpdate 请求速率	每秒 1 个，突增到每秒 1 个

《账户管理用户指南》的文档历史记录

下表描述了 Amazon 账户管理的文档版本。

变更	说明	日期
更新了账户关闭配额值	在疑难解答主题中，将账户关闭配额百分比从 10% 更正为 20%，并将最小值从 10 修正为 250。	2026年6月23日
新的账户名称 API	支持新的 GetAccountInformation 和 PutAccountName API，以便查看或修改账户名称。	2025 年 4 月 22 日
停止支持安全问题的编辑	由于支持已终止，因此已从指南中删除了编辑您的安全问题主题。	2025 年 1 月 6 日
重写“关闭账户”主题	全面修改了整个关闭账户主题，包括添加了如何关闭成员和管理账户的步骤。	2024 年 2 月 1 日
不再支持添加新的安全问题	添加了新内容，表示添加安全问题的选项已从账户页面中移除。	2024 年 1 月 5 日
不再支持 aws-portal 命名空间	Amazon 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	全面修改了整个区域主题，包括添加了展开和折叠控件。	2023 年 10 月 8 日

将根用户主题迁移到 IAM 用户指南中	将有关根用户的讨论整合到一个主题中，并添加了已迁移至 IAM 用户指南的根用户主题交叉引用链接。	2023 年 9 月 18 日
主账户联系人主题中添加了新的部分	添加了新的电话号码和电子邮件地址要求部分。	2023 年 9 月 12 日
新的联系人信息 API	支持新的 GetContactInformation 和 PutContactInformation API。	2022 年 7 月 22 日
Amazon 账户管理现在支持通过 Amazon Organizations 控制台更新备用联系人。	现在，您可以使用更新的 Amazon Organizations 托管政策提供的账户 API 权限，通过 Amazon Organizations 控制台更新组织的备用联系人。	2022 年 2 月 22 日
初始版本	《Amazon 账户管理参考指南》的首次发布	2021 年 9 月 30 日

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