



使用者指南

AWS 帳戶管理



AWS 帳戶管理: 使用者指南

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

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AWS 帳戶？	1
功能 AWS 帳戶	2
您是第一次 AWS 使用嗎？	3
支援和意見回饋	3
其他 AWS 資源	4
比較註冊選項	5
支援 AWS 服務 註冊 AWS（新）	5
AWS 服務 包含在新 AWS 體驗的免費方案中	5
AWS 服務 包含在我們新 AWS 體驗的付費計劃中	10
AWS 服務 不支援我們的新 AWS 體驗	12
選擇如何註冊 的考量事項 AWS	17
比較註冊選項的功能	17
比較存取管理	18
管理您的 AWS 帳戶	20
註冊 AWS（新）	23
使用註冊 for AWS（新） 進行註冊	25
後續步驟	26
使用 AWS 設定	26
連接 AI 編碼工具	27
將編碼工具連線至專案的考量事項	27
將您的 AI 編碼工具連接至您的專案	28
使用多個專案	29
AWS 專案擁有者的 動作	31
更新您的密碼	32
管理多重要素驗證 (MFA)	33
重點	33
新 AWS 體驗可用的 MFA 類型	33
註冊您的 MFA 裝置	35
將安全金鑰註冊為您的 MFA 裝置	36
重新命名 MFA 裝置	37
刪除您的 MFA 裝置	37
刪除所有工作階段	38
管理您的名稱或暱稱	38
變更您的電子郵件地址	39

編輯您的聯絡資訊	40
選擇不使用您的內容以改善服務	40
請求您的 AWS 建置器 ID 資料	41
建立專案	42
建立專案的考量事項	42
建立專案	42
AWS 區域 您的專案	43
尋找 AWS 區域 為您的專案選取的	44
在美國東部（俄亥俄）佈建區域資源的國家/地區 (us-east-2)	44
在亞太區域（雪梨）佈建區域資源的國家/地區 (ap-southeast-2)	47
在歐洲（斯德哥爾摩）佈建區域資源的國家/地區 (eu-north-1)	50
組織的受管政策	57
專案的服務控制政策	57
專案免費方案的服務控制政策	79
專案付費計劃的服務控制政策	90
專案的資源控制政策	101
在專案之間切換	103
從 切換作用中工作階段的專案 AWS 管理主控台	104
在 AWS 設定中的專案之間切換	104
從 切換專案 AWS 管理主控台	104
邀請團隊成員	105
團隊成員的考量事項	105
團隊成員如何存取您的 AWS 資源	106
邀請團隊成員	107
邀請團隊成員參與專案	107
從專案中移除團隊成員	108
移除團隊成員	108
撤銷邀請	109
重新傳送邀請	109
升級您的帳戶	110
升級帳戶的考量事項	110
升級您的帳戶	111
建立支出限制	111
什麼是支出限制？	111
設定您的花費限制	112
通知	112

使用選用的早期成本控制來自訂您的支出限制設定	112
如果您達到限制會發生什麼情況	114
其他需要注意的重要事項	114
在 AWS 設定中建立支出限制	114
更新支出限制	115
在 AWS 設定中更新支出限制	115
移除支出限制	116
在 AWS 設定中移除支出限制	116
免費方案	116
追蹤您的免費方案用量	117
獲得額外的點數	118
在 AWS 設定中檢視您的帳單資訊	119
依專案檢視您的成本	119
在 AWS 設定中檢視帳單歷史記錄	119
管理您的付款方式	120
在 AWS 設定中進行付款	121
在 AWS 設定中變更您偏好的貨幣	121
在 AWS 設定中管理稅務註冊	122
更新與刪除稅務登記號碼	122
管理您的美國免稅資料	123
檢視和兌換點數	123
管理印度的帳戶	124
向 AWS 印度註冊 AWS (新)	125
管理您的客戶驗證資訊	126
設定您的印度帳單	129
新增或編輯永久帳號	129
編輯多個永久帳號	129
編輯 Goods and Services Tax number	130
檢視稅務發票	130
變更往來 AWS 印度的記錄賣方	131
存取 AWS 支援	132
專案支援	132
Technical support (技術支援)	133
支援所有專案和組織是否關閉	133
開始商業支援 + 試用	133
監控您的專案	134

使用 AWS CloudTrail 監控您的專案	135
使用 CloudTrail 查看誰修改了您的專案	135
關閉專案	137
關閉專案之前您需要知道什麼	138
關閉專案	138
關閉後期間	139
重新開啟您的專案	139
啟用進階功能	139
啟用進階功能時會發生什麼情況	139
啟用進階功能之後的專案帳戶	141
啟用進階功能後 AWS ，設定會如何變更？	142
啟用進階功能後，我仍然可以在 AWS 設定中建立專案嗎？	143
如何準備啟用進階功能	143
如何啟用進階功能	143
啟用進階功能之後	144
設定根使用者密碼	144
管理人力資源成員	145
變更身分來源	147
移除組織政策	148
在 AWS 設定中關閉您的帳戶	149
關閉管理帳戶之前需要知道什麼	149
關閉專案	150
關閉您的管理帳戶	150
刪除您的 AWS 建置器 ID	150
註冊 AWS （進階）	152
步驟 1：建立您的帳戶	152
步驟 2：（建議）安裝 AWS CLI	154
步驟 3：（建議）設定 AWS MCP 伺服器	155
相關 AWS 服務	155
使用根使用者	156
存取您的帳戶	157
規劃您的控管結構	158
使用多個 的優點 AWS 帳戶	158
使用時機 AWS Organizations	159
使用時機 AWS Control Tower	165
了解 API 操作模式	165

設定您的帳戶	168
建立或更新您的帳戶別名	169
AWS 區域 在您的帳戶中啟用或停用	169
更新 的帳單 AWS 帳戶	179
更新根使用者電子郵件	179
更新根使用者密碼	183
更新 AWS 帳戶 名稱	184
更新 的替代聯絡人 AWS 帳戶	188
更新 的主要聯絡人 AWS 帳戶	196
檢視您的帳戶識別符	205
對您的帳戶進行故障診斷	210
帳戶建立問題	210
帳戶關閉問題	211
其他問題	213
管理印度的帳戶	214
AWS 帳戶 使用 AWS 印度建立	214
管理您的客戶驗證資訊	216
關閉您的帳戶	220
關閉帳戶之前您需要知道什麼	220
如何關閉您的帳戶	222
關閉帳戶後預期會發生的情況	224
重新開啟您的帳戶	225
重新開啟帳戶之前需要了解的事項	225
如何重新開啟您的帳戶	226
重新開啟帳戶後預期會發生的情況	226
重新開啟後準備您的帳戶以供使用	227
區域可用性	227
保護您的帳戶	228
資料保護	228
AWS PrivateLink	229
建立端點	230
Amazon VPC 端點政策	230
端點政策	230
身分和存取權管理	231
目標對象	231
使用身分驗證	232

使用政策管理存取權	233
AWS 帳戶管理和 IAM	234
身分型政策範例	241
使用身分型政策	244
疑難排解	246
AWS 受管政策	248
AWSAccountManagementReadOnlyAccess	248
AWSAccountManagementFullAccess	249
政策更新	250
法規遵循驗證	250
恢復能力	251
基礎設施安全性	252
監控您的帳戶	253
CloudTrail 日誌	253
CloudTrail 中的帳戶管理資訊	253
了解帳戶管理日誌項目	254
使用 EventBridge 監控帳戶管理事件	258
帳戶管理事件	258
配額	261
文件歷史紀錄	263
.....	cclxvi

什麼是 AWS 帳戶？

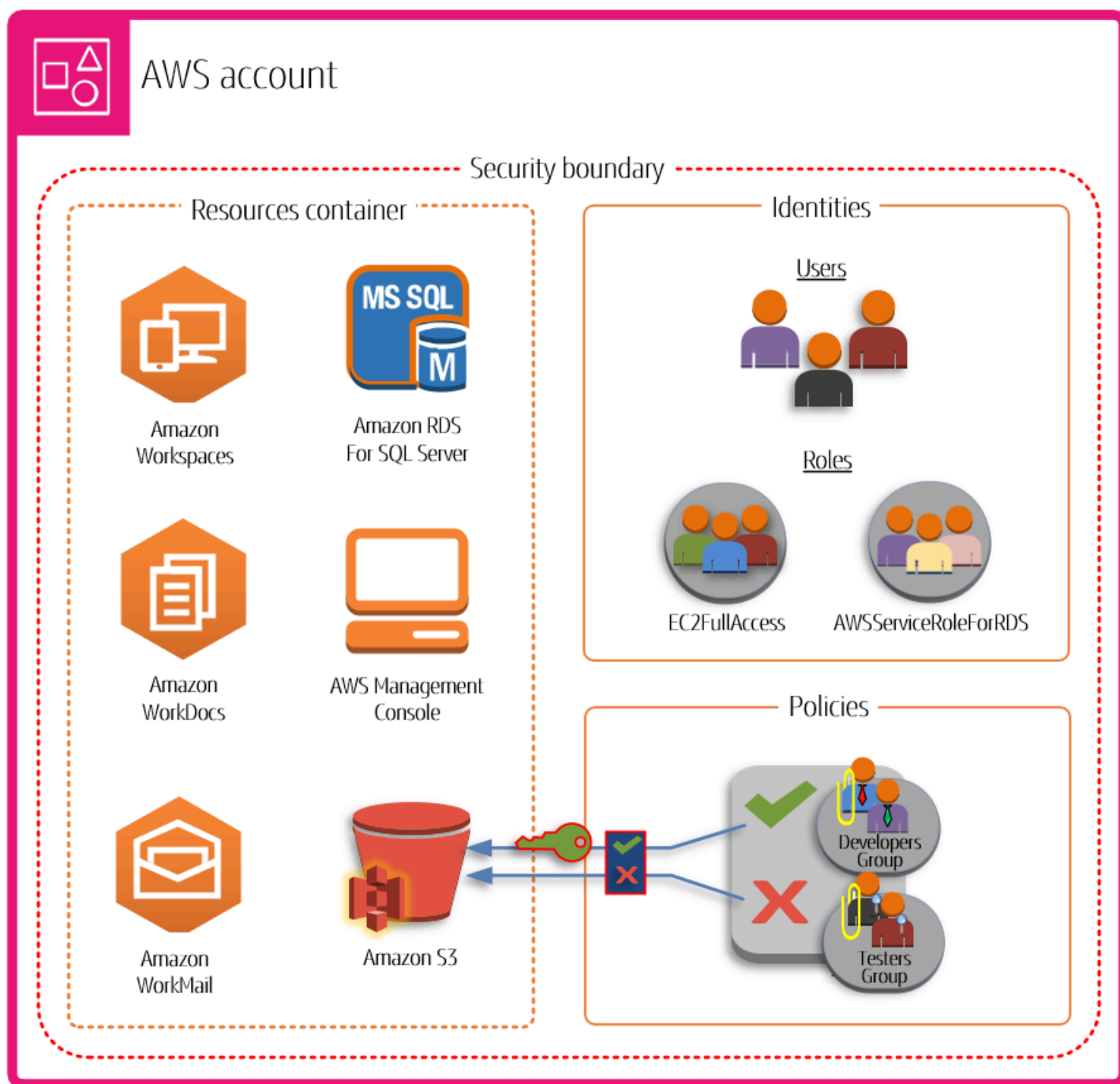
AWS 帳戶 代表與您建立的正式商業關係 AWS。您可以在 中建立和管理 AWS 資源 AWS 帳戶，而且您的帳戶提供存取和計費的身分管理功能。每個 AWS 帳戶 都有唯一的 ID，它與其他 ID 不同 AWS 帳戶。

註冊時 AWS，您可以選擇註冊 AWS（新）和註冊 AWS（進階）。根據您的選擇，您可以存取 AWS 帳戶 或 專案。專案包含與其他協作者共用的 AWS 帳戶 和 設定。如需詳細資訊，請參閱[比較註冊選項](#)。

您的雲端資源和資料包含在 中 AWS 帳戶。帳戶充當身分和存取管理隔離界限。當您需要在兩個帳戶之間共用資源和資料時，您必須明確允許此存取。根據預設，帳戶之間不允許存取。例如，如果您指定不同的帳戶來包含您的生產和非生產資源和資料，則預設不允許在這些環境之間進行存取。

AWS 帳戶 也是存取 AWS 服務的基本部分。如下圖所示，AWS 帳戶 提供兩個主要函數：

- 資源容器 – AWS 帳戶 是您以 AWS 客戶身分建立之所有 AWS 資源的基本容器。例如，Amazon Simple Storage Service (Amazon S3) 儲存貯體、Amazon Relational Database Service (Amazon RDS) 資料庫和 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體都是資源。每個資源都是由 Amazon Resource Name (ARN) 唯一識別，其中包含包含或擁有資源之帳戶的帳戶 ID。
- 安全界限 – AWS 帳戶 也是 AWS 資源的基本安全界限。您在帳戶中建立的資源可供擁有您帳戶登入資料的使用者使用。您可以在帳戶中建立的關鍵資源包括身分，例如使用者和角色。身分具有登入資料，可供某人用來登入 (驗證) AWS。身分也有許可政策，可指定使用者可以對帳戶中的資源執行哪些操作 (授權)。



使用多個 AWS 帳戶 是擴展您環境的最佳實務，因為它提供成本的自然帳單界限、隔離資源以確保安全、為個人和團隊提供靈活性，以及適應新的業務流程。如需詳細資訊，請參閱[使用多個的優點 AWS 帳戶](#)。

的功能 AWS 帳戶

AWS 帳戶 包含下列核心功能：

- **監控和控制成本** – 帳戶是配置 AWS 成本的預設方式。因此，針對不同的業務單位和工作負載群組使用不同的帳戶，可協助您更輕鬆地追蹤、控制、預測、預算和報告雲端支出。除了帳戶層級的成本報告之外，如果您 AWS Organizations 選擇在某個時間點使用，AWS 也具有內建支援，可合併和報告整個帳戶集的成本。您也可以使用 AWS Service Quotas 來協助保護您免於意外過度佈建 AWS 資源和惡意動作，進而大幅影響您的 AWS 成本。
- **隔離單位** – AWS 帳戶 為您的 AWS 資源提供安全、存取和計費界限，可協助您實現資源自主權和隔離。根據設計，帳戶內佈建的所有資源都會邏輯上與其他帳戶中佈建的資源隔離，即使在您自己的 AWS 環境中也是如此。此隔離界限可讓您限制應用程式相關問題、設定錯誤或惡意動作的風險。如果一個帳戶內發生問題，可以減少或消除對其他帳戶中所含工作負載的影響。
- **鏡像您的業務工作負載** – 使用多個帳戶，將不同帳戶中具有共同業務目的的工作負載分組。因此，您可以將所有權和決策與這些帳戶保持一致，並避免與其他帳戶中工作負載的安全和管理方式發生相依性和衝突。根據您的整體商業模式，您可以選擇隔離不同帳戶中的不同業務單位或附屬公司。這種方法也可能隨著時間的推移，簡化這些單位的分離。

您是第一次 AWS 使用嗎？

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

如果您是第一次使用 AWS，您的第一個步驟是註冊 AWS。您可以在完全控制帳戶組態和內容存放位置 AWS 帳戶 的中建立，這是 HIPAA 或 FedRAMP 等受管制工作負載的必要項目，也可以使用預先設定的預設值建立 AWS 帳戶。若要了解哪種註冊適合您，請參閱 [比較註冊選項](#)。

如需如何設定新帳戶的step-by-step說明，您可以在其中完全控制初始設定，請參閱 [註冊 AWS \(進階 \)](#)。

如需如何設定新帳戶的step-by-step說明，其中 會使用預先設定的預設值 AWS 建立帳戶，請參閱 [註冊 AWS \(新 \)](#)。

支援 AWS 帳戶管理

您可以使用[AWS 帳戶管理支援論壇](#)來張貼意見回饋和問題。如需 AWS 論壇的一般資訊，請參閱 [AWS re:Post](#)。

如果找不到您要尋找的答案 AWS re:Post，您可以使用 [建立帳戶或帳單相關支援案例](#) AWS 管理主控台。如需詳細資訊，請參閱[範例：建立帳戶和帳單的支援案例](#)。

其他 AWS 資源

- [AWS 訓練和課程](#) – 連結至以角色為基礎的特殊課程，以及可自行安排進度的實驗室，以協助強化您的 AWS 技能並取得實際經驗。
- [AWS 開發人員工具](#) – 開發人員工具和資源的連結，提供文件、程式碼範例、版本備註和其他資訊，協助您使用 建置創新應用程式 AWS。
- [AWS 支援 中心](#) – 建立和管理 AWS 支援案例的中樞。同時包含與其他實用資源的連結，例如論壇、常見技術問答集、服務運作狀態，以及 AWS Trusted Advisor。
- [AWS 支援](#) – Support 相關資訊的主要網頁 AWS，這是一個one-on-one的快速回應支援管道，可協助您在雲端中建置和執行應用程式。
- [聯絡我們](#) – 詢問有關 AWS 帳單、帳戶、事件、濫用和其他問題的聯絡中心。
- [AWS 網站條款](#) – 有關我們的著作權和商標、您的帳戶、授權和網站存取，以及其他主題的詳細資訊。

比較註冊選項

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

當您註冊時 AWS，即可解鎖全球最完整且廣泛採用的雲端。在最廣泛的全球基礎設施上，我們提供最強大的創新雲端和 AI 功能和專業知識選擇，具有業界領先的安全性、可靠性和效能。

有兩種註冊方式 AWS。如果您想要完全控制帳戶組態和內容的存放位置，或者如果您有受管制的工作負載，例如 HIPAA、FedRAMP，請使用 [註冊 AWS \(進階\)](#)。如果您是新使用者，並想要使用您已擁有的登入來登入，AWS 並在選取中建立 AWS 具有預先設定預設值的環境 [AWS 區域](#)，請使用 [註冊 AWS \(新\)](#)。

支援 AWS 服務 註冊 AWS (新)

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

當您使用註冊 AWS (新) 時，您可以存取免費方案。免費方案可讓您存取特定 AWS 服務。您可以將您的帳戶升級至付費計劃，以存取其他 AWS 服務和功能。若要了解如何升級您的帳戶，請參閱 [在 AWS 設定中升級您的帳戶](#)。

並非所有 AWS 服務都可用於註冊 AWS (新)。如果服務未列在下列任一清單中，或具有不支援的功能，您必須使用 [註冊 AWS \(進階\)](#) 或建立帳戶 [啟用進階 AWS 功能](#)。

AWS 服務 包含在新 AWS 體驗的免費方案中

下列 AWS 服務包含在註冊的免費方案 AWS (新) 中。任何服務都不支援多區域或跨區域功能。如需詳細資訊，請參閱 [AWS 區域 您的專案](#)。

- Amazon API Gateway
- Amazon Athena

- Amazon AppFlow
- AWS App2Container
- Amazon 增強版 AI
- Amazon Bedrock
- Amazon Bedrock 代理程式核心
- Amazon CloudFront
 - 不支援 Lambda@Edge。
- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon 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)
 - 不支援購買容量區塊和購買容量區塊延伸。
- 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
- Amazon OpenSearch Service
- Amazon Polly
- Amazon Quick
 - 僅支援 Amazon Quick Free 或 Quick Plus。如需詳細資訊，請參閱 [Amazon Quick 定價](#)。
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon Route 53
- Amazon SageMaker
- Amazon SageMaker AI
- Amazon SageMaker Unified Studio
- Amazon Simple Email Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service
 - 不支援 Amazon S3 Access Grants。
- Amazon Simple Workflow Service
- Amazon Verified Permissions
- Amazon Virtual Private Cloud
- Amazon Aurora
- Amazon Aurora DSQL
- AWS Amplify
- AWS AppConfig
- AWS AppSync
- Application Auto Scaling
- AWS Transform MGN
- AWS Artifact

- (HIPAA) 不支援 AWS 商業夥伴增補合約、(HIPAA) AWS 組織商業夥伴增補合約、AWS SEC 規則 17a-4 增補合約，以及 AWS SEC 規則 18a-6 增補合約。
- AWS B2B 資料交換
- AWS Backint Agent
- AWS Backup
- AWS Batch
- AWS 帳單與成本管理
 - 使用 AWS 設定來設定帳單、建立支出限制以控制成本，以及擷取和支付發票。您可以使用 Billing and Cost Management 來建立預算、分析和最佳化成本。如需詳細資訊，請參閱[使用 Billing and Cost Management 主控台搭配我們的新 AWS 體驗](#)。
- AWS Budgets
- AWS Certificate Manager
 - 不支援 [AWS Certificate Manager 匯出公有憑證](#)。
- AWS 雲端控制 API
- AWS Cloud Map
- AWS Cloud9
- AWS CloudFormation
- AWS CloudShell
- AWS CloudTrail
- AWS CodeArtifact
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- AWS Compute Optimizer
- AWS Config
- AWS Console Mobile Application
- AWS Cost Explorer
- AWS Data Pipeline
- AWS 資料傳輸

- AWS DataSync
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS 終端用戶訊息社交服務
- AWS Entity Resolution
- AWS Glue
- AWS Health
- AWS Identity and Access Management
- AWS IoT
 - AWS 不支援 Greengrass。
- AWS IoT Device Defender
- AWS IoT 裝置管理
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- AWS Lake Formation
- AWS Lambda
 - 不支援 Lambda@Edge。
- AWS Launch Wizard
- AWS License Manager
- AWS 管理主控台
- AWS Marketplace
 - 僅限 Bedrock 和 Free。
- AWS Network Manager
- AWS Payment Cryptography
- AWS PrivateLink
- AWS Resource Access Manager (RAM)
- AWS 資源總管
- AWS Resource Groups

- Route 53 Amazon 應用程式復原控制器 (ARC)
- AWS SDKs與工具
- AWS Secrets Manager
- AWS Security Token Service
- AWS Serverless Application Repository
- Service Quotas
- AWS Signer
- AWS Step Functions
- AWS 支援
- AWS Systems Manager
- 適用於 SAP 的 AWS Systems Manager
- AWS 使用者通知
 - 不支援使用者設定的通知和受管通知組態操作。如需詳細資訊，請參閱[什麼是 AWS 使用者通知？](#)
- AWS WAF
 - AWS 不支援 Shield。
- AWS Well-Architected Tool
- AWS X-Ray
- AWS CodeBuild
- Elastic Load Balancing
- AWS SQL Workbench
- Amazon OpenSearch Service Serverless
- Amazon Timestream

若要查看控制免費方案服務存取權的政策，請參閱 [專案免費方案的服務控制政策](#)。

AWS 服務 包含在我們新 AWS 體驗的付費計劃中

如果您有付費計劃，則可以註冊 AWS（新）下列服務。如需詳細資訊，請參閱在 [AWS 設定中升級您的帳戶](#)。任何服務都不支援多區域或跨區域功能。如需詳細資訊，請參閱[AWS 區域 您的專案](#)。

- Amazon DevOps Guru

- Amazon DocumentDB (with MongoDB compatibility)
- 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
- AWS AppFabric
- AWS Data Exchange
- AWS End User Messaging SMS
- AWS Fault Injection Service
- AWS Firewall Manager
- AWS Network Firewall
- AWS 安全代理程式
- AWS Storage Gateway
- DevOps 代理程式

若要查看控制付費計劃服務存取權的政策，請參閱 [專案付費計劃的服務控制政策](#)。

AWS 服務 不支援我們的新 AWS 體驗

除非您有 [啟用進階 AWS 功能](#)，否則新 AWS 體驗不支援下列 AWS 服務。新開發人員或小型團隊不需要這些服務 AWS。其中一些服務會自動為您的帳戶開啟並由 [管理 AWS](#)。如需詳細資訊，請參閱 [比較註冊選項的功能](#)。

- 企業版 Alexa
- Alexa Top Sites
- Alexa Web Information Service
- Amazon Braket
- Amazon Chime
- Amazon Chime Business 呼叫 AMCS LLC 銷售的服務
- Amazon Chime 呼叫我
- Amazon Chime 呼叫我 AMCS LLC 銷售的服務
- Amazon Chime Dial 由 AMCS LLC 銷售的服務
- Amazon Chime 撥入
- Amazon Chime 功能
- Amazon Chime SDK
- Amazon Chime Services
- Amazon Chime SMS
- Amazon Chime Voice Connector 是由 AMCS LLC 銷售的服務
- Amazon 雲端目錄
- Amazon CloudSearch
- Amazon CodeWhisperer
- Amazon Connect 客戶
- Amazon Connect 客戶設定檔
- Amazon Connect Customer Voice ID
- AWS Deadline Cloud
- Amazon Detective
- Amazon Elastic Inference

- Amazon Elastic Transcoder
- Amazon FinSpace
- Amazon Flexible Fleet
- Amazon Fraud Detector
- Amazon FSx
- Amazon GameLift Servers
- Amazon GameLift Streams
- Amazon GameSparks
- Amazon GuardDuty
- AWS HealthOmics
- Amazon Inspector Classic
- Amazon Interactive Video Service
- Amazon IVS 聊天功能
- Amazon Kendra
- Amazon Keyspaces (適用於 Apache Cassandra)
- 開羅
- Amazon Macie
- Amazon Managed Grafana
- Amazon Mechanical Turk
- Amazon Mechanical Turk 工作者獎勵
- Amazon Mobile Analytics
- Amazon Monitron
- Amazon Nimble Studio
- Amazon OpenSearch Service Ingestion Service
- Amazon Q
- Amazon Q Business
- Amazon Q Developer
- Amazon Quantum Ledger Database (Amazon QLDB)

- Amazon S3 on Outposts
- Amazon SageMaker Ground Truth
- Amazon Security Lake
- Amazon Sumerian
- Amazon WorkDocs
- Amazon WorkSpaces
- Amazon WorkSpaces 執行個體
- Amazon WorkSpaces 應用程式 (Amazon WorkSpaces 應用程式)
- Amazon WorkSpaces 精簡型客戶端
- Amazon WorkSpaces Web
- Amazon WorkLink
- Amazon WorkMail
- AWS 應用程式成本分析器
- AWS Clean Rooms
- AWS App Studio
- AWS Application Discovery Service
- AWS Audit Manager
- AWS Billing Conductor
- AWS CloudHSM
- AWS Client VPN
- AWS 雲端 WAN
- AWS Control Tower
- AWS 資料庫遷移服務
- AWS DeepRacer
- AWS Device Farm
- AWS Direct Connect
- AWS 彈性災難復原
- AWS Elemental Live

- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Elemental MediaPackage
- AWS Elemental MediaStore
- AWS Elemental MediaTailor
- AWS Global Accelerator
- AWS Ground Station
- AWS HealthImaging
- AWS IAM Identity Center
- AWS Identity and Access Management Access Analyzer
- AWS 互連
- AWS IoT 活動
- AWS IoT FleetWise
- AWS IoT RoboRunner
- AWS Mainframe Modernization
- AWS Migration Hub
- AWS Migration Hub Refactor Spaces
- AWS Modular Data Center
- AWS OpsWorks
- AWS Organizations
- AWS Outposts
- AWS Parallel Computing 服務
- AWS Partner Network
- AWS 定價計算工具
- AWS 私有憑證授權單位
- AWS Proton
- AWS re:Post Private

- AWS Resilience Hub
- AWS RoboMaker
- AWS RTB Fabric
- AWS Security Hub
- AWS 安全事件應變
- AWS Service Catalog
- AWS Shield
- AWS SimSpace Weaver
- AWS Snowball
- AWS Supply Chain
- AWS Telco Network Builder
- AWS Transform
- AWS Transfer Family
- AWS Transit Gateway
- AWS Trusted Advisor
- AWS Verified Access
- Site-to-Site VPN
- Amazon VPC Lattice
- AWS Wickr
- Amazon CodeCatalyst
- Amazon Comprehend Medical
- Conferencing 電信 (AMCS LLC 銷售的服務)
- 聯絡中心電信 (AMCS LLC 銷售的服務)
- 韓國電信聯絡中心
- 南非電信聯絡中心
- DynamoDB Accelerator
- Amazon Elastic VMware Service
- Oracle Database@AWS
- Red Hat OpenShift Service on AWS

- AWS App Runner

選擇如何註冊 的考量事項 AWS

選擇註冊方法之前，請考慮下列事項。您可以視需要啟用帳戶的所有 AWS 功能。

- 如果您有特定的產品需求，例如包含 HIPAA 或 FedRAMP 的受管制工作負載，請勿使用我們的新 AWS 體驗。
- 您的內容將存放在根據您的聯絡資訊選取的指定區域中。
- 新的 AWS 體驗可讓您更輕鬆地開始建置，而無需建立 AWS 許可。如果您需要精細控制使用者或角色型許可，請勿使用註冊 AWS（新）。
- 如果您需要由 設定帳戶特定的付款組態 AWS，也稱為網路條款帳單，請勿使用註冊 AWS（新）。
- 如果您需要存取整組 AWS 服務，請勿使用註冊 AWS（新）。如需詳細資訊，請參閱[支援 AWS 服務 註冊 AWS（新）](#)。

比較註冊選項的功能

下表比較註冊 AWS（新）或註冊 AWS（進階）支援的 AWS 廣泛需求。如果此資料表中未列出或中描述的功能[比較存取管理](#)，則可以使用此功能。如果您需要任何不支援的功能，您可以啟用帳戶的進階功能。如需詳細資訊，請參閱[啟用進階 AWS 功能](#)。

功能	註冊 AWS（新）	註冊 AWS（進階）
加入 AWS 合作夥伴網路	否	是
建立專業服務合約	否	是
使用 註冊 Enterprise 協議 AWS	否	是
購買 AWS 技能建置器團隊訂閱	否	是
使用 AWS 訓練合作夥伴	否	是
從 AWS 啟用獲得額外點數	否	是
使用 AWS Marketplace	否	是

功能	註冊 AWS (新)	註冊 AWS (進階)
將 AWS 您的帳戶指定為 HIPAA 或 SEC 合規	否	是
選取特定 AWS 區域 以建立您的區域資源	否。如需詳細資訊，請參閱 AWS 區域 您的專案 。	是
存取選擇加入區域	否	是
IAM Access Analyzer	否	是
登入存取政策	否	是
為您的帳戶建立支出限制	是	否
Savings Plans	否	是
為付費計劃自動選擇加入 Cost Optimization Hub	是	否
自動選擇加入 AWS Organizations	是	否
自動選擇加入 IAM Identity Center	是	否
自動選擇加入 IAM 角色管理員	是	否
主控台帳戶顏色	否	是
使用 AWS Console Mobile Application	否	是
停用多工作階段主控台支援	否	是。如果您使用建置器 ID 再次登入，系統會自動啟用多工作階段支援。

比較存取管理

當您使用我們的新 AWS 體驗時，會 AWS 建立預先設定的預設值，以協助您開始建置。您的 AWS 資源會組織在專案中。專案包含 AWS 帳戶，稱為專案帳戶，以及與其他協作者共用的設定。如果您使用

付費計劃，您的專案也可以有一組每月稅前成本，稱為支出限制。您擁有的所有專案都組成您的組織，您可以在 AWS 設定中透過管理帳戶進行控制。此組織與 AWS 組織相同；不過，AWS 會代表您管理此組織的層面。

AWS 會管理您 AWS Organization 的下列元素：

- 組織管理政策。當您使用我們的新 AWS 體驗時，會 AWS 管理組織管理政策，包括資源控制政策 (RCPs) 和服務控制政策 (SCPs)。如果您想要建立自己的，請使用註冊 AWS (進階)。
- 人工存取角色。人工存取角色是授予人工特定許可的任何角色。為您和您的團隊成員 AWS 提供對專案的管理員存取權。身為專案擁有者，您可以新增和移除團隊成員。如需詳細資訊，請參閱[邀請團隊成員在 AWS 設定中協作](#)。您不會建立根使用者。您的 AWS 建置器 ID 擁有您的專案帳戶，而不是根使用者電子郵件地址，這不會在您啟用進階功能時變更。您可以視需要建立 IAM 角色和 IAM 使用者，但只能用於程式設計存取，不能用於主控台存取。

每個專案都有受管安全實作，讓您輕鬆自信地建置。根據預設，專案中的任何應用程式或程式碼都可以存取 AWS 相同專案中的所有資源。您不需要執行額外的存取組態。

AWS 除非您針對特定資源開啟跨專案存取，否則不同專案中的資源無法彼此存取。例如，您可以在一個專案中建立 Lambda 函數，然後使用不同專案中的 API 叫用它。這描述為跨帳戶整合。如需詳細資訊，請參閱[跨帳戶 Lambda 整合](#)。只要這兩個專案都由相同的管理帳戶擁有，就會支援此功能。

根據預設，您的專案不會提供任何資源的外部存取權。您必須設定 AWS 資源以允許公開存取。您可以執行下列動作：

- 建立公有 S3 儲存貯體以託管簡單的靜態網站或檔案。如需詳細資訊，請參閱[Amazon S3 入門](#)。
- 建立 API Gateway API 做為應用程式的前門。如需詳細資訊，請參閱[建置 HTTP API](#)。
- 使用公有 IP 地址建立 EC2 執行個體，以允許執行個體與網際網路之間的通訊。如需詳細資訊，請參閱[啟動您的第一個 EC2 執行個體](#)。
- 建立 CloudFront 分佈，將靜態和動態 Web 內容交付給您的使用者，例如 .html、.css、.js 和映像檔案。如需詳細資訊，請參閱[CloudFront 入門](#)。
- 建立 Lambda 函數 URL，為 Lambda 函數提供簡單、直接可公開存取的 HTTP 端點。請確定您的 Lambda 函數具有正確的許可。如需詳細資訊，請參閱[建立函數 URL](#)，以及[Lambda 函數 URLs 的安全和驗證模型](#)。
- 使用這些機制或其他 AWS 機制的組合。

此外，當您啟用進階功能時，您可以存取更多機制，以提供資源的外部存取權。

管理您的 AWS 帳戶

您可以 AWS 帳戶 根據您正在使用的 類型來管理 AWS 。下表顯示在何處尋找每個管理任務的文件。

任務	註冊 AWS (新)	註冊 AWS (進階)
註冊	註冊 AWS (新)	註冊 AWS (進階)
建立 帳戶	在 AWS 設定中建立專案	註冊 AWS (進階)
關閉 帳戶	在 AWS 設定中關閉專案	關閉 AWS 帳戶
更新您的密碼	在 AWS 設定中更新您的密碼	更新根使用者密碼
註冊 MFA 裝置	在 AWS 設定中管理多重重要素驗證 (MFA)	步驟 3 : (建議) 設定 AWS MCP 伺服器
變更您的電子郵件	在 AWS 設定中變更您的電子郵件地址	更新根使用者電子郵件地址
變更您的名稱	在 AWS 設定中管理您的姓名或暱稱	更新 AWS 帳戶 名稱
更新聯絡資訊	在 AWS 設定中編輯您的聯絡資訊	更新 的主要聯絡人 AWS 帳戶
更新替代聯絡人	不適用	更新 的替代聯絡人 AWS 帳戶
管理帳單	在 AWS 設定中管理您的付款方式	更新 的帳單 AWS 帳戶
管理稅務資訊	在 AWS 設定中管理稅務註冊	管理您的付款
啟用或停用 AWS 區域	不適用。您無法修改 AWS 區域。	AWS 區域 在您的帳戶中啟用或停用

任務	註冊 AWS (新)	註冊 AWS (進階)
檢視帳戶識別符	不適用	檢視 AWS 帳戶 識別符
建立帳戶別名	不適用	建立 AWS 帳戶 別名
升級您的帳戶	在 AWS 設定中升級您的帳戶	免費方案
建立支出限制	在 AWS 設定中建立支出限制	不適用
更新支出限制	在 AWS 設定中更新支出限制	不適用
移除支出限制	在 AWS 設定中移除支出限制	不適用
邀請團隊成員	邀請團隊成員在 AWS 設定中協作	IAM 身分
在專案之間切換	在專案之間切換	多工作階段支援
連接 AI 編碼工具	連接 AI 編碼工具	不適用
刪除所有工作階段	刪除 AWS 設定中的所有工作階段	不適用
選擇退出 AI 資料使用	在 AWS 設定中選擇不使用您的內容以改善服務	AI 服務選擇退出政策
請求您的資料	請求您的 AWS 建置器 ID 資料	請求您的資料
刪除您的 AWS 設定檔	在 AWS 設定中關閉您的帳戶	關閉 AWS 帳戶

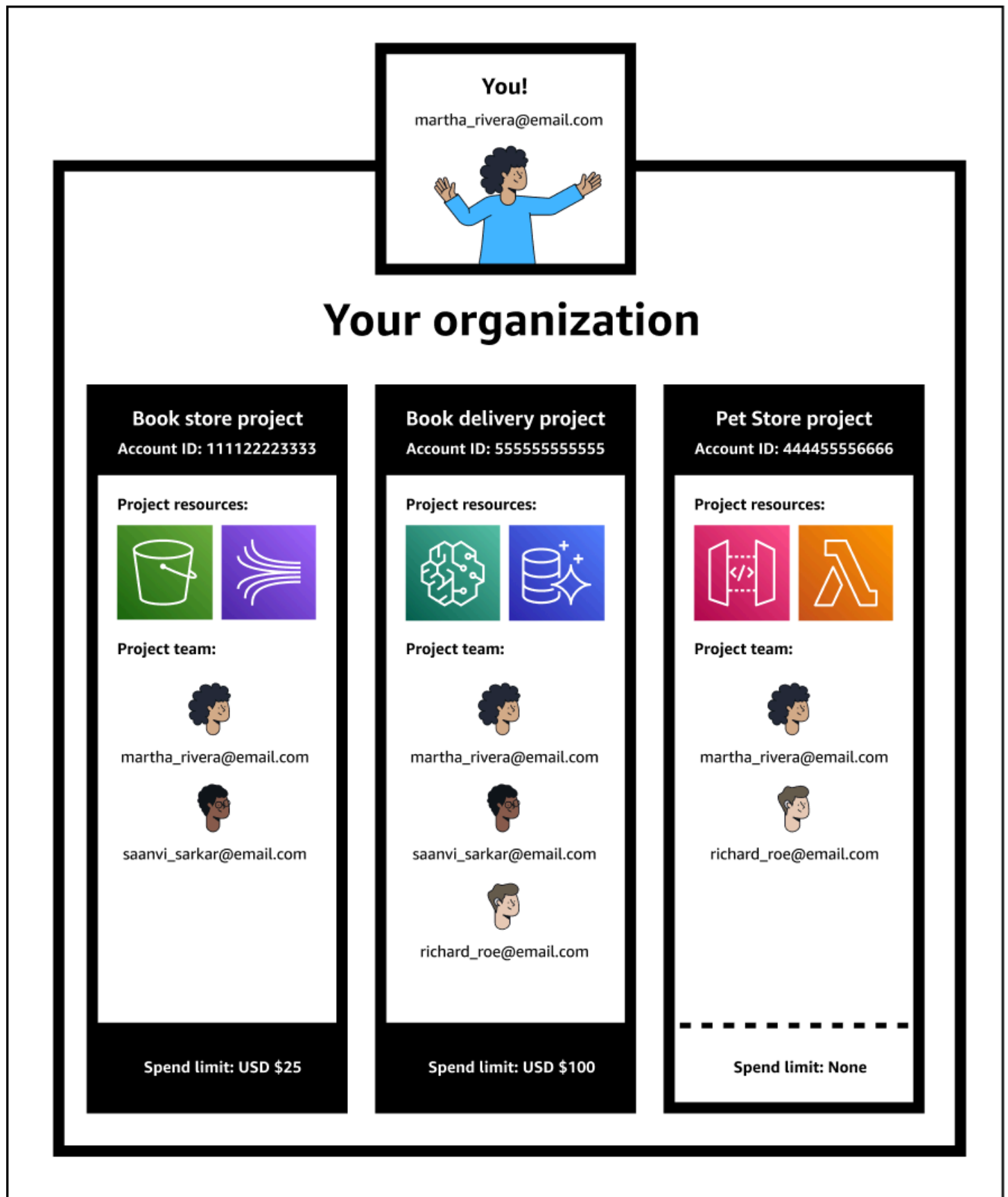
任務	註冊 AWS（新）	註冊 AWS（進階）
管理印度的帳戶	在 AWS 設定中管理印度的帳戶	管理印度的帳戶
建立管理員使用者	不適用	註冊 AWS（進階）
規劃您的帳戶控管結構	不適用	規劃您的 AWS 帳戶控管結構

註冊 AWS（新）

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

當您使用註冊 AWS（新）時，您可以建立預先設定 AWS 的環境，讓您使用如 Google 或 GitHub 等您已擁有的登入來存取 AWS 資源。您的資源會組織在專案中。專案包含 AWS 帳戶和設定，可與其他協作者共用。如果您使用付費計劃，您的專案也可以有一組每月稅前成本，稱為支出限制。您擁有的所有專案都組成您的組織。您可以在 AWS 設定中管理組織、存取專案，以及新增團隊成員。



當您註冊 AWS 使用註冊 for AWS（新）時，AWS 也會建立 AWS 建構家 ID 帳戶，這是代表您做為個人的個人設定檔。AWS 建構家 ID 每個電子郵件地址只能有一個。如果您已建立，AWS 建構家 ID 但尚未建立 AWS 帳戶，則可能已經為您進行一些設定，之後您必須修改這些設定。

如需註冊 AWS（新）的詳細資訊，請參閱下列文件：

- [比較註冊選項](#)
- [支援 AWS 服務 註冊 AWS（新）](#)

使用註冊 for AWS（新）進行註冊

當您註冊時 AWS，我們可能會請求付款資訊。我們的驗證程序會保留 1 USD（或同等金額）3-5 天，以驗證您的帳戶並防止詐騙。在升級至付費計劃之前，您不會產生費用。您可以隨時透過 AWS 設定來管理您的付款方式或關閉帳戶。此外，當您註冊時 AWS，您可能不符合免費方案的資格。在這種情況下，您將需要提供付款資訊，並將您列入付費計劃。當您在付費計劃中時，您可以設定支出限制，以在可預測且受控制的預算內操作。

註冊 for AWS (new) 支援為您的帳戶使用 Google、GitHub、Apple 或 Amazon。如果您已在瀏覽器中登入 Google 帳戶，註冊時將會使用該帳戶 AWS。

AWS 使用註冊 AWS（新）註冊

1. 開啟[註冊頁面 AWS](#)。
2. 輸入您的電子郵件或選擇登入，例如 Google、Apple、GitHub 或 Amazon。
3. 如果您使用已擁有的登入，系統會將您導向至供應商的登入。登入後，系統會將您重新導向至 AWS 註冊。
4. 輸入您的名稱，然後選擇繼續。

當您授予團隊成員存取專案的權限時，就會與團隊成員共用此名稱。

5. 輸入驗證碼，驗證與您的登入相關聯的電子郵件。驗證您的電子郵件後，請選擇繼續。

當您提供團隊成員存取專案的權限時，此電子郵件會與團隊成員共用。

6. 輸入您帳戶的高強度密碼，然後選擇繼續。

AWS 需要您的密碼符合下列條件：

- 它必須至少有 8 個字元，最多 128 個字元。
- 它至少混用 3 種下列類型字元：大寫、小寫、數字和 ! @ # \$ % ^ & * () < > [] { } | _ + = 符號。

- 它不能與 AWS 帳戶 您的姓名或電子郵件地址相同。
7. 輸入您的聯絡詳細資訊，然後選擇繼續。
 8. AWS 會將您的第一個專案佈建在 AWS 區域 具有新名稱的三個 之一中。如需詳細資訊，請參閱[AWS 區域 您的專案](#)。您可以隨時變更名稱。

您現在可以存取 AWS 管理主控台。若要存取 AWS 設定，請從 選擇管理專案 AWS 管理主控台。在 AWS 設定中，您可以邀請團隊成員、建立新專案，以及修改您的帳單和其他設定。

後續步驟

註冊後 AWS，您可以連接 AI 編碼工具、新增團隊成員進行協作，而且如果您有付費計劃，請建立支出限制。

- [連接 AI 編碼工具](#)
- [邀請團隊成員在 AWS 設定中協作](#)
- [在 AWS 設定中建立支出限制](#)

使用 AWS 設定

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

[AWS 設定](#)是您管理和存取專案的位置。當您使用註冊 AWS（新）註冊時，即可使用 AWS 設定。您可以使用 AWS 設定來執行下列動作：

- 建立和存取您擁有的專案。如需詳細資訊，請參閱[在 AWS 設定中建立專案](#)。
- 存取已與您共用的專案。
- 邀請團隊成員協作您的專案。如需詳細資訊，請參閱[邀請團隊成員在 AWS 設定中協作](#)。
- 在專案之間切換。如需詳細資訊，請參閱[在專案之間切換](#)。
- 管理您的付款方式。如需詳細資訊，請參閱[在 AWS 設定中管理您的付款方式](#)。
- 從免費方案升級至付費計劃。如需詳細資訊，請參閱[在 AWS 設定中升級您的帳戶](#)。
- 管理專案的支出限制。如需詳細資訊，請參閱[在 AWS 設定中建立支出限制](#)。

- 檢視您的帳單資訊。如需詳細資訊，請參閱[在 AWS 設定中檢視您的帳單資訊](#)。
- 管理您的設定檔資訊。如需詳細資訊，請參閱[在 AWS 設定中管理您的姓名或暱稱](#)、[在 AWS 設定中變更您的電子郵件地址](#)及[在 AWS 設定中編輯您的聯絡資訊](#)。
- 管理您的安全設定和登入偏好設定。如需詳細資訊，請參閱[在 AWS 設定中更新您的密碼](#)及[在 AWS 設定中管理多重要素驗證 \(MFA\)](#)。

當您管理設定檔資訊或安全性設定時，系統會將您重新導向至 AWS 建構家 ID 中樞。您的 AWS 建構家 ID 會在您使用註冊 AWS（新）時建立。如需詳細資訊，請參閱[什麼是 AWS 建構家 ID？](#)。

連接 AI 編碼工具

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以為 AI 編碼工具提供對專案的存取權，並安裝 Agent Toolkit，該工具組封裝了 AWS MCP 伺服器組態和一組精選的代理程式技能。這可讓您的 AI 編碼工具代表您建立和管理 AWS 資源。

將編碼工具連線至專案的考量事項

- 您可以將 AI 編碼工具連接到您擁有的專案或已與您共用的專案。
- 當 AI 編碼工具或本機代理程式建立 AWS 資源時，您仍需對其負責。這包括[共同責任模型](#)所定義之資源的適當安全性，以及這些資源可能產生的任何費用，無論這些費用是否計入免費計劃或付費計劃。
- 您對 AI 編碼工具在專案中代表您採取的任何動作負責。
- 若要檢視代理程式建立的資源，請前往該服務的服務主控台。
- 您產生的登入資料可供 AWS CLI、AWS Tools for PowerShell 和 AWS SDKs 使用。可能不支援外部工具。對您資源的存取有效期為 12 小時。使用下列命令來續約您的登入資料：

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

將 *profile-name* 取代為您在初始設定期間選擇的設定檔名稱。命令會自動開啟您的預設瀏覽器。您需要選擇專案名稱才能完成登入程序。AWS 可以續約您的登入資料 90 天。90 天後，您將需要再次在瀏覽器視窗中授予存取權。

將您的 AI 編碼工具連接至您的專案

每個專案都有自己的一組登入資料，AI 編碼工具可用來代表您建立和管理 AWS 資源。

AWS 管理主控台

使用 AWS 主控台將您的 AI 編碼工具連接到您的專案

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇您要存取的專案。
3. 在右上角的導覽列中，選擇建立和管理雲端基礎設施。
4. 選擇搭配 AI 編碼工具使用您的 AWS 登入資料。
5. 選擇複製代理程式提示，然後在編碼代理程式中輸入它。

這會建立提示，與您的 AI 編碼代理器共用轉向檔案。轉向檔案會從 存取指令碼 AWS ，以設定專案登入資料與 AI 編碼代理程式之間的連線。

您將輸入專案的設定檔名稱。此設定檔名稱是 AI 編碼工具存取 資源的方式。

Use your terminal

執行下列命令來下載並遵循設定指示：

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

當您使用我們的新 AWS 體驗時，您的代理程式會安裝 AWS MCP 伺服器，而且您可以存取可與專案搭配使用的代理程式技能。您也會收到規則檔案，其中包含針對此體驗調整的指引。規則檔案也可讓您定義您希望客服人員提供的協助層級。以下是支援的說明層級：

- 低：在您建置時，技能只會標記安全風險。它不會為您的架構建議任何改進或替代方案。
- 中：在您建置時，如果技能偵測到潛在問題，可能會詢問一些釐清性問題。它不會為您的架構建議任何改進或替代方案。
- 高：在您建置時，技能將提供高層級的支援。它會為您的架構建議改進或替代方案。

使用多個專案

每個專案都有自己的一組登入資料，AI 編碼工具可用來代表您建立和管理 AWS 資源。您可以使用設定檔來存取每個專案。設定檔是由 維護的組態設定和登入資料檔案 AWS CLI，您會為每個設定檔提供唯一的名稱。

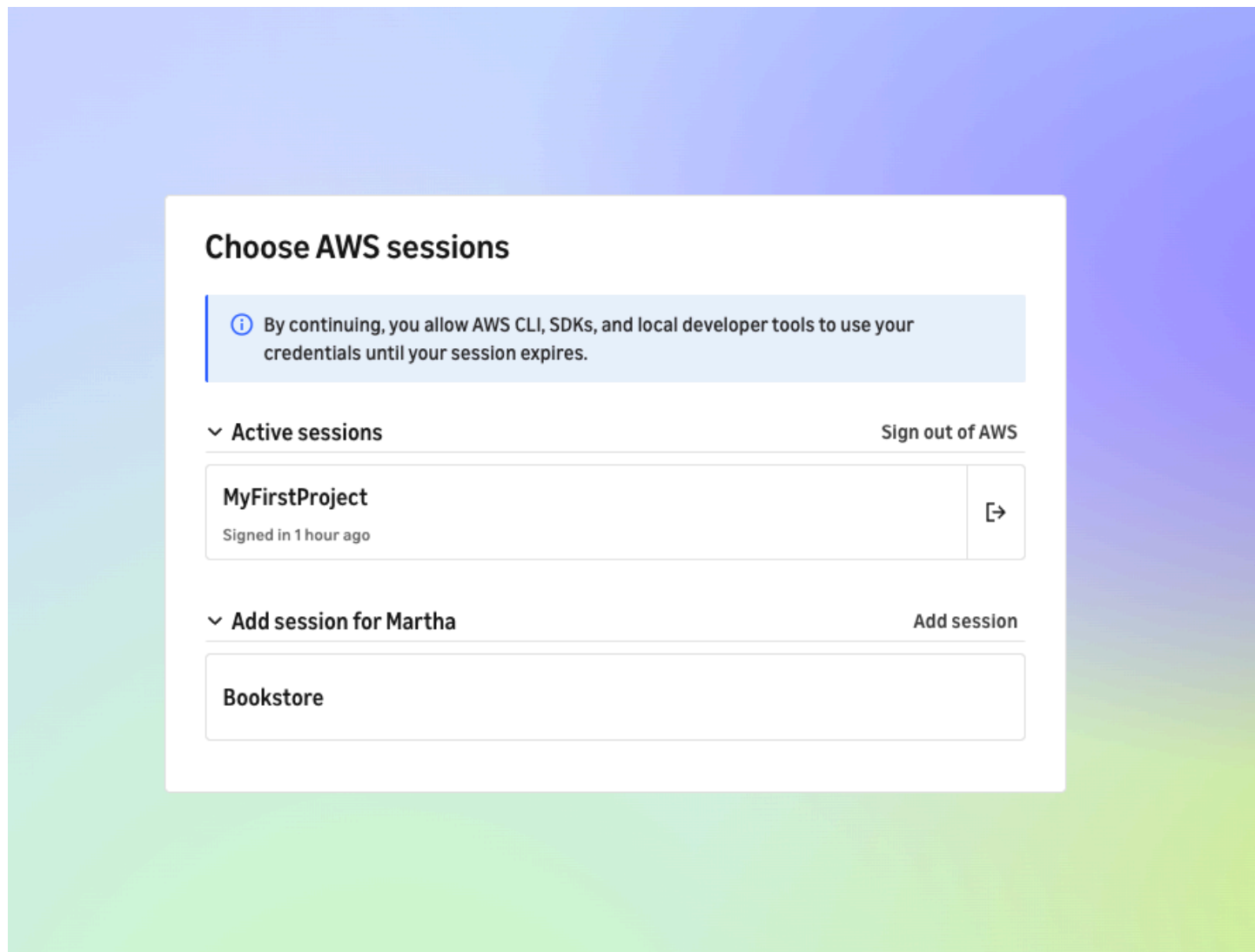
例如，如果您的第一個專案是 `MyFirstProject`並在設定`MyFirstProjectProfile`期間選擇設定檔名稱，您可以使用 AWS CLI 下列命令登入 來存取該專案：

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

如果您建立另一個名為 `Bookstore` 的專案，您可以使用設定指令碼並建立設定檔 來存取它`BookstoreProfile`。然後，您可以使用 AWS CLI 下列命令登入：

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

不過，當您執行其中一個命令時，您需要在選擇工作階段頁面上為 AWS 登入資料選擇 AWS 工作階段。



此頁面顯示您可以新增的作用中工作階段和工作階段。工作階段會以您的 AWS 登入資料代表經過驗證的狀態，並提供 AI 編碼代理程式用來建立和管理資源的相同登入資料。

在此範例中，您已登入 MyFirstProject，且尚未登入 Bookstore。在選擇 AWS 工作階段頁面上，您可以執行下列動作：

- 若要繼續 AWS 將用於 MyFirstProject，請選擇 MyFirstProject。
- 若要存取 Bookstore，請選擇 Bookstore。
- 若要移除任何目前的工作階段，請選擇結束圖示。
- 若要 AWS 帳戶使用 IAM 使用者存取，例如您使用建立的帳戶[註冊 AWS（進階）](#)，請選擇新增工作階段。

您選擇的登入資料將與 AI 編碼代理程式用來建立和管理資源的登入資料相同。例如，您可以使用 AWS CLI 下列命令登入：

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

如果您接著選擇 Bookstore 工作階段，您的 AI 編碼工具將在 Bookstore 專案中建立 AWS 資源。

一律選擇與您的設定檔相關聯專案相符的工作階段。

AWS 專案擁有者的 動作

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

當您擁有專案時，您可以對專案進行管理控制。這包括您可以在 [使用 AWS 設定](#) 中完成的任務。您也可以執行僅限根的動作。您的團隊成員無法完成這些動作。

您可以執行的目前僅限根動作如下：

- 編輯或刪除拒絕所有委託人的 S3 儲存貯體政策。您可以執行此操作，以使用設定錯誤的儲存貯體政策來解鎖 S3 儲存貯體。
- 編輯或刪除拒絕所有委託人的 SQS 資源型政策。您可以執行此操作，以使用設定錯誤的資源型政策來解鎖 SQS 佇列。

執行僅限根的動作

1. 登入您的專案，並在 <https://console.aws.amazon.com/iam/> 開啟 IAM 主控台。
2. 在主控台的導覽窗格中，選擇根存取權管理。
3. 針對權限動作，選擇您要在成員帳戶中採取的特權動作。
 - 選取刪除 Amazon S3 儲存貯體政策，以移除設定錯誤的儲存貯體政策，此政策拒絕所有主體存取 Amazon S3 儲存貯體。
 - a. 輸入 S3 URI，或選擇瀏覽 S3，從專案中的儲存貯體中選取名稱。
 - b. 選擇刪除儲存貯體政策。

- c. 刪除設定錯誤的政策後，使用 Amazon S3 主控台來更正儲存貯體政策。如需詳細資訊，請參閱 Amazon S3 User Guide 中的 [Adding a bucket policy by using the Amazon S3 console](#)。
- 選取刪除 Amazon SQS 政策以刪除資源型政策，拒絕所有主體存取 Amazon SQS 佇列。
 - a. 在 SQS 佇列名稱中輸入佇列名稱。
 - b. 選擇刪除 SQS 政策。
 - c. 刪除設定錯誤的政策後，使用 Amazon SQS 主控台來更正佇列政策。如需詳細資訊，請參閱《Amazon SQS 開發人員指南》中的 [在 Amazon SQS 中設定存取政策](#)。

在 AWS 設定中更新您的密碼

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以在 AWS 設定中更新密碼。

在 AWS 設定中更新您的密碼

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理安全性和登入。

系統會將您重新導向至 AWS 您的建置器 ID 設定檔。

3. 針對授權，選擇更新密碼。
4. 針對 Current password (目前的密碼)，請輸入目前的密碼。
5. 針對新密碼，輸入新密碼。

AWS 需要您的密碼符合下列條件：

- 它必須至少有 8 個字元，最多 128 個字元。
 - 它至少混用 3 種下列類型字元：大寫、小寫、數字和 ! @ # \$ % ^ & * () < > [] { } | _ + = 符號。
6. 針對確認新密碼，輸入您的新密碼。
 7. 選擇更新。

在 AWS 設定中管理多重要素驗證 (MFA)

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

多重要素驗證 (MFA) 是一種簡單且有效的機制，可增強您的安全性。第一個因素：您的密碼，是您記住的秘密，也稱為知識因素。其他因素可以是擁有因素 (您擁有的事物，例如安全金鑰) 或繼承因素 (您自身的事物，例如生物特徵掃描)。我們強烈建議您設定 MFA 為您的帳戶新增額外的圖層。

您可以註冊內建驗證器，也可以註冊您保存在實體安全位置的安全金鑰。如果您無法使用內建驗證器，則可以使用已註冊的安全金鑰。對於驗證器應用程式，您也可以在這些應用程式中啟用雲端備份或同步功能。如果您遺失或損壞 MFA 裝置，這可協助您避免失去對設定檔的存取權。

重點

當您註冊和管理 MFA 裝置時，請記住下列重點：

- 我們建議您註冊多個 MFA 裝置。如果您無法存取所有已註冊的 MFA 裝置，您將無法復原您的帳戶。
- 我們建議您定期檢閱已註冊的 MFA 裝置，以確保它們是最新且正常運作的。此外，您應該將這些裝置存放在不使用時實際安全的位置。
- 如果您使用繼續 Google 建立帳戶，您可以透過 Google 帳戶啟用多重驗證。如需詳細資訊，請參閱[開啟2-Step驗證](#)。
- 如果您使用 Continue with Apple 建立帳戶，您的 Apple 帳戶中可能已啟用多重驗證。如果沒有，如需如何啟用的詳細資訊，請參閱[Apple 帳戶的雙重驗證](#)。
- 如果您使用繼續 GitHub 建立帳戶，您可以透過 GitHub 帳戶啟用多重驗證。如需詳細資訊，請參閱[設定 \(GitHub\) 雙重驗證](#)。
- 如果您使用 Continue with Amazon 建立帳戶，您可以透過 Amazon 帳戶啟用多重驗證。如需詳細資訊，請參閱[什麼是兩步驟驗證？](#)。

新 AWS 體驗可用的 MFA 類型

我們的新 AWS 體驗支援下列多重要素驗證 (MFA) 裝置類型。

FIDO2 驗證器

[FIDO2](#) 是包含 CTAP2 和 [WebAuthn](#) 的標準，以公有金鑰密碼編譯為基礎。FIDO 登入資料具有網路釣魚防護，因為它們對建立登入資料的網站是唯一的 AWS。

AWS 支援 FIDO 驗證器的兩種最常見形式因素：內建驗證器和安全金鑰。如需 FIDO 驗證器最常見類型的詳細資訊，請參閱下文。

內建驗證器

有些裝置具有內建驗證器，例如 MacBook 上的 TouchID 或 Windows Hello 相容相機。如果您的裝置與 FIDO 通訊協定相容，包括 WebAuthn，您可以使用指紋或臉部作為第二個因素。如需詳細資訊，請參閱 [FIDO 身分驗證](#)。

安全金鑰

您可以購買與 FIDO2-compatible 外部 USB、BLE 或 NFC 連接的安全金鑰。系統提示您輸入 MFA 裝置時，請輕觸金鑰的感應器。YubiKey 或 Feitian 會建立相容的裝置。如需所有相容安全金鑰的清單，請參閱 [FIDO 認證產品](#)。

密碼管理器、通行金鑰提供者和其他 FIDO 驗證器

多個第三方供應商支援行動應用程式中的 FIDO 身分驗證，作為密碼管理員、具有 FIDO 模式的智慧卡和其他形式因素的功能。這些與 FIDO 相容的裝置可與 IAM Identity Center 搭配使用，但我們建議您先自行測試 FIDO 驗證器，再為 MFA 啟用此選項。

Note

有些 FIDO 驗證器可以建立可探索的 FIDO 登入資料，稱為通行金鑰。通行金鑰可能繫結至建立通行金鑰的裝置，也可能可同步並備份至雲端。例如，您可以在支援的 Macbook 上使用 Apple Touch ID 註冊通行金鑰，然後在登入時依照螢幕上的提示，使用 Google Chrome 搭配 iCloud 中的通行金鑰，從 Windows 筆記型電腦登入網站。如需有關哪些裝置支援作業系統和瀏覽器之間的可同步通行金鑰和目前通行金鑰互通性的詳細資訊，請參閱 passkeys.dev 中的 [裝置支援](#)，這是 FIDO Alliance and World Wide Web Consortium (W3C) 維護的資源。

驗證器應用程式

驗證器應用程式是一次性密碼 (OTP) 型第三方身分驗證器。您可以使用安裝在行動裝置或平板電腦上的驗證器應用程式，做為授權的 MFA 裝置。第三方驗證器應用程式必須符合 RFC 6238，這是標準型的一次性密碼 (TOTP) 演算法，能夠產生六位數驗證碼。

當提示輸入 MFA 時，您必須在顯示的輸入方塊中輸入來自驗證器應用程式的有效代碼。每個指派給使用者的 MFA 裝置都必須是唯一的。您可以為任何指定的使用者註冊兩個驗證器應用程式。

您可以從下列知名的第三方驗證器應用程式進行選擇。不過，任何符合 TOTP 的應用程式都適用於 AWS Builder ID MFA。

作業系統	已測試的驗證器應用程式
Android	1Password 、 Authy 、 Duo Mobile 、 Microsoft Authenticator 、 Google Authenticator
iOS	1Password 、 Authy 、 Duo Mobile 、 Microsoft Authenticator 、 Google Authenticator

註冊您的 MFA 裝置

Note

註冊 MFA、登出，然後在同一個裝置上登入後，可能不會提示您在信任的裝置上輸入 MFA。

使用驗證器應用程式註冊您的 MFA 裝置

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理安全性和登入。

系統會將您重新導向至 AWS 您的建置器 ID 設定檔。

3. 在安全頁面上，選擇註冊裝置。
4. 在註冊 MFA 裝置頁面上，選擇驗證器應用程式。
5. AWS Builder ID 會操作並顯示組態資訊，包括 QR 程式碼圖形。圖形是「秘密組態金鑰」的表示，可在不支援 QR 代碼的驗證器應用程式中手動輸入。
6. 開啟您的驗證器應用程式。如需應用程式清單，請參閱 [驗證器應用程式](#)。

如果驗證器應用程式支援多個 MFA 裝置或帳戶，請選擇建立新 MFA 裝置或帳戶的選項。

7. 判斷 MFA 應用程式是否支援 QR 代碼，然後在設定您的驗證器應用程式頁面上執行下列其中一項操作：

1. 選擇顯示 QR 碼，然後使用應用程式掃描 QR 碼。例如，您可以選擇攝影機圖示或選擇類似於掃描碼的選項。然後使用裝置的相機掃描程式碼。
2. 選擇顯示私密金鑰，然後在 MFA 應用程式中輸入該私密金鑰。

完成後，您的驗證器應用程式將產生並顯示一次性密碼。

8. 在驗證器程式碼方塊中，輸入目前出現在驗證器應用程式中的一次性密碼。選擇 Assign MFA (指派 MFA)。

Important

產生代碼之後立即提交您的請求。如果您產生程式碼，然後等待太久才提交請求，則 MFA 裝置已成功與您的 AWS 建置器 ID 建立關聯，但 MFA 裝置不同步。會發生這種情況是因為定時式的一次性密碼 (TOTP) 在過了一小段時間後就會過期。這種情況下，您可以重新同步裝置。如需詳細資訊，請參閱#####。

9. 若要在 AWS 建置器 ID 中為裝置提供易記的名稱，請選擇重新命名。此名稱可協助您區分此裝置與您註冊的其他人。

MFA 裝置現在可以與 AWS 設定、專案和 AWS 建置器 ID 搭配使用。

將安全金鑰註冊為您的 MFA 裝置

使用安全金鑰註冊您的 MFA 裝置

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理安全性和登入。

系統會將您重新導向至 AWS 您的建置器 ID 設定檔。

3. 在安全頁面上，選擇註冊裝置。
4. 在註冊 MFA 裝置頁面上，選擇安全金鑰。
5. 確保您的安全金鑰已啟用。如果您使用單獨的實體安全金鑰，請將其連接到您的電腦。
6. 遵循畫面上的指示。您的體驗會根據您的作業系統和瀏覽器而有所不同。
7. 若要在 AWS 建置器 ID 中為裝置提供易記的名稱，請選擇重新命名。此名稱可協助您區分此裝置與您註冊的其他人。

MFA 裝置現在可以與 AWS 設定、專案和 AWS 建置器 ID 搭配使用。

重新命名 MFA 裝置

重新命名 MFA 裝置

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理安全性和登入。

系統會將您重新導向至 AWS 您的建置器 ID 設定檔。

3. 選擇 Security (安全性)。當您抵達頁面時，您會看到重新命名呈現灰色。
4. 選取您要變更的 MFA 裝置。這可讓您選擇重新命名。然後會出現對話方塊。
5. 在開啟的提示中，在 MFA 裝置名稱中輸入新名稱，然後選擇重新命名。重新命名的裝置會顯示在多重要素驗證 (MFA) 裝置下。

刪除您的 MFA 裝置

我們建議您保留兩個或多個作用中的 MFA 裝置。若要停用多重要素驗證，請從設定檔中移除所有已註冊的 MFA 裝置。

刪除 MFA 裝置

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理安全性和登入。

系統會將您重新導向至 AWS 您的建置器 ID 設定檔。

3. 在安全性頁面上，選取要變更的 MFA 裝置，然後選擇刪除。
4. 在刪除 MFA 裝置中？ 模態，請依照指示刪除您的裝置。
5. 選擇 刪除。

刪除的裝置不會再出現在多重要素驗證 (MFA) 裝置下。

刪除 AWS 設定中的所有工作階段

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以在 AWS 設定中刪除跨裝置的所有工作階段。如果您有無法辨識的裝置，請變更您的密碼並刪除所有工作階段。

刪除所有工作階段

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理安全性和登入。

系統會將您重新導向至 AWS 您的建置器 ID 設定檔。

3. 針對已登入的裝置，選擇刪除所有工作階段。
4. 確認您的選擇，然後選擇刪除所有工作階段。

您將登出 AWS 設定。

在 AWS 設定中管理您的姓名或暱稱

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以隨時變更名稱。所有團隊成員都可以查看您的名稱，如果您已升級至付費計劃，這是顯示在帳單資訊上的名稱。如果您在 AWS 印度註冊，您的名稱必須與計劃用於客戶驗證的文件上顯示的名稱完全相符。

當您變更名稱時，您可以在 AWS Builder ID 中變更名稱。這將影響您在 AWS 設定、AWS 建置器 ID 以及您透過 AWS 建置器 ID 直接存取的任何 AWS 資源中的名稱。

您的名稱是您在與他人互動時在工具和服務中被提及的方式。您的暱稱指出您希望如何被 AWS、朋友和與您緊密合作的其他人知道。

變更您的名稱或暱稱

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理設定檔。
3. 針對設定檔資訊，選擇管理設定檔。

系統會將您重新導向至 AWS 您的建置器 ID 設定檔。

4. 如需設定檔資訊，請選擇編輯。
5. （選用）針對名稱，輸入新名稱。
6. （選用）對於暱稱，輸入新的暱稱。
7. 選擇儲存變更。

在 AWS 設定中變更您的電子郵件地址

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以在 AWS 設定中變更您的電子郵件。當您變更電子郵件時，您先前的電子郵件將與您的 AWS 設定檔和 AWS 建置器 ID 分開。您將無法使用該電子郵件存取 AWS 設定中的任何專案，但您可以使用該電子郵件 AWS 再次註冊。

當您允許團隊成員存取您的專案時，會與團隊成員共用您的電子郵件地址。

變更您的電子郵件

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理設定檔。
3. 針對設定檔資訊，選擇管理設定檔。

系統會將您重新導向至 AWS 您的建置器 ID 設定檔。

4. 如需聯絡資訊，請選擇編輯。
5. 對於電子郵件地址，輸入新的電子郵件地址，然後選擇驗證電子郵件。我們會傳送新電子郵件地址的驗證碼給您。您會在驗證電子郵件快顯方塊中輸入。
6. 針對驗證碼，輸入我們傳送至您新電子郵件的驗證碼。

7. 選擇 Verify (驗證)。

在 AWS 設定中編輯您的聯絡資訊

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以編輯與 AWS 設定相關聯的電話號碼或地址。當您修改這些值時，可能會影響稅務義務。

若要編輯您的聯絡資訊

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理設定檔。
3. 如需聯絡資訊，請選擇編輯。
4. 輸入新的聯絡資訊。
5. 選擇儲存。

在 AWS 設定中選擇不使用您的內容以改善服務

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

AWS AI 服務可能會使用和存放客戶內容以改善服務，例如修正操作問題、評估服務效能、偵錯或模型訓練。為此，我們可能會將這類內容存放在 AWS 區域 您使用 服務的 AWS 區域 外部。您可以透過 AWS 設定選擇不使用您的內容來改善服務。選擇退出的影響是將 AI 服務選擇退出政策 AWS 連接到您的 AWS 組織。如需選擇退出政策的詳細資訊，請參閱 [AI 服務選擇退出政策](#) 文件。

選擇不接收所有 服務，將針對 AI 服務選擇不接收政策支援的目前和未來支援的 AI 服務，使用您的內容來選擇不接收所有專案。

選擇退出 Amazon Monitron 需要其他步驟。如需詳細資訊，請參閱 [AWS 服務條款](#)。只有專案擁有者可以選擇退出 AWS AI 服務的資料使用。

選擇不讓 AWS AI 服務使用資料

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇專案。
3. 針對概觀，選擇動作，然後選擇不讓 AWS AI 服務使用資料。
4. 確認您的選擇，然後選擇選擇退出。

請求您的 AWS 建置器 ID 資料

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以請求和檢視與 AWS Builder ID 相關的個人資訊，以及您使用 AWS Builder ID 存取 AWS 的應用程式和服務。我們將在 30 天內處理您的請求，並在您的資料準備就緒時通知您。當資料請求處於待定狀態時，您無法關閉 AWS 設定檔。您仍然可以關閉擁有所有專案的專案或組織。

如需行使資料主體權利的詳細資訊，包括與其他 AWS 網站、應用程式、產品、服務、事件和體驗相關的個人資訊，請參閱 [AWS 隱私權](#)。

請求您的資料

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理設定檔。
3. 選擇管理設定檔。

系統會將您重新導向至 AWS 您的建置器 ID 設定檔。

4. 選擇隱私權和資料。
5. 選擇 以請求您的建置器 ID 資料或 AWS 您的資料。

綠色確認訊息會出現在我們收到您的請求的頁面頂端，並在 30 天內完成。

6. 當您收到我們已處理請求的電子郵件時，請導覽回 AWS 建置器 ID 設定檔的隱私權與資料頁面。選擇使用您的資料下載 ZIP 封存的新可用按鈕。

當資料請求處於待定狀態時，您將無法刪除 AWS 您的建置器 ID。

在 AWS 設定中建立專案

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

專案包含您建立 AWS 資源 AWS 帳戶 的單一。專案也包含與其他協作者共用的設定。您建立 AWS 的資源應代表應用程式或一組相關的使用案例。一個專案可以跨越應用程式的開發和生產環境。例如，您可以建立名為書店的專案，該專案保留書店應用程式的資源，包括資料庫、運算資源和儲存。

您可以與其他團隊成員共用此專案，他們可以為書店應用程式建置和管理資源。

根據帳戶中的資源，每個專案都有自己的成本控制。如果您使用的是付費計劃，您可以在 AWS 設定中為每個專案設定支出限制。如需詳細資訊，請參閱[在 AWS 設定中建立支出限制](#)。身為專案擁有者，您必須負責每月發票的使用費和經常性費用。

建立專案的考量事項

- 您可以存取不是以團隊成員身分擁有的專案。
- 每個專案名稱對於您的專案必須是唯一的。其他團隊成員擁有的專案可以具有相同的名稱。
- 專案名稱可包含下列有效字元：a-z、A-Z、0-9 和句點 (.)。
- 當您建立專案時，會根據您聯絡地址中的國家/地區，將專案 AWS 指派給美國東部（俄亥俄）(us-east-2)、歐洲（斯德哥爾摩）(eu-north-1) 或亞太區域（雪梨）(ap-southeast-2)。您建立的任何區域資源都會託管在該區域。如需詳細資訊，請參閱[AWS 區域 您的專案](#)。

建立專案

建立專案

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇專案。
3. 選擇建立專案。
4. 在專案名稱中，輸入專案的描述性名稱。

當您邀請團隊成員協作時，會與團隊成員共用此名稱。

5. 選擇建立。

建立專案需要幾秒鐘的時間。當您的專案可用時，您可以選擇專案並存取 AWS 管理主控台 以開始建置。

如果您已設定 AI 編碼工具以與您的 連接 AWS 帳戶，您可以提示它在新專案中建立資源。

使用 AI 編碼工具的範例提示來開始使用：

```
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.
```

AWS 區域 您的專案

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

當您建立專案時，會根據您聯絡地址中的國家/地區，將專案 AWS 指派給美國東部（俄亥俄）(us-east-2)、歐洲（斯德哥爾摩）(eu-north-1) 或亞太區域（雪梨）(ap-southeast-2)。您建立的任何區域資源都會託管在該區域。

以下是 AWS 區域 為您的帳戶選取的 的考量事項：

- 如果您在 AWS 設定中變更聯絡資訊，您選取的區域將不會變更。如果您需要存取特定區域，請使用註冊 AWS（進階）。您也可以為您的帳戶啟用進階功能，以選取不同的區域。
- AWS 可能會引進其他支援的區域，但這些區域僅適用於新的註冊。若要查看截至 2026 年 8 月 18 日的最新支援區域，請參閱下表。如果您已有專案，您可以在[AWS 設定](#)中找到您選取的區域。
- 全球服務可供您的專案使用。這些服務是透過單一區域存取，該區域可能與您的主要區域不同。如需詳細資訊，請參閱[AWS 故障隔離界限](#)。此外，某些服務可在特定區域中使用。在 AWS 管理主控台，您可以在特定區域中檢視這些服務，但當您導覽至不同的服務時，將返回所選區域。
- 如果您使用 Amazon Bedrock，則可以使用 API APIs 不會在所有預設為啟用 AWS 區域 的商用中建立資源。
- 如果您使用 CloudFront，則無法在所選區域之外建立資源的特定功能無法使用。這包括 AWS WAF 搭配 CloudFront 使用。

- 有些涉及 全域服務的 CloudTrail 事件會記錄在 全域服務運作的區域中。您可以存取這些事件。
- AWS WAF 和 Amazon CloudWatch Logs 在美國東部（維吉尼亞北部）(us-east-1) 提供。

您可以使用 AWS 設定，尋找您帳戶中所有專案的所選區域。在 中 AWS 管理主控台，大多數服務主控台託管在您所在的區域，包括 Bedrock 和 SageMaker。如果您從全球服務查看服務主控台，主控台會自動將所有 API 呼叫路由到全球服務的適當區域。

尋找 AWS 區域 為您的專案選取的

最佳實務是，建議您在建立任何 AWS 資源之前，一律確認專案 AWS 區域 的。

尋找 AWS 區域 為您的專案選取的

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇專案。
3. 在概觀區段中，選擇其他資訊。

在此檢視中，您也可以找到與專案相關聯的 AWS 帳戶 ID。

4. 對於 區域，您會看到 AWS 區域 您的專案已佈建在其中。

當您在任何專案中建立區域 AWS 資源時，這些資源的 Amazon Resource Name 會包含此項目 AWS 區域。

在美國東部（俄亥俄）佈建區域資源的國家/地區 (us-east-2)

國名	國家代碼
安地卡及巴布達	AG
阿根廷	AR
巴哈馬	BS
巴貝多	BB
貝里斯	BZ
玻利維亞	BO

國名	國家代碼
巴西	BR
加拿大	CA
智利	CL
哥倫比亞	CO
哥斯大黎加	CR
多米尼克	DM
多明尼加共和國	DO
厄瓜多	EC
薩爾瓦多	SV
格瑞那達	GD
瓜地馬拉	GT
蓋亞納	GY
海地	HT
宏都拉斯	HN
牙買加	JM
墨西哥	MX
尼加拉瓜	NI
巴拿馬	PA
巴拉圭	PY
秘魯	PE

國名	國家代碼
聖克里斯多福及尼維斯	KN
聖露西亞	LC
聖文森及格瑞那丁	VC
蘇利南	SR
千里達及托巴哥	TT
美國	美國
烏拉圭	UY
委內瑞拉	VE
安圭拉	AI
阿魯巴島	AW
百慕達	BM
Bonaire、Sint Eustatius 和 Saba	BQ
英屬維京群島	VG
開曼群島	KY
庫拉索	CW
福克蘭群島	FK
法屬圭亞那	GF
瓜地洛普	GP
馬丁尼克	MQ
蒙特色拉特島	MS

國名	國家代碼
波多黎各	PR
聖巴泰勒米島	BL
法屬聖馬丁	MF
聖皮埃赫及密克隆	PM
荷屬聖馬丁	SX
英屬土克斯及開科斯群島	TC
美屬維京群島	VI

在亞太區域（雪梨）佈建區域資源的國家/地區 (ap-southeast-2)

國名	國家代碼
阿富汗	AF
澳洲	AU
孟加拉	BD
不丹	BT
汶萊	BN
柬埔寨	KH
中國	CN
東帝汶 (Timor-Leste)	TL
斐濟	FJ
香港	HK

國名	國家代碼
印度	IN
印尼	ID
日本	JP
哈薩克	KZ
吉里巴斯	KI
吉爾吉斯	KG
寮國	LA
澳門	MO
馬來西亞	MY
馬爾地夫	MV
馬紹爾群島	MH
密克羅尼西亞	FM
蒙古	MN
緬甸	MM
諾魯	NR
尼泊爾	NP
紐西蘭	NZ
巴基斯坦	PK
帛琉	PW
巴布亞紐幾內亞	PG

國名	國家代碼
菲律賓	PH
薩摩亞	WS
新加坡	SG
索羅門群島	SB
南韓	KR
斯里蘭卡	LK
臺灣	TW
塔吉克	TJ
泰國	TH
東加	TO
土庫曼	TM
吐瓦魯	TV
烏茲別克	UZ
萬那杜	VU
越南	VN
美屬薩摩亞	AS
聖誕島	CX
可可斯群島	CC
庫克群島	CK
法屬玻里尼西亞	PF

國名	國家代碼
關島	GU
赫德島和麥克唐納群島	HM
新喀里多尼亞	NC
紐埃島	NU
諾福克島	NF
北馬里亞納群島	MP
皮特肯群島	PN
托克勞	TK
美國次要離島	UM
瓦利斯和富圖那	WF

在歐洲（斯德哥爾摩）佈建區域資源的國家/地區 (eu-north-1)

國名	國家代碼
阿爾巴尼亞	AL
阿爾及利亞	DZ
安道爾	AD
安哥拉	AO
亞美尼亞	AM
奧地利	AT
亞塞拜然	AZ

國名	國家代碼
巴林	BH
白俄羅斯	BY
比利時	BE
貝南	BJ
波士尼亞與赫塞哥維納	BA
波札那	BW
保加利亞	BG
布吉納法索	BF
蒲隆地	BI
維德角	CV
喀麥隆	CM
中非共和國	CF
查德	TD
葛摩	KM
剛果 (布拉柴維爾)	CG
剛果 (DRC)	CD
Côte d'Ivoire	CIS
克羅埃西亞	HR
賽普勒斯	CY
捷克	CZ

國名	國家代碼
丹麥	DK
吉布地	DJ
埃及	EG
赤道幾內亞	GQ
厄利垂亞	ER
愛沙尼亞	EE
史瓦帝尼	SZ
衣索比亞	ET
芬蘭	FI
法國	法國
加彭	GA
甘比亞	GM
喬治亞	GE
德國	DE
迦納	GH
希臘	GR
幾內亞	GN
幾內亞比索	GW
匈牙利	HU
冰島	IS

國名	國家代碼
伊拉克	IQ
愛爾蘭	IE
以色列	IL
義大利	IT
約旦	JO
肯亞	KE
科索沃	XK
科威特	KW
拉脫維亞	LV
黎巴嫩	LB
賴索托	LS
賴比瑞亞	LR
利比亞	LY
列支敦斯登	LI
立陶宛	LT
盧森堡	LU
馬達加斯加	MG
馬拉威	MW
馬利	機器學習 (ML)
馬爾他	MT

國名	國家代碼
茅利塔尼亞	MR
模里西斯	MU
摩爾多瓦	MD
摩納哥	MC
蒙特內哥羅	ME
摩洛哥	MA
莫三比克	MZ
納米比亞	NA
荷蘭	NL
尼日	NE
奈及利亞	NG
北馬其頓	MK
挪威	NO
阿曼	OM
巴勒斯坦	PS
波蘭	PL
葡萄牙	PT
卡達	QA
羅馬尼亞	RO
俄羅斯	RU

國名	國家代碼
盧安達	RW
聖馬利諾	SM
聖多美普林西比	ST
沙烏地阿拉伯	SA
塞內加爾	SN
塞爾維亞	RS
賽席爾	SC
獅子山	SL
斯洛伐克	SK
斯洛維尼亞	SI
索馬利亞	SO
南非	ZA
南蘇丹	SS
西班牙	ES
瑞典	SE
瑞士	CH
坦尚尼亞	TZ
多哥	TG
突尼西亞	TN
土耳其	TR

國名	國家代碼
烏干達	UG
烏克蘭	UA
阿拉伯聯合大公國	AE
英國	GB
梵蒂岡	VA
葉門	YE
尚比亞	ZM
辛巴威	ZW
奧蘭群島	AX
南極洲	AQ
布威島	BV
英屬印度洋領地	IO
法羅群島	FO
法屬南部領地	TF
直布羅陀	GI
格陵蘭	GL
根西島	GG
曼島	IM
澤西島	JE
馬約特島	YT

國名	國家代碼
留尼旺	RE
聖赫勒拿	SH
南喬治亞和南桑威奇群島	GS
斯瓦巴和揚馬延	SJ
西撒哈拉	EH

組織的受管政策

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

當您使用我們的新 AWS 體驗時，會 AWS 管理組織管理政策，包括資源控制政策 (RCPs) 和服務控制政策 (SCPs)。這些保護性控制可防止專案擁有者或團隊成員執行會抑制 AWS 已定義之預先設定預設值的動作，以協助您快速建置和開發。

專案的服務控制政策

以下是專案中所有使用者的服務控制政策，無法變更：

```
{
  "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"
        }
      }
    }
  ]
}

```

當您啟用進階功能時，不會移除此政策。如需詳細資訊，請參閱[啟用進階 AWS 功能](#)。

啟用進階功能後，此政策會保持連接至組織的根目錄，因此適用於每個成員帳戶，包括您稍後建立或邀請的帳戶。

此外，我們為專案中的所有使用者套用下列服務控制政策，以限制對不支援或必須在 AWS 設定中完成的專案進行特定修改：

```

{
  "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"
    }
  }
}
]
}

```

當您啟用進階功能時，會移除此政策。如需詳細資訊，請參閱[啟用進階 AWS 功能](#)。

移除此政策不會讓您更新專案帳戶的根使用者電子郵件地址。如需詳細資訊，請參閱[啟用進階功能之後的專案帳戶](#)。

此外，我們也會對專案中的所有使用者套用下列服務控制政策，以限制 AWS 區域 以允許 支援分割區服務，視您####而定：

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partitioinal",
      "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"
        ]
      }
    }
  }
]
}

```

啟用進階功能後，下列服務控制政策會套用至您的帳戶：

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UsEast1Partitioal",
      "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"
            ]
        }
    }
}
]
}

```

支出限制的服務控制政策

如果您使用支出限制，下列服務控制政策會在接近支出限制時套用至您的專案。如需支出限制的詳細資訊，請參閱 [在 AWS 設定中建立支出限制](#)。

```

{
  "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": "*"
}
]

```

```
}
```

專案免費方案的服務控制政策

下列服務控制政策控制對新 AWS 體驗免費方案中可用 AWS 服務的存取。此政策無法修改。若要存取其他服務，請升級您的帳戶。如需詳細資訊，請參閱[在 AWS 設定中升級您的帳戶](#)。

```
{
  "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-HZTdNwJuq0KLReXC"
    ]
},
{
    "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"
            }
        }
    }
}

```

```
]
}
```

專案付費計劃的服務控制政策

下列服務控制政策控制對新 AWS 體驗付費計劃中可用 AWS 服務的存取。此政策無法修改。若要存取其他服務，請啟用進階功能。如需詳細資訊，請參閱[啟用進階 AWS 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:*",
"texttract:*",
"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-9c1kBcYznTkcpRI",
        "arn:aws:artifact::agreement/agreement-y03aUwMAEorHtqjv",
        "arn:aws:artifact::agreement/agreement-bexgr7sjvXAW4Gxu",
        "arn:aws:artifact::agreement/agreement-HZTdNwJuq0KLReXC"
    ]
},
{
    "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"
        }
    }
}
]
}

```

專案的資源控制政策

以下是[專案中](#)資源的資源控制政策。此政策無法修改：

```

{
  "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:*",
    "texttract:*",
    "transcribe:*",
    "translate:*"
  ],
  "Resource" : "*",
  "Condition" : {
    "Null" : {
      "aws:SourceAccount" : "false"
    },
    "StringNotEquals" : {
      "aws:SourceOrgID" : "${aws:ResourceOrgID}"
    }
  }
}
]
```

在專案之間切換

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您一次只能管理一個專案 AWS 的資源。您一律可以根據主控台右上角的名稱來判斷您所在的 AWS 專案。

從 切換作用中工作階段的專案 AWS 管理主控台

從 切換作用中工作階段的專案 AWS 管理主控台

1. 開啟 [AWS 管理主控台](#)。
2. 選擇右上角的專案名稱 AWS 管理主控台。
3. 選擇切換專案。
4. 在作用中工作階段下，選擇作用中工作階段。作用中工作階段是已登入長達 12 小時的工作階段。作用中的工作階段時間無法變更。
5. 系統會將您重新導向至新專案的 AWS 主控台首頁。

在 AWS 設定中的專案之間切換

在 AWS 設定中切換專案

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇您要存取的專案。
3. 在右上角的導覽列中，選擇建立和管理雲端基礎設施。

系統會將您重新導向回新專案 AWS 管理主控台 的。

從 切換專案 AWS 管理主控台

從 切換專案 AWS 管理主控台

1. 開啟 [AWS 管理主控台](#)。
2. 選擇管理專案。
3. 在 AWS 設定中，選擇您要存取的專案。
4. 在右上角的導覽列中，選擇建立和管理雲端基礎設施。

系統會將您重新導向回新專案 AWS 管理主控台 的。

邀請團隊成員在 AWS 設定中協作

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以讓團隊成員存取您的專案。當您與團隊成員共用專案時，您無法控制他們有權存取 AWS 的服務。您和團隊成員都可以存取專案。這表示團隊成員具有存取專案可用所有 AWS 服務的許可。這包括為服務和應用程式建立存取控制。不過，他們沒有執行管理或財務動作的許可，例如刪除專案或修改支出限制。若要檢視哪些團隊成員修改了 AWS 服務，請參閱 [使用 AWS CloudTrail 監控您的專案](#)。

在 AWS 設定中，您和您的團隊成員具有不同的存取層級。若要檢視套用至團隊成員的 AWS 受管政策，請參閱 [AWSManagedSettingsReadOnlyAccess](#)。若要檢視套用至專案擁有者的 AWS 受管政策，請參閱 [AWSManagedSettingsAdminAccess](#)。

將團隊成員新增至您的專案時，請考慮下列事項。

團隊成員的考量事項

團隊成員可以執行下列動作：

- 檢視、建立、編輯、刪除和修改專案中的 AWS 資源。
- 存取 AWS 設定。
- 檢視支出限制。
- 請求提高 AWS 服務的配額。

團隊成員無法執行下列動作：

- 離開專案。
- 採取任何根動作。如需詳細資訊，請參閱 [AWS 專案擁有者的動作](#)。
- 邀請團隊成員參與專案。
- 管理任何團隊成員的許可。
- 從專案中移除任何團隊成員。
- 變更專案的名稱。
- 設定或更新付款方式。

- 檢視或更新帳單詳細資訊，包括地址或電話號碼。
- 檢視或更新稅務資訊。
- 從免費方案升級至付費方案。
- 設定或修改每個專案的支出限制。
- 檢視每個專案的成本趨勢。
- 檢視所有專案的總 AWS 支出。
- 檢視和兌換非免費方案促銷點數。
- 檢視所有點數類型的剩餘點數和過期日期。
- 檢視完整的點數歷史記錄，包括獲得、套用和過期的點數。
- 檢視點數如何跨專案套用。
- 檢視未結餘額。
- 執行付款至 AWS。
- 下載發票或檢視過去的交易。
- 驗證 AWS 費用是否正確，包括套用的點數。
- 接收管理帳戶層級帳單通訊。
- 在組織層級取得帳單問題的協助。
- 請求提高帳戶和帳單配額。

團隊成員如何存取您的 AWS 資源

我們的新 AWS 體驗會為組織建立服務連結角色，其中包含您無法修改的所有專案。此角色會定期驗證團隊成員的內部記錄是否與您的實際團隊成員保持同步。

AWSServiceRoleForAccountAccessManager 服務連結角色信任下列服務擔任該角色：

- `account-access.amazonaws.com`

名為 `AccountAccessManagerServiceRolePolicy` 的角色許可政策允許帳戶存取管理員對指定的資源完成下列動作：

- 動作：`organizations:ListAccounts`、`organizations:ListAWSServiceAccessForOrganizations` 和 `organizations:DescribeAccount` 上的 `"arn:aws:organizations::*:account/o-*/*"`

如需詳細資訊，請參閱[AWS 帳戶存取管理員](#)。

邀請團隊成員在 AWS 設定中協作

若要邀請團隊成員，您可以從 AWS 設定中的 團隊頁面傳送邀請給他們。團隊成員有 14 天的時間接受邀請。團隊成員必須建立 AWS 建構家 ID 才能存取您的專案。他們可以使用註冊 AWS（新）來執行此操作。

邀請團隊成員在 AWS 設定中協作

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇團隊。
3. 選擇邀請新團隊成員。
4. 在電子郵件中，輸入電子郵件地址或電子郵件地址清單。以逗號 (,) 或分號 (;) 分隔電子郵件地址。
5. 選擇要與新團隊成員共用的一或多個專案。
6. 選擇傳送邀請。

如果您的團隊成員未收到邀請，請他們檢查垃圾郵件和垃圾桶資料夾。

在 AWS 設定中邀請團隊成員加入專案

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以邀請團隊成員存取專案。如需團隊成員可以在專案中執行哪些操作的資訊，請參閱 [邀請團隊成員在 AWS 設定中協作](#)。

邀請團隊成員參與專案

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇您要存取的專案。
3. 針對成員，選擇邀請新的團隊成員。
4. 在電子郵件中，輸入電子郵件地址或電子郵件地址清單。以逗號 (,) 或分號 (;) 分隔電子郵件地址。

5. 選擇要與新團隊成員共用的專案。
6. 選擇傳送邀請。

如果您的團隊成員未收到邀請，請他們檢查垃圾郵件和垃圾桶資料夾。

從 AWS 設定中的專案中移除團隊成員

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以隨時將團隊成員從專案中移除。您的團隊成員無法自行執行此操作。當您移除團隊成員時，他們將無法再存取該專案。團隊成員建立的任何資源都會保留在您的專案中，您必須加以管理。

從專案移除團隊成員

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇您要存取的專案。
3. 在成員索引標籤中，選取要從專案中移除的成員，然後選擇移除。
4. 確認您的選擇，然後選擇移除。

團隊成員仍然是您團隊的一部分，您可以將他們新增至其他專案。若要從 AWS 設定完全移除團隊成員，請參閱 [在 AWS 設定中移除團隊成員](#)。

在 AWS 設定中移除團隊成員

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以使用 團隊頁面，從所有專案中移除團隊成員。它們會自動失去對任何專案的存取權。不會刪除團隊成員建立的任何資源。

移除團隊成員

1. 在 [https : //https://settings.aws.com](https://settings.aws.com) 開啟 AWS 設定。
2. 在主導覽窗格中，選擇團隊。
3. 選取您要移除之團隊成員的核取方塊。
4. 選擇移除。
5. 確認您的選擇，然後選擇移除。

在 AWS 設定中撤銷對團隊成員的邀請

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以撤銷待定邀請。邀請將在 AWS 設定中保留 14 天。當您撤銷待定邀請時，邀請電子郵件中的存取連結將會停用。您無法撤銷已接受的邀請，而是移除團隊成員。如需詳細資訊，請參閱[在 AWS 設定中移除團隊成員](#)。

撤銷邀請

1. 在 [https : //https://settings.aws.com](https://settings.aws.com) 開啟 AWS 設定。
2. 在主導覽窗格中，選擇團隊。
3. 選取具有待定邀請之團隊成員的核取方塊。
4. 選擇撤銷。
5. 確認您的選擇，然後選擇撤銷邀請。

在 AWS 設定中重新傳送邀請給團隊成員

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以為已撤銷、過期或拒絕的邀請重新傳送邀請給團隊成員。當您重新傳送邀請時，您的團隊成員會收到一封電子郵件，其中包含您重新傳送邀請後 14 天的過期日期。

重新傳送邀請

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇團隊。
3. 選取已撤銷、過期或拒絕邀請之團隊成員的核取方塊。
4. 選擇重新傳送。
5. 確認您的選擇，然後選擇重新傳送邀請。

在 AWS 設定中升級您的帳戶

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

當您註冊註冊 AWS（新）時，您的帳戶位於免費方案中。在免費方案中，您會收到 100 USD 的註冊點數，並獲得高達 100 USD 的額外點數。當您用完點數或帳戶超過 6 個月時，您必須升級至付費計劃。您也可以隨時升級至付費計劃。升級到付費計劃時，您可以存取中列出的服務 [AWS 服務 包含在我們新 AWS 體驗的付費計劃中](#)。

升級帳戶的考量事項

升級到付費計劃時，請考慮下列事項：

- 您無法升級個別專案。當您升級帳戶時，所有專案都會升級。
- 升級時，您可以存取 Always Free 服務和短期試用優惠。
- 您符合其他促銷點數和折扣的資格。
- 您必須支付超出點數餘額的費用。
- 您可以建立支出限制，以設定您每月為專案支付的最高金額。如需詳細資訊，請參閱 [在 AWS 設定中 建立支出限制](#)。
- 您無法將任何專案指定為 HIPAA 或 SEC 合規。
- 點數用盡時，您的帳戶不會關閉。

- 這不會將您升級至 [註冊 AWS \(進階\)](#)。當您升級帳戶時，只有使用 建立的帳戶才支援的任何功能 [註冊 AWS \(進階\)](#) 都無法使用。不過，您可以 [啟用進階 AWS 功能](#) 為您的帳戶提供。
- 您無法反轉升級程序。

在 AWS 設定中升級您的帳戶

升級您的帳戶

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇帳單。
3. 選擇 Upgrade (升級)。
4. 選擇開始使用。
5. 新增您的付款方式。

根據您的位置，您可能需要提供一些稅務資訊。

6. 選擇升級帳戶。
7. 選擇繼續以返回建置，或選擇設定支出限制以設定支出限制。如需花費限制的詳細資訊，請參閱 [在 AWS 設定中建立支出限制](#)。
8. 選擇前往主控台。

您的升級已完成。

在 AWS 設定中建立支出限制

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

什麼是支出限制？

支出限制可讓開發人員 AWS 放心地在可預測且受控制的預算內操作。使用支出限制來設定您每月為專案支付的最高金額。支出限制位於專案層級。您可以為某些專案設定支出限制，同時不針對其他專案設定支出限制。

如果您在專案中的用量達到其限制，會 AWS 暫停該專案以停止其資源，讓您的成本保持在其中。支出限制專為實驗、學習和沙盒工作負載而設計。當您的應用程式產生意外成本時，如果可以短暫暫停您的資源，則可以將其用於生產環境。

擁有專案存取權的任何人都可看見支出限制，但只能由專案擁有者管理。您必須參與付費計劃才能建立支出限制。如需詳細資訊，請參閱[在 AWS 設定中升級您的帳戶](#)。

支出限制是一種 [AWS Budgets](#)。

設定您的花費限制

您的支出限制是專案稅前成本的上限，而不是費用。當您設定支出限制時，允許的最小值為 20 USD 或可能支出的保守估計。

存在最低限度的原因：抑制支出限制是一種破壞性體驗。最小值存在，使得使用中的正常變化不太可能導致達到支出限制。

計算保守估計的方式：估計是根據您的活動月份迄今，但它不是嚴格線性 extrapolation. AWS looks 迄今為止的花費，以及您目前執行的資源。AWS 也會使用上個月的活動，如果此值很高，則會變成最小值。

如果您有許多資源正在執行：可能支出的保守估計將會很高。如果您想要設定較低的支出限制，您必須先停止這些資源。

如果您要重新啟用暫停的專案：可能花費的保守估計是本月至今的花費，加上任何未收費的用量。

Note

支出限制不包括抵用金，並適用於稅前費用。

通知

當實際成本達到限制的 50%、75% 和 90% 時，或當您有望在未來 10 天內達到或超過您的支出限制時，您將會收到通知。

使用選用的早期成本控制來自訂您的支出限制設定

您的支出限制會防止您的帳單超過您設定的金額。如果您的用量達到此上限，會 AWS 暫停您的資源來保護您。這些選用控制項會更早且更柔和地運作，因此您遠低於限制。

停止建立新資源

在達到限制之前大約 7 天，新資源會停止啟動。這可透過套用由管理的服務控制政策來實現 AWS。服務控制政策取決於服務。若要檢視可能套用至專案的所有服務控制政策，請參閱 [支出限制的服務控制政策](#)。

所有已在執行的資源都會保持執行中。在大多數情況下，您建置的任何內容都不會受到影響。不過，在某些情況下，這可能會導致破壞性體驗。例如，如果您已啟用自動調整規模，且符合執行此動作的條件，則新執行個體將不會啟動。

暫停閒置資源

在您達到限制之前大約 5 天，閒置資源會暫停。您的作用中應用程式會繼續執行。閒置資源會根據 AWS Compute Optimizer 的建議暫停。如需詳細資訊，請參閱 [檢視閒置建議](#)。

您也可以登入專案並檢視節省成本的機會，以檢視閒置資源建議。如需詳細資訊，請參閱 [成本最佳化中樞](#)。目前，作為您的支出限制體驗的一部分，我們將自動暫停 EC2、RDS 和 SageMaker 端點。

我們暫停 EC2 執行個體的原因：如果尖峰 CPU 使用率低於 5%，且您的網路 I/O 在過去 14 天內每天少於 5 MB，我們會暫停 EC2 執行個體。

如果您有 G 或 P 執行個體類型，則會有不同的閒置條件。如果 G 或 P 執行個體類型在過去 14 天內為 true，則會暫停：

- GPU 主動運作的時間未超過回溯期間的 99%
- GPU 編碼器的使用時間未達執行個體執行時期的 99% 或更長時間
- 執行個體層級的 GPU 記憶體用量低於 5%
- CPU 最大使用率未達 5%
- 網路使用率小於 5 MB/天

我們暫停 RDS 資料庫的原因：如果資料庫執行個體不是僅供讀取複本，且在過去 14 天內具有下列項目，我們會暫停 RDS for MySQL 和 RDS for PostgreSQL：

- 沒有資料庫連線
- CPU 用量低
- 低讀取/寫入活動

我們暫停閒置 SageMaker 端點的原因：如果端點在過去 14 天內沒有調用，我們會暫停 SageMaker 端點。

暫停最高成本驅動因素

在達到限制之前大約 4 天，會產生最高成本的作用中資源會暫停。這可能是破壞性的體驗。目前，我們從這五個服務中選取資源：EC2、RDS、Lambda、Bedrock 和 SageMaker。如果您有失控的 Lambda 或非預期的 Bedrock 峰值，此選擇加入控制可能會阻止您產生成本。

如果您達到限制會發生什麼情況

AWS 會暫停您的專案並停止所有資源。您的資料會保留。

若要重新啟用專案，請從 AWS 設定增加您的支出限制。重新啟用後，某些資源可能需要手動重新啟動。

Important

如果您在專案暫停的 90 天內未採取任何動作，會 AWS 永久刪除專案資料。

其他需要注意的重要事項

- 如果您使用 Amazon Route 53，則每 24 小時只能購買一個網域。您必須確保網域成本在支出限制內，否則您的網域購買將不會通過。在這種情況下，您必須在進行購買之前提高支出限制。
- 您最多可以將花費限制套用至 10 個專案。

在 AWS 設定中建立支出限制

在 AWS 設定中建立支出限制

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇帳單。
3. 在依專案的成本中，針對花費限制，選擇設定專案的限制。
4. 您可以選擇建議的支出限制或自訂限制。
5. 如果您選擇自訂限制，請輸入自訂數量。
6. 選擇設定支出限制。

- 若要使用早期成本控制自訂您的支出限制，您可以選取停止新資源啟動、暫停閒置資源或暫停最高成本驅動因素。
- 選擇儲存早期成本控制。

支出限制會立即生效。

在 AWS 設定中更新支出限制

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

專案擁有者可以隨時在 AWS 設定中更新支出限制。您可以增加或減少支出限制，或變更選用的提早成本控制。如果 AWS 因為您即將接近限制而封鎖了新資源啟動或暫停的資源，您可以提高支出限制。如果您的專案因為達到限制而暫停，請提高支出限制以重新啟用專案。如需支出限制運作方式的詳細資訊，請參閱 [在 AWS 設定中建立支出限制](#)。

在 AWS 設定中更新支出限制

更新支出限制

- 在 <https://settings.aws.com> 開啟 AWS 設定。
- 在主要導覽窗格中，選擇帳單。
- 在依專案成本中，針對花費限制，選擇鉛筆圖示。
- 針對每月花費限制 (USD)，輸入新的花費限制。

我們根據您目前的花費提供建議。

- 若要修改您想要在專案上使用的保護，請選取停止新資源啟動、暫停閒置資源或暫停最高成本驅動程式。
- 選擇儲存設定。

支出限制變更會立即生效。

在 AWS 設定中移除支出限制

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

專案擁有者可以隨時在 AWS 設定中移除支出限制。當您移除支出限制時，AWS 將不再監控您的成本，也不會對您的專案採取任何早期成本控制。如需支出限制運作方式的詳細資訊，請參閱 [在 AWS 設定中建立支出限制](#)。

在 AWS 設定中移除支出限制

移除支出限制

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇帳單。
3. 在依專案成本中，針對花費限制，選擇鉛筆圖示。
4. 選擇移除限制。
5. 確認您的選擇，然後選擇移除。

您的花費限制將立即移除。

我們新 AWS 體驗中的免費方案

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以使用 AWS 免費方案來探索 AWS 服務，無需成本承諾。如果您是初次使用 AWS，無論您的帳戶計劃為何，您都會在建立帳戶後獲得 100 USD 的額度。完成活動還可以額外獲得 100 美元抵用金，讓您運用在所有專案中。如需獲得額外點數的詳細資訊，請參閱 [獲得額外的點數](#)。此外，您還可以存取超過 30 個一律提供免費 AWS 服務，這些服務提供每月免費用量限制。

免費帳戶計劃非常適合試用 AWS 服務並建立概念驗證的客戶，免費有效期長達六個月。除非您升級為付費帳戶計畫，否則在此期間不會產生任何費用。您的免費帳戶計畫會在六個月後或抵用金用完時結

束，以先發生者為準。此外，免費帳戶計劃無法存取會快速使用整個 AWS 免費方案點數或硬體購買的特定 AWS 服務。如需免費帳戶計劃的合格服務清單，請參閱[註冊 AWS（新）支援的 AWS 服務](#)。

付費帳戶計劃非常適合用於建置超出初始額度的生產應用程式。當您的用量超過抵用金餘額，或使用抵用金不適用的服務時，您需要支付標準隨pay-as-you-go定價。

您擁有的所有專案都屬於相同的計劃類型。如果您升級至付費帳戶計劃，則所有專案都可以存取其他服務，並為所有專案支付標準隨pay-as-you-go定價。如需詳細資訊，請參閱[設定中的 AWS 升級您的帳戶](#)。

您可以使用 成本管理主控台來追蹤所有 AWS 服務的用量，為您的專案提供免費方案。

追蹤您的免費方案用量

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

AWS 當您超過每個服務免費方案限制的 85% 時，免費方案用量提醒會自動透過電子郵件通知您。如需其他追蹤，您可以設定零支出預算，將設定為將用量追蹤至免費方案限制的 100%。您還可以篩選預算以追蹤個別服務。

您可以透過下列方式追蹤 AWS 免費方案用量。

使用 AWS 設定

您可以在 AWS 設定中監控您的免費帳戶計劃過期日期、點數餘額和剩餘天數。如需詳細資訊，請參閱在[AWS 設定中檢視和兌換點數](#)。您也會在接近免費帳戶計劃期間結束時，定期收到有關點數餘額的電子郵件提醒。

如果您有付費計劃，您可以在 AWS 設定中的點數頁面上監控點數餘額和過期日期。如需升級至付費計劃的詳細資訊，請參閱[在 AWS 設定中升級您的帳戶](#)。

使用 Billing and Cost Management 主控台

您可以使用 Billing and Cost Management 主控台來追蹤每個專案的免費方案用量。帳單和成本管理主控台會顯示month-to-date用量和任何服務方案達到或超過用量限制的摘要。對於每個使用中的免費方案優惠，您可以檢視下列項目：

- 服務
- AWS 免費方案用量限制
- 您目前的用量
- 您的預測用量
- 您的month-to-date(MTD) 實際用量
- 您的預測month-to-date(MTD) 用量

下列程序說明如何使用帳單和成本管理主控台，根據month-to-date的實際用量來排序 免費方案用量。

排序 免費方案用量

1. 開啟 Billing and Cost Management 主控台，網址為 <https://console.aws.amazon.com/cost-management/>。
2. 選擇免費方案。
3. 若要依month-to-date的實際用量排序，請選擇 MTD 實際用量 %。

獲得額外的點數

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

如果您是新 AWS 客戶，無論您的帳戶計劃為何，只要完成活動，您都可以獲得額外的 100 USD 的點數。這些活動可協助您學習 AWS 服務。您可以在 AWS 主控台首頁儀表板的探索 AWS 小工具中找到活動。所有這些活動都會產生從 AWS 免費方案點數中扣除的 AWS 服務費用，但是當您完成每個活動時，您會收到 20 USD 的點數。

要完成的活動

- [使用 Amazon EC2 啟動執行個體](#)
- [在 Amazon Bedrock 遊樂場中使用基礎模型](#)
- [建立預算](#)
- [使用 Lambda 建立 Web 應用程式](#)
- [建立 Amazon RDS 資料庫](#)

在 AWS 設定中檢視您的帳單資訊

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以使用 AWS 設定來檢視帳單資訊。如果您使用的是免費方案，此頁面會顯示您有多少天的免費方案和 AWS 您的點數。您也可以檢視每個專案的成本。如果您使用的是付費計劃，您可以檢視餘額、目前費用和每個專案的成本。如果您使用的是支出限制，您可以檢視與限制相關的資訊。您也可以 [在 AWS 設定中管理您的付款方式](#) 和 [在 AWS 設定中管理稅務註冊](#)。

當您使用免費計劃時，AWS 免費方案點數涵蓋所有用量。如果您用完 AWS 免費方案點數或在 184 天後，以先發生者為準，則需要升級至付費計劃。如需升級至付費計劃的詳細資訊，請參閱 [在 AWS 設定中升級您的帳戶](#)。

依專案檢視您的成本

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇帳單。
3. 在依專案的成本下，您會看到 month-to-date 費用和預測 month-to-date 費用。您將看到專案的所有費用。
4. （選用）若要在檢查成本下檢視專案費用明細，請選擇檢視。系統會將您重新導向至 AWS Billing and Cost Management 主控台。

您在 Billing and Cost Management Console 上看到的帳單資料和 Cost Explorer 資料每天至少重新整理一次。AWS 重新整理時的節奏可能會有所不同。如果您使用支出限制，這可能會導致 AWS 設定和 AWS 成本管理主控台中 month-to-date 預估費用的差異。

在 AWS 設定中檢視帳單歷史記錄

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以在 AWS 設定中檢視帳單歷史記錄。只有在您有付款方式時，才能使用您的帳單歷史記錄。如果您使用的是免費方案，則不會看到您的帳單歷史記錄。

您可以下載您在計費期間交易的每個服務提供者的發票。這包括費用類型、發票日期和美元總計等資訊。如果您的發票以其他幣別開立，畫面上還會顯示以其他幣別表示的總計。發票不會分割到每個專案。

檢視您的帳單歷史記錄

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇帳單。
3. 在餘額旁邊，選擇檢視帳單歷史記錄。系統會將您重新導向至帳單歷史記錄。
4. 若要下載發票，請選取發票 ID。

在 AWS 設定中管理您的付款方式

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以在 AWS 設定中管理您的付款方式。您的付款方式用於支付所有專案中的 AWS 資源使用量。只有在您在建立帳戶時提供資訊，或將帳戶升級至付費計劃時，才能管理您的付款方式。

管理您的付款方式

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇帳單。
3. 在餘額下，您會看到付款資訊。選擇管理。
4. 針對付款方式，選擇更新。
5. 輸入您的新付款方式，然後選擇儲存。

在 AWS 設定中進行付款

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以在 AWS 設定中支付 AWS 帳單。會在每月開始時自動向您的預設付款方式 AWS 收費。如果無法成功處理收費，您可以使用主控台來更新付款方式並進行付款。

在付款之前，請確定您要在未來自動收費的付款方式已設定為您的預設付款方式。如果您使用信用卡，請確認該張信用卡未過期。

若要進行付款

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇帳單。
3. 在餘額旁邊，選擇檢視帳單歷史記錄。系統會將您重新導向至帳單歷史記錄。
4. 在動作下，您會看到任何未結發票的付款發票。如果沒有列出的發票，您不需要執行任何動作。
5. 選擇支付發票。
6. 確認您的選擇，然後選擇付款。

如果您對於向銀行帳戶收費或結清逾期未付餘額的問題有任何疑問，請至 [Support 中心](#) 申請立案處理。

在 AWS 設定中變更您偏好的貨幣

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以在 AWS 設定中變更偏好的貨幣。您偏好的貨幣僅適用於您擁有的專案。某些帳單國家會限制付款貨幣。您的發卡銀行可能會收取其他貨幣轉換的費用。

變更您偏好的顯示貨幣

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇帳單。
3. 在餘額下，您會看到付款資訊。選擇管理。如果您沒有看到餘額，則無法變更貨幣。
4. 選擇設定貨幣。
5. 對於預設付款貨幣，選取付款貨幣。
6. 選擇儲存。

在 AWS 設定中管理稅務註冊

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以在 AWS 設定中管理您的稅務註冊號碼和免稅項目。您的稅務資訊僅適用於您擁有的專案。

更新與刪除稅務登記號碼

請透過下列步驟，更新或刪除一或多組稅務登記號碼。

Note

如果國家/地區未列在稅務設定頁面下拉式清單中，AWS 目前不會收集該國家/地區的稅務註冊。

更新稅金註冊號碼

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇帳單。
3. 在餘額下，您會看到付款資訊。選擇管理。
4. 選擇稅務設定。
5. 修改您的稅務註冊資訊。
6. 選擇儲存。

管理您的美國免稅資料

如果您的州符合資格，您可以在 AWS 設定中的計劃和帳單頁面上管理您的美國免稅額。您為豁免上傳的文件會在 24 小時內由 Support 審核。只有在您的帳戶註冊為企業時，您才能管理您的免稅額。

上傳或新增您的美國免稅資料

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇帳單。
3. 在餘額下，您會看到付款資訊。選擇管理。
4. 選擇 Manage tax exemption (管理免稅)，然後選取 Add tax exemption (新增免稅)。
5. 指定您的免稅類型和司法管轄區。
6. 上傳憑證文件。
7. 檢閱您的資訊，然後選擇 Submit (提交)。

在 24 小時內，如果支援案例需要其他資訊，或者您的任何文件無效，支援將透過支援案例通知您。

一旦核准獲得免稅後，您可以在免稅分頁下看見，並包含 Active (有效) 期。

如果您的免稅申請遭到拒絕，系統將透過個案協助聯絡人通知您。

在 AWS 設定中檢視和兌換點數

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

您可以在 AWS 設定中檢視和兌換可用的抵用金。抵 AWS 用金會自動套用至帳單，以協助支付與合格服務相關聯的成本。如需合格服務的詳細資訊，請參閱[兌換您的 AWS 促銷點數](#)。點數會套用至您擁有的所有專案，直到用盡或過期為止。您無法選取哪個專案使用您兌換的點數，它們會套用至您擁有的所有專案。

檢視您的點數

1. 在 <https://settings.aws.com> 開啟 AWS 設定。

2. 在主要導覽窗格中，選擇帳單。
3. 在目前費用容器中，您會看到可用的點數。選擇您的點數。

視您的計劃類型而定，系統會將您重新導向至作用中和過期的點數檢視，或是您的點數和過去 6 個月的非作用中點數檢視。

4. 若要檢視可與點數搭配使用 AWS 的服務，請選擇查看服務清單。

兌換您的 AWS 促銷點數

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇帳單。
3. 在目前費用容器中，您會看到可用的點數。選擇您的點數。

視您的計劃類型而定，系統會將您重新導向至作用中和過期的點數檢視，或是您的點數和過去 6 個月的非作用中點數檢視。

4. 選擇兌換點數以兌換您的點數。
5. 針對促銷碼，輸入出現的促銷碼。當您兌換抵用金時，表示您已閱讀並同意 [AWS 促銷抵用金條款與條件](#)。
6. 選擇兌換點數。

在 AWS 設定中管理印度的帳戶

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

如果您註冊 AWS 並選擇印度做為聯絡地址和帳單地址，您的使用者協議是與 AWS Amazon Web Services India Private Limited (AWS India) 簽訂的。印度 AWS 會管理您的帳單，而您的發票總計會以印度盧比 (INR) 而非美元 (USD) 列出。

如果您的帳戶位於 AWS 印度，請遵循本主題中的程序來管理您的帳戶。本主題說明如何註冊 AWS 印度帳戶、編輯有關 AWS 印度帳戶的資訊、管理客戶驗證，以及新增或編輯您的永久帳戶號碼 (PAN)。

主題

- [向 AWS 印度註冊 AWS \(新\)](#)

- [管理您的客戶驗證資訊](#)

向 AWS 印度註冊 AWS（新）

AWS 印度是印度 AWS 的本地賣方。如果您的聯絡人和帳單地址位於印度，請使用下列程序註冊。

使用註冊 AWS（新）與 AWS 印度

1. 前往 <https://aws.amazon.com>。
2. 在說明註冊 AWS（新）和註冊 AWS（進階）之間差異的橫幅上，選擇註冊 AWS。
3. 選擇登入，例如 Google、Apple、GitHub 或 Amazon。
4. 系統會將您導向至供應商的登入。登入後，系統會將您重新導向至 AWS 註冊。
5. 輸入您的名稱，然後選擇繼續。

當您授予團隊成員存取專案的權限時，此名稱將會與團隊成員共用。

6. 輸入驗證碼，驗證與您的登入相關聯的電子郵件。驗證您的電子郵件後，請選擇繼續。
7. 輸入您帳戶的高強度密碼，然後選擇繼續。

AWS 需要您的密碼符合下列條件：

- 它必須至少有 8 個字元，最多 128 個字元。
- 它必須至少包含下列三種字元類型：大寫、小寫、數字和 ! @ # \$ % ^ 管理入口網站 * () < > 【】 {} | _ + = 符號。
- 它不能與 AWS 帳戶 您的姓名或電子郵件地址相同。

8. 輸入您的聯絡詳細資訊，然後選擇繼續。

如果您的聯絡地址或帳單地址位於印度，且符合印度電腦緊急應變團隊 (CERT-In) 法規，AWS 則必須先收集並驗證您的身分資訊，才能授予您 AWS 服務的存取權。

您在聯絡或帳單資訊之間選擇的名稱必須與計劃用於客戶驗證的文件上顯示的名稱完全相符。例如，如果您計劃使用公司註冊憑證來驗證企業帳戶，您必須提供文件上顯示的商業名稱。如需接受的證件類型清單，請參閱[the section called “用於客戶驗證的可接受印度證件”](#)。

9. 選擇您註冊帳戶的主要目的。
10. 選擇最能代表帳戶擁有者的所有權類型。如果您選擇公司、組織或合作夥伴關係做為所有權類型，請輸入關鍵管理人員的名稱。主要管理人員可以是主管、營運主管，或負責業務營運的人員。
11. 根據您選擇的所有權類型，選擇要用於驗證的已接受印度文件類型，並輸入您的文件資訊。

 Note

如果您有個人帳戶，並打算使用不是由印度聯發行的駕照，我們建議您使用不同的個人文件類型進行驗證。

12. 選擇您要用於客戶驗證的名稱。

如果帳單名稱和聯絡資訊與印度地址相關聯，則會顯示這些名稱以供選擇。請確定您選擇的名稱符合您計劃用於客戶驗證的文件類型名稱。如果您需要變更與帳單或聯絡地址相關聯的名稱，您可以在完成帳戶註冊後進行變更。

13. 同意提交資訊以供驗證，然後選擇繼續。

完成帳戶註冊後，系統會透過電子郵件通知您客戶驗證結果。您也可以在我的 AWS 設定中的設定檔頁面上檢查狀態。您必須通過客戶驗證才能存取 AWS 服務。

14. AWS 將佈建您的第一個專案。

若要存取 AWS 設定，請從 選擇管理專案 AWS 管理主控台。在 AWS 設定中，您可以邀請團隊成員、建立新專案，以及修改您的帳單和其他設定。

管理您的客戶驗證資訊

為了符合印度電腦緊急回應團隊 (CERT-In) 法規，AWS 在授予您新的或繼續存取 AWS 服務之前，需要收集並驗證您的身分資訊。您的身分必須使用您提供的印度帳單或聯絡地址中的名稱進行驗證。在驗證期間，AWS 將檢查文件號碼是否有效，以及您提供的名稱是否與您用於客戶驗證的文件相關聯的名稱相符。您在聯絡或帳單資訊之間選擇的名稱必須與文件上顯示的名稱完全相符。

若要更新您的帳單名稱、地址和其他聯絡資訊，請參閱 [使用 AWS 設定](#)。如果您編輯先前用於客戶驗證的任何資訊，例如帳單或聯絡資訊中的名稱或印度地址，您可能需要更新並重新提交客戶驗證資訊。

檢查您的客戶驗證狀態

您可以隨時在管理設定檔頁面上檢視您的客戶驗證狀態。如果您的驗證狀態為需要驗證或驗證失敗，請建立或更新客戶驗證資訊並提交以進行驗證。

建立您的客戶驗證資訊

若要完成客戶驗證，您需要提供已接受印度文件的資訊。如需接受的證件類型清單，請參閱 [the section called “用於客戶驗證的可接受印度證件”](#)。

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理設定檔。
3. 針對客戶驗證，選擇建立客戶驗證。
4. 選擇與您計劃用於客戶驗證的文件名稱完全相符的名稱。例如，如果您計劃使用公司註冊憑證來驗證企業帳戶，您必須提供文件上顯示的商業名稱。
5. 提供頁面上請求的其餘資訊。根據您選擇的文件類型，您可能需要上傳文件正面和背面的副本。如果您上傳映像檔案，請確定文件中的所有資訊都可見且清晰。
6. 選擇提交。

您將透過電子郵件或在 AWS 運作狀態儀表板上收到客戶驗證結果和任何後續步驟的通知。

編輯您的客戶驗證資訊

您可以編輯客戶驗證資訊，例如帳戶註冊的主要用途、組織類型，以及您想要用於驗證的名稱、文件類型、文件上傳或文件資訊。

如果您編輯用於客戶驗證的名稱或文件類型，或更新任何文件資訊，儲存變更將需要再次驗證您的身分。

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理設定檔。
3. 針對客戶驗證，選擇客戶驗證。
4. 選擇編輯，然後更新您要變更的資訊。

當您更新資訊時，請注意下列指引：

- 如果您選擇不同的名稱，名稱必須與計劃用於客戶驗證的文件上的名稱完全相符。例如，如果您計劃使用公司註冊憑證來驗證企業帳戶，您必須提供文件上顯示的商業名稱。
 - 如果您選擇不同的文件類型，您將需要上傳文件的正反面（如適用）的副本。文件上傳中的所有資訊都應清晰可見。
 - 如果您有個人帳戶，並打算使用不是由印度聯發行的駕照，我們建議您使用不同的個人文件類型進行驗證。
 - 如需接受的證件類型清單，請參閱 [the section called “用於客戶驗證的可接受印度證件”](#)。
5. 選擇提交。

如果因為儲存的變更類型而必須再次驗證您的身分，您將會透過電子郵件收到客戶驗證結果和任何後續步驟的通知。您也可以返回客戶驗證頁面或在 AWS 運作狀態儀表板中檢視結果。

用於客戶驗證的可接受印度證件

接受以下列印度政府核發的證件類型進行客戶驗證。

Note

下列共用的連結可能由政府變更。

- **PAN 卡** - 提供數位和實體格式，永久帳號 (PAN) 卡包含由印度稅務局核發給個人、公司和實體的唯一英數字元識別符。PAN 有十個字元，包括英文字母和數字，格式為 **AAAAA1111A**。若要使用此文件進行驗證，您還必須提供出現在 PAN 文件上的出生日期（個人）或成立日期（商業），並上傳卡片正面。您可以前往[收入稅部門的官方網站](#)，檢查 PAN 的有效性。
- **選民身分證/EPIC** - 選民身分證，也稱為選舉人照片身分證 (EPIC)，包含由印度選舉委員會核發給印度合格選民的唯一身分證號碼。選民 ID/EPIC 號碼包含十個字元，包括字母和數字。您可以前往[印度選舉委員會](#)的官方網站，檢查選民 ID 的有效性。若要使用此文件進行驗證，您必須同時上傳卡片的正面和背面。
- **駕照** - 如果您的駕照不是由印度聯邦核發，我們建議您使用不同的文件類型進行驗證。駕照號碼包含 12-16 個字元，包括字母、數字和空格或連字號。若要使用此文件進行驗證，您必須提供您的出生日期，並上傳卡片的正面和背面。您可以前往道路運輸和高速公路部的 [Parivahan Sewa 網站](#)，檢查駕照的有效性。
- **公司註冊憑證** - 公司註冊憑證是由公司事務部 (MCA) 發行的文件，該文件將企業註冊為法人實體。憑證用於唯一識別和追蹤在印度註冊的公司。每個憑證都包含企業識別號碼 (CIN)，這是由 21 個字元組成的唯一英數識別符，包括字母和數字。若要使用此文件進行驗證，您必須上傳公司註冊憑證文件。您可以前往[公司事務部入口網站](#)，檢查 CIN 的有效性。

個人和企業帳戶接受不同的印度證件類型：

- 對於個人帳戶 - PAN 卡、選民 ID 卡/EPIC 和駕照。
- 對於商業帳戶 - PAN 卡和公司註冊憑證。

在設定中設定您的印度帳單 AWS

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

如果您註冊 AWS 並選擇印度做為聯絡地址和帳單地址，您的使用者協議是與印度當地 AWS 賣方 Amazon Web Services India Private Limited (AWS India) 簽訂的。AWS India 會管理您的帳單，您的發票總計會以盧比列出，而不是美元。所有稅務資訊只能由專案擁有者建立或修改。

如需其他稅務或帳單資訊，您可以針對每個專案使用 AWS Billing 主控台。

使用 AWS 設定之管理設定檔頁面中的計劃和帳單區段來執行下列任務：

- 新增或編輯永久帳號
- 編輯多個永久帳號
- 編輯 Goods and Services Tax number
- 檢視稅務發票

新增或編輯永久帳號

您可以新增 Permanent Account Number (PAN) 到您的帳戶並進行編輯。

若要新增或編輯 PAN

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理設定檔，然後選擇計劃和帳單。
3. 在 Tax Settings (稅金設定) 導覽列中選擇 Edit (編輯)。
4. 對於 Permanent Account Number (PAN)，輸入您的 PAN，然後選擇 Update (更新)。

編輯多個永久帳號

您可以編輯帳戶中的多重 Permanent Account Number (PAN)。

編輯多重 PAN 號碼

1. 在 <https://settings.aws.com> 開啟 AWS 設定。

2. 在主導覽窗格中，選擇管理設定檔，然後選擇計劃和帳單。
3. 在 Manage Tax Registration Numbers (管理稅金註冊號碼)，選擇想要編輯的 PAN 號碼。
4. 在 Manage Tax Registration (管理稅金註冊) 底下，選擇 Edit (編輯)。
5. 更新要變更的欄位，然後選擇 Update (更新)。

編輯 Goods and Services Tax number

您可以編輯帳戶中的多重 Goods and Services Tax number (GST)。

編輯多重 GST 號碼

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理設定檔，然後選擇計劃和帳單。
3. 在 Manage Tax Registration Numbers (管理稅金註冊號碼)，選擇想要編輯的 GST 號碼或選擇 Edit all (全部編輯)。
4. 在 Manage Tax Registration (管理稅金註冊) 底下，選擇 Edit (編輯)。
5. 更新要變更的欄位，然後選擇 Update (更新)。

檢視稅務發票

您可以在 AWS 設定中檢視您的稅務發票。

若要檢視稅務發票

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理設定檔，然後選擇計劃和帳單。
3. 向下捲動並選擇發票標籤。
4. 在稅務發票區段中，選擇文件 ID 下提及的發票連結。

Note

只有在有可用的稅金發票時，才會看見稅金發票區段。

變更往來 AWS 印度的記錄賣方

您可以透過更新您的帳單或稅務資訊，將記錄 AWS 帳戶 賣方 (SOR) 變更為另一個 SOR。如果您的 AWS 印度帳戶在無法使用此功能的舊版模型中操作，則不適用此選項。當您在帳單或稅務詳細資訊中編輯您的國家或地區時，如果新位置的服務提供者與您目前的位置不同，您帳戶的 SOR 將自動變更。

如果您要將帳戶變更為印度或從 AWS 印度進行變更，則不需要更新設定為發票或電匯的預設付款方式。如果您的預設付款方式是信用卡或簽帳金融卡，您必須重新確認您的預設支付卡詳細資訊。這是為了確保付款方式與 AWS 印度以外的交易分開存放。如需詳細資訊，請參閱[檢視 AWS 印度發票適用的信用卡或簽帳金融卡](#)。

Note

如果您有使用信用卡或簽帳金融卡作為預設付款方式的 AWS 印度帳戶，且已設定自動付款的電子授權，則必須先停用電子授權，才能編輯預設付款偏好設定。

若要變更帳戶的 SOR，您可以使用下列選項編輯此資訊：

使用帳單和稅務資訊變更 SOR

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理設定檔，然後選擇計劃和帳單。
3. 在預設付款偏好設定區段中選擇編輯。
4. 輸入新的帳單地址。
5. 在付款貨幣區段中，從新 SOR 的已接受貨幣清單中選擇預設貨幣。
6. （如果您的預設付款方式是信用卡或簽帳金融卡）在確認付款方式區段下，重新輸入預設支付卡的詳細資訊，以確認新服務供應商的使用情形。

若要在新的 SOR 下變更預設卡片，請稍後新增您的卡片，並變更您的預設付款方式設定。

7. 選擇儲存變更。

幾分鐘後，包含更新 SOR 的變更會出現在付款偏好設定頁面上。

使用帳單和稅務資訊變更 SOR

若要將您的帳戶移至不同的 SOR，您必須更新與帳戶相關聯的稅務註冊號碼 (TRN)，並提供新的有效 TRN。您也可以刪除與帳戶相關聯的 TRN。您帳戶的新 SOR 會根據新稅務地址的國家/地區，以及您

目前的帳單地址，依可用性和優先順序自動解析。當帳戶的 SOR 變更時，您會收到通知，指出您的帳戶正移入或移出 AWS 印度。

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇管理設定檔，然後選擇計劃和帳單。
3. 選取您的帳戶，然後選擇管理稅務註冊，然後選擇編輯、全部編輯或刪除 TRN。
4. （如果您的預設付款方式是信用卡或簽帳金融卡）在主導覽窗格中，選擇管理設定檔，然後選擇計劃和帳單。
5. 選擇新增付款方式以重新輸入預設支付卡的詳細資訊，或新增新的支付卡。
6. 儲存卡片之後，請選擇設為預設。

預設付款偏好設定區段提醒您，您先前的預設付款方式不符合在新 SOR 中使用的資格。新增支付卡以讓此提醒消失後，請重新整理頁面。

存取 AWS 支援

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

當您註冊我們的新 AWS 體驗時，有兩個地方可以與 AWS Support 合作。

您可以存取基本支援或商業支援+。根據預設，您已註冊基本支援。您可以開始試用 Business Support+，免費使用長達六個月。

專案支援

如果您遇到專案、團隊管理或帳單相關問題，您可以在 AWS 設定中存取基本支援或商業支援+。您可以為您的組織請求其他專案，或請求提高與帳單相關的配額。

建立支援案例

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇支援。
3. 針對專案支援，選擇建立案例。
4. 針對主旨，輸入支援案例的主旨。

5. 針對描述，描述您的問題。如果可以，請描述重現問題的步驟。
6. 選擇建立案例。

建立支援案例之後，您可以檢視案例資訊，以繼續使用支援。

檢視您的案例資訊

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇支援。
3. 選擇您的支援案例。在此檢視中，您可以看到有關案例的所有通訊。
4. 若要傳送回覆至支援，請在回覆中輸入您的回覆，然後選擇傳送回覆。

當您的案例解決時，您可以解決它，將其從 AWS 設定中移除。

解決您的案例

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇支援。
3. 選擇 Resolve case (解決案例)。

解決後，您將無法存取案例詳細資訊。

Technical support (技術支援)

如果您的 AWS 資源有問題，您需要技術支援。若要存取技術支援，請在[AWS 支援中心](#)為有問題的專案開啟案例。

支援所有專案和組織是否關閉

如果您的所有專案和組織都已關閉，請填寫支援[意見回饋表單來聯絡支援](#)。

在請求資訊區段的 如何協助您，包括您使用我們新的 AWS 體驗，以及您所有的專案都已關閉。

開始商業支援 + 試用

您可以獲得長達六個月的免費 Business Support+。Business Support+ 於 2026 年 10 月 31 日前免費提供。自 2026 年 11 月 1 日起，標準定價開始，您會收到 174 USD 的 Business Support+ 點數，以

涵蓋每月 29 USD 的六個月。當免費期間結束且抵用金開始時，您會保持訂閱狀態，並在您的抵用金餘額不足時 AWS 通知您，再開始任何原價計費。

您的商業支援 + 費用為每月 29 美元或 AWS 您的花費百分比，以較高者為準。如需詳細資訊，請參閱[定價詳細資訊](#)。您的計劃會每月續約，直到您取消為止。

啟動您的 Business Support+ 試用

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇支援。
3. 選擇開始試用。這會影響組織中的所有專案。
4. 檢閱詞彙，選取協議核取方塊，然後選擇開始試用。

您可以隨時取消，無需承諾也不會受到懲罰。當您取消時，商業支援 + 存取會立即結束，而且任何未使用的點數都會遭到沒收。您可以隨時以標準定價重新註冊，但一旦取消，就無法恢復 Business Support+ 促銷優惠。

取消商業支援+

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇支援。
3. 選擇取消計劃。
4. 選取核取方塊以確認取消 Business Support+ 會立即將您返回基本支援，您將無法存取列出的利益，而且您的 174 美元抵用金將被移除且無法恢復。
5. 選擇取消計劃以返回基本支援。

使用 AWS CloudTrail 監控您的專案

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

使用 AWS CloudTrail 監控您的專案

您的專案已與 AWS CloudTrail 整合，CloudTrail 是一種服務，可提供團隊成員 AWS 或服務所採取動作的記錄。CloudTrail 會將專案的所有 API 呼叫擷取為事件。擷取的呼叫包括來自主控台的呼叫，以及所有支援服務的 API 操作 AWS。您可以使用 CloudTrail 所收集的資訊，判斷對您的專案提出的請求、提出請求的人員、提出請求的時間，以及其他詳細資訊。

使用 CloudTrail 查看誰修改了您的專案

本教學課程適用於熟悉的使用者 AWS CLI。如果您與多個團隊成員共用專案，您可以使用 CloudTrail 檢視誰修改了專案中的任何資源。您或團隊成員在使用 AWS 設定或 AWS 管理主控台存取您的專案時所採取的每個動作都會由 `onBehalfOf` 參數記錄。此參數會顯示使用者 ID 和身分存放區 ID。這些值共同定義您受邀存取專案的建置器 ID。

若要尋找 `onBehalfOf` 參數並將其連接到團隊成員，您需要存取 AWS CLI 和 AWS 管理主控台。如果您沒有 AWS CLI 設定，您可以使用 AWS CloudShell 存取瀏覽器型、預先驗證的 Shell，您可以直接從啟動 AWS 管理主控台並執行 AWS CLI 命令。

步驟 1. 尋找 AWS CloudTrail 事件

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/cloudtrail/> 開啟 CloudTrail 主控台。
2. 在導覽窗格中，選擇 Event history (事件歷史記錄)。您可以看到已篩選的事件清單，並最先顯示最近的事件。選擇事件。
3. 在事件記錄中，您會看到下列內容：

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

這是定義建立 CloudTrail 事件之團隊成員的身分。

步驟 2. 將 onBehalfOf 參數連線至團隊成員

若要使用 將 `onBehalfOf` 參數連線至團隊成員 AWS CLI：

在終端機 AWS CLI 中使用

1. 執行下列命令以登入 AWS CLI。您可以使用 [尋找您的 區域](#)[AWS 區域](#) [您的專案](#)。

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

2. 執行下列命令以取得身分存放區的 ID。CloudTrail 事件會顯示身分存放區 ARN，但不表示身分存放區 ID。在尋找身分存放區的 ID AWS 區域 us-east-1 時，一律使用。

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

輸出將如下所示：

```
{
  "Instances": [
    {
      "InstanceArn": "arn:aws:sso:::instance/ssoins-000000000000",
      "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
        }
      ]
    }
  ]
}
```

您想要複製身分存放區 ID。在此情況下，身分存放區 ID 為 d-000000。

3. 執行下列命令來描述對應至 onBehalfOf 參數的團隊成員。

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

輸出將如下所示：

```
{
  "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"
}
```

此輸出會提供團隊成員的顯示名稱和電子郵件。

若要使用 AWS CloudShell 將 `onBehalfOf` 參數連線至團隊成員，請登入 AWS 管理主控台 並存取 CloudShell。如需詳細資訊，請參閱 [AWS CloudShell 入門](#)。您將自動擁有存取 CloudShell 的正確 IAM 許可。

在 AWS 設定中關閉專案

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

如果您不再需要專案，可以將其關閉。關閉專案後，您可以在關閉專案後的 90 天內重新開啟專案。您關閉專案當天到 AWS 永久關閉專案的期間是關閉後期間。

關閉專案之前您需要知道什麼

關閉專案之前，請考慮下列事項：

- 如果專案因為超過支出限制而暫停，則無法關閉專案。您需要關閉支出限制，然後關閉專案。如需詳細資訊，請參閱[在 AWS 設定中更新支出限制](#)。
- 所有團隊成員將自動失去對此專案及其內部所有資源的存取權。
- 關閉您的專案將做為您終止此專案客戶 AWS 協議的通知。
- 您不需要在關閉專案之前刪除專案中的資源。不過，我們建議您備份任何要保留的資源或資料。如需如何備份特定資源的說明，請參閱該服務的適當 AWS 文件。
- 您可以在關閉後期間重新開啟專案。如果您重新開啟，仍保留在專案中的服務費用將會重新啟動。您仍需對任何未支付發票負責。
- 您仍需負責專案關閉前所使用服務的所有未結費用。您將在關閉專案後的下個月收到 AWS 帳單。例如，如果您在 1 月 15 日關閉帳戶，您將會在 2 月初收到 1 月 1 日至 1 月 15 日所產生用量的帳單。
- 專案關閉後，AWS 會每天傳送電子郵件最多五天，然後再暫停網域。網域暫停後，根據網域的註冊商，我們將在 30 天內刪除網域，或將網域釋出給其註冊商。如需詳細資訊，請參閱[我的 AWS 帳戶已關閉或永久關閉，且我的網域已向 Route 53 註冊](#)。此資訊是針對撰寫 AWS 帳戶，但資訊對於專案而言是準確的。
- AWS CloudTrail 是基礎安全服務。這表示即使專案關閉後，使用者建立的線索仍可繼續存在並交付事件，除非使用者在關閉前明確刪除其專案中的線索。如需有關如何在關閉 AWS 帳戶後請求刪除線索的詳細資訊，請參閱 CloudTrail 使用者指南中的[AWS 帳戶 關閉和線索](#)。此資訊是針對撰寫 AWS 帳戶，但專案的資訊是準確的。

關閉專案

關閉專案

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主導覽窗格中，選擇您要存取的專案。
3. 針對關閉專案，選擇關閉專案。
4. 確認您的選擇，然後選擇關閉專案。

專案頁面仍會顯示您的專案 90 天，直到永久刪除為止。

關閉後期間

關閉後期間是指您關閉帳戶當天到 AWS 永久關閉專案之間的時間長度。關閉後期間為 90 天。在關閉後期間，您只能透過重新開啟專案來存取內容 AWS 和服務。在關閉後期間之後，會 AWS 永久關閉您的專案，您無法再重新開啟。AWS 也會刪除您帳戶中的內容和資源 (CloudTrail 追蹤除外)。專案永久關閉後，其專案 ID 永遠無法重複使用。

重新開啟您的專案

您的專案將在 90 天內永久關閉，之後您將無法重新開啟專案，AWS 並將刪除您專案中剩餘的內容。若要在專案永久關閉之前重新開啟專案，(1) 您必須 [支援 盡快聯絡](#)，以及 (2) 我們必須在帳戶關閉之日起 60 天內收到任何未結餘額的完整付款，包括提供發票上指定的必要資訊。

Note

如果您重新開啟，仍保留在專案中的服務費用將會重新啟動。

啟用進階 AWS 功能

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

當您啟用進階功能時，您可以完全控制 AWS 組織、管理帳戶和委派管理員帳戶，這些帳戶用於管理您建立的專案和您邀請的團隊成員。您將直接管理環境 AWS 的安全、控管和團隊成員。您可以存取其他服務 AWS、多區域功能，以及增強的管理和帳單控制。

您必須先升級帳戶，才能啟用進階功能。如需詳細資訊，請參閱[在 AWS 設定中升級您的帳戶](#)。

啟用進階功能時會發生什麼情況

當您啟用進階功能時，下列變更會立即套用至您的管理帳戶和包含您專案 AWS 的組織：

- 您現在是包含專案之 AWS 組織的管理員。

- 您可以為您的管理帳戶設定根電子郵件地址。您也需要設定根使用者密碼。如需詳細資訊，請參閱[為您的管理帳戶設定根使用者密碼](#)。
- 您以組織中的成員帳戶來管理專案。身為此組織的管理員，您可以在組織中建立成員帳戶。您的 AWS 建置器 ID 會繼續擁有您的專案帳戶。如需詳細資訊，請參閱[啟用進階功能之後的專案帳戶](#)。
- 若要為邀請加入組織的成員帳戶提供管理員角色，您必須建立 OrganizationAccountAccessRole。如需詳細資訊，請參閱[在受邀成員帳戶中建立 OrganizationAccountAccessRole](#)。
- 您的團隊成員稱為人力身分，他們仍然可以存取 AWS 您的帳戶。您也可以選擇使用 IAM Identity Center 自訂人力的身分來源。您可以繼續使用 AWS Builder ID 做為身分來源，也可以將其變更為外部身分來源。如果您將身分來源從 AWS Builder ID 變更為另一個身分來源，則無法復原。您無法在未來重新啟用 AWS Builder ID 做為身分來源。如需詳細資訊，請參閱[從 AWS 建置器 ID 變更身分來源](#)。
- 您可以使用帳戶 AWS 存取管理員，控制 IAM Identity Center 組織執行個體中使用者和群組的存取。您可以使用此功能修改使用者存取，同時仍允許您的使用者使用登入aws login，以從瀏覽器接收其 IAM 角色工作階段憑證。如需詳細資訊，請參閱[AWS 帳戶存取管理員](#)。
- AWS 會在組織中使用委派管理員角色建立名為 Identity Delegated Admin 的成員帳戶。此角色用於在 IAM Identity Center 和帳戶存取管理員中執行大多數管理任務。委派管理員角色必須在美國東部（維吉尼亞北部）使用。如需詳細資訊，請參閱[委派的管理](#)。

您的 AWS 建置器 ID 擁有身分委派管理員帳戶，例如您的專案帳戶。

- 您現在可以設定資源控制政策 (RCPs) 和服務控制政策 (SCPs)，在您的組織中強制執行自訂護欄。先前是代表您 AWS 管理 RCPs SCPs。您可以在啟用進階功能後修改這些政策。如需詳細資訊，請參閱[移除組織政策](#)。

當您啟用進階功能時，下列變更也會套用至您的 AWS 組織：

- 如果您有任何 AWS 帳戶的支出限制，則會將其移除。目前暫停的任何專案都會重新啟用。如果您啟用進階功能，則無法建立支出限制。相反地，您可以存取整個帳單和成本管理工具套件。這包括設定預算、下載成本總管報告，以及使用 AWS 成本異常偵測來偵測異常支出。您可以使用這些進階工具來分析、組織、規劃和最佳化成本。
- 您可以存取所有 AWS 服務。可用的服務會列在 [the section called “AWS 服務 不支援我們的新 AWS 體驗”](#)。您應該規劃架構，並在啟用這些服務之前參閱服務文件。此外，Agent Toolkit 提供許多使用這些服務的[技能](#)。
- 您可以存取其他 AWS 區域選擇加入的區域，以及存取多區域功能。多區域架構可改善工作負載的彈性。我們建議您規劃如何限制和稽核您的區域足跡。請務必確保您建立的資源僅存在於您要使用的區域中。

- 您可以關閉 AWS 帳戶 組織中每個的 IAM 角色管理員。IAM 角色管理員是選用的帳戶設定，可自動佈建角色，因此您和您的員工不需要進行設定。如需詳細資訊，請參閱[如何啟用和停用角色管理員 \(主控台\)](#)。
- 您可以使用 [IAM Access Analyzer](#)。

當您啟用進階功能時，下列變更也會套用至您的使用者體驗：

- 先前，AWS 管理主控台 會顯示簡化的檢視，其中包含您用來在專案和存取 AWS 設定之間變更的選單。AWS 管理主控台 擴展以包含其他功能，例如區域選擇器、其他服務，以及為帳戶設定顏色，供您存取以明顯區分。如需詳細資訊，請參閱 [主控台功能](#)。
- 您現在可以執行下列動作：
 - 停用多工作階段主控台支援。
 - 將 AWS 您的帳戶指定為 HIPAA 或 SEC 合規。
 - 使用 AWS Marketplace。
 - 從 AWS 啟用獲得額外點數。
 - 使用 AWS 訓練合作夥伴。
 - 購買 AWS 技能建置器團隊訂閱。
 - 向 註冊 Enterprise 協議 AWS。
 - 建立 Professional Services 合約。
 - 加入 AWS 合作夥伴網路。

啟用進階功能之後的專案帳戶

您在 AWS 設定中建立的每個專案都包含 AWS 帳戶，稱為專案帳戶。AWS Builder ID 擁有每個專案帳戶，而不是根使用者電子郵件地址。當您啟用進階功能時，您的專案帳戶會成為組織中的成員帳戶，而您的 AWS 建置器 ID 會繼續擁有這些帳戶，即使您稍後變更身分來源。您的 AWS 建置器 ID 也擁有在啟用進階功能時 AWS 建立的 Identity Delegated Admin 帳戶。

由於專案帳戶沒有根使用者電子郵件地址，其運作方式與您組織中的其他成員帳戶不同：

- AWS Organizations 主控台為專案帳戶顯示的電子郵件地址是 AWS 產生的預留位置。DescribeAccount、ListAccounts、ListDelegatedAdministrators、ListAccountsForParent 和 GetPrimaryEmail 操作會傳回相同的預留位置。這不是您可以使用或變更的電子郵件地址。

- 您無法更新專案帳戶的根使用者電子郵件地址。呼叫專案帳戶 `StartPrimaryEmailUpdate` 或 `AcceptPrimaryEmailUpdate` 專案帳戶的 時發生錯誤，即使呼叫者具有必要的許可也 `AccessDeniedException` 一樣。
- 您無法以根使用者身分登入專案帳戶，也無法復原其根使用者密碼。
- 您無法從您的組織移除專案帳戶，也無法離開您的組織或加入其他組織。如果您 `RemoveAccountFromOrganization` 為專案帳戶呼叫，呼叫會失敗，並顯示帳戶由建置器 ID 所擁有的 `ConstraintViolationException` 錯誤。

若要停止使用專案帳戶，請從您的管理帳戶將其關閉。由於您無法從組織移除專案帳戶，因此只有在包括 Identity Delegated Admin 帳戶在內的所有專案帳戶都永久關閉後，才能刪除組織。在關閉後 90 天期間結束時，會 AWS 永久關閉帳戶。

您在啟用進階功能後在組織中建立的成員帳戶具有根使用者電子郵件地址，這些差異不適用於他們。如果您需要可以變更其根使用者電子郵件地址的帳戶，或稍後可以從組織中移除的帳戶，請建立新的成員帳戶，並將您的資源移至其中。

啟用進階功能後 AWS，設定會如何變更？

啟用進階功能後，只要您使用 AWS Builder ID 做為身分來源，即可 AWS 使用 AWS 設定。設定只能從 <https://settings.aws.com> 存取。您將無法從 存取它 AWS 管理主控台。AWS 設定將提供連結，以使用您的管理帳戶來管理您的帳戶。使用 管理帳戶，您可以從 AWS 設定存取下列 AWS 管理主控台位置。僅使用 管理帳戶來執行管理任務，包括：

- 存取帳單和成本管理主控台以檢視您的帳單資訊。
- 存取 AWS Organization 主控台來修改管理組織的 SCPs RCPs。
- 存取 AWS Account Access Manager 主控台，以修改人力資源身分的精細存取權。
- 存取 IAM Identity Center 以變更您的身分來源。

使用 管理帳戶來執行這些任務。雖然您也可以存取根使用者電子郵件和密碼，但我們建議您僅使用根使用者憑證來緊急存取您的帳戶。

您也可以使用 AWS 設定來存取組織中 AWS 的帳戶，以及與您共用的任何專案。

如果您想要建立自訂角色並從帳戶中 AWS 的設定存取它們，則必須將工作階段長度設定為 12 小時。

如果您擁有專案的團隊成員存取權，您可以像在啟用進階功能之前一樣檢視和存取專案。如果您為自己的管理帳戶和 AWS 組織啟用進階功能，則與您共用的任何專案都不會受到影響。

啟用進階功能後，我仍然可以在 AWS 設定中建立專案嗎？

啟用進階功能後，您無法在目前的 AWS Organization 中建立專案。您必須在組織中建立成員帳戶。

您可以使用預先設定的預設值建立新的受管 AWS 組織。若要這樣做，請在 AWS 設定中建立新的專案。然後，您可以建立其他專案並邀請團隊成員協作。您也可以為此管理帳戶啟用進階功能。

您存取的新預先設定環境將不會連線到您第一次註冊時建立的先前 AWS 組織 AWS。

如何準備啟用進階功能

我們建議您在啟用進階功能之前執行下列動作：

- 通知所有團隊成員您將啟用進階功能。除非您修改任何設定，否則您的團隊成員將擁有對專案的相同存取權，但 AWS 管理主控台 從簡化檢視變更為顯示區域並提供對更多服務的存取權的檢視。如果您稍後變更身分來源或新增 SCPs 或 RCPs，請通知您的人力資源，因為這些變更可能會影響他們登入的方式以及他們可以存取的內容。
- 檢視所有目前專案的支出，並記下是否有任何專案包含大幅波動的成本。如果沒有支出限制，您將負責資源產生的所有成本。建議您先刪除或暫停閒置資源，再啟用進階功能。
- 規劃您將對 AWS 組織進行哪些變更，並研究最佳實務。如果您打算在不同 中建立資源 AWS 區域，請修改套用供所有使用者限制的服務控制政策 AWS 區域。您需要修改的 statementID，RegionFloor 才能包含任何新的區域。如需詳細資訊，請參閱[專案的服務控制政策](#)。
- 如果您遵循 中的步驟[連接 AI 編碼工具](#)，您的 AI 工具只有新 AWS 體驗的相關內容。當您使用進階功能進行開發時，這可能會導致問題。我們建議下列作法：
 - 從您儲存檔案的位置移除aws-starter-rules.md檔案。規則檔案已根據您的代理程式儲存。如需詳細資訊，請參閱[放置規則檔案的位置](#)。

如何啟用進階功能

您可以在 AWS 設定中啟用進階功能。無法反轉啟用。

啟用進階功能

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇專案。
3. 針對動作，選擇探索進階功能。

由於無法反轉啟用，我們將提供更多時間來探索和了解啟用程序。

4. 當您準備好啟用時，請執行下列動作：

- a. 針對團隊名稱，輸入團隊名稱。這是用來存放您人力資源身分的 IAM Identity Center 執行個體名稱。您的人力會看到此名稱。
- b. 針對選擇管理帳戶電子郵件地址，選擇電子郵件地址。此電子郵件地址用於存取管理帳戶和執行任務。如果您使用不同的電子郵件地址，AWS 只要您仍然使用建置器 ID 做為身分來源，AWS 建置器 ID 電子郵件仍可從 AWS 設定存取管理帳戶。
- c. 完成管理帳戶電子郵件地址的驗證程序。
- d. 選擇檢閱並完成啟用。
- e. 確認您的選擇，然後選擇啟用。如果您這樣做，則無法還原您的帳戶。

恭喜，您已啟用進階 AWS 功能！

啟用進階功能之後

啟用進階功能之後，您可以執行下列動作：

- [管理人力資源成員](#)
- [從 AWS 建置器 ID 變更身分來源](#)
- [移除組織政策](#)
- [建立組織單位](#)
- [AWS 區域 在您的帳戶中啟用或停用](#)
- [建立 IAM 角色](#)

為您的管理帳戶設定根使用者密碼

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

啟用進階功能之後，您的管理帳戶現在會使用根電子郵件地址進行帳戶復原。雖然您仍然可以使用自助式選項來復原對 AWS Builder ID 的存取權，但您現在可以使用根使用者憑證來復原對管理帳戶的存取權。<https://docs.aws.amazon.com/signin/latest/userguide/recover-builder-id.html>若要存取根使用者，您需要建立根使用者密碼。此外，我們建議您開啟多重要素驗證 (MFA)，以增強根使用者的安全性。

設定根使用者密碼

1. 開啟 [AWS 管理主控台](#)，然後選擇使用根使用者電子郵件登入。
2. 對於電子郵件地址，輸入根使用者電子郵件地址。

這是您在啟用進階功能時為管理帳戶設定的電子郵件地址。

3. 選擇 **Forgot your password?** (忘記您的密碼?)。

密碼重設程序也是您在啟用進階功能後設定根使用者密碼的方式。

4. 輸入與帳戶相關聯的電子郵件地址。
5. 提供 CAPTCHA 文字並選擇我不是機器人。
6. 檢查與您的相關聯的電子郵件 AWS 帳戶 是否有來自 Amazon Web Services 的訊息。電子郵件來自於結尾為 `@verify.signin.aws` 的地址。依照電子郵件中的指示設定根使用者密碼。若您在帳戶中沒有看到電子郵件，請檢查您的垃圾郵件資料夾。如果您不再能夠存取電子郵件，請參閱 AWS 登入使用者指南中的 [我無法存取我 AWS 帳戶的電子郵件](#)。

設定根使用者密碼後，您可以復原對帳戶的存取。接下來，請遵循[帳戶根使用者多重要素驗證 AWS](#)中的指引，以開啟根憑證的 MFA。

僅使用根使用者來復原您的帳戶，或在必要時執行[需要根使用者憑證的任務](#)。對於日常工作，請使用您的身分來源登入，例如 AWS 建置器 ID。

管理人力資源成員

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

啟用進階功能後，您可以邀請新的人力資源成員或移除現有的人力資源成員。這包括將現有的人力資源新增至新 AWS 帳戶。以下資訊僅適用於使用 AWS Builder ID 做為身分來源 AWS 的組織。如果您使用外部身分提供者 (IdP)，您可以在這些身分提供者中管理您的人力資源。如果您使用 Identity Center 目錄，請使用 [Identity Center 目錄中管理使用者](#)中所述的文件。

邀請新的人力資源成員

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇專案。

3. 請造訪 AWS 主控台以取得您的身分委派管理員帳戶。
4. 在 AWS 主控台首頁中，搜尋 **IAM Identity Center** 並選擇它。
5. 在 IAM Identity Center 主控台的使用者頁面上，選擇邀請新的團隊成員。
6. 在電子郵件中，輸入電子郵件地址或電子郵件地址清單。以逗號 (,) 或分號 (;) 分隔電子郵件地址。
7. 選擇傳送邀請。

授予新的人力資源成員存取 AWS 帳戶的權限

人力資源成員接受邀請後，您可以設定他們有權存取 AWS 的帳戶。

為您在啟用進階功能之前建立的帳戶授予完整許可

1. 識別您要授予存取權之帳戶的帳戶 ID。若要尋找帳戶 ID，請參閱[檢視 AWS 帳戶識別符](#)。
2. 在主導覽窗格中，選擇群組。
3. 選取以您識別的帳戶 ID 開頭的群組名稱。
4. 選擇新增使用者至群組。
5. 選取您要新增的使用者。
6. 選擇新增 1 個使用者。

將自訂許可授予新的或現有的 AWS 帳戶

您可以在 AWS Account Access Manager 中設定自訂存取。如需詳細資訊，請參閱[管理 AWS 帳戶的存取權](#)。

Note

如果您想要建立自訂角色並從 AWS 設定授予存取權，則必須將工作階段長度設定為 12 小時。

移除人力成員

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇專案。
3. 針對動作，選擇管理團隊。

這會開啟 IAM Identity Center。

4. 在 IAM Identity Center 主控台的使用者頁面上，選取團隊成員，然後選擇移除。
5. 確認您的選擇，然後選擇移除。

團隊成員將立即失去組織的所有存取權 AWS。

這些步驟會示範如何透過先存取 AWS 設定來管理人力資源成員。不過，您可以使用 AWS 管理主控台委派管理員帳戶登入，並存取 IAM Identity Center 或 IAM 主控台來管理您的人力資源成員。

從 AWS 建置器 ID 變更身分來源

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

啟用進階功能之後，您可以從 Builder ID 變更身分來源 AWS。如果您從 AWS Builder ID 變更身分來源，則永遠不能重複使用 AWS Builder ID 作為 AWS 組織的身分來源。變更您的身分來源會變更您的人力資源登入的方式。您的 AWS 建置器 ID 會繼續擁有您的專案帳戶。

從 AWS Builder ID 變更您的身分來源

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇專案。
3. 在管理此組織中，選擇變更身分來源。

這會開啟 IAM Identity Center。

4. 在 IAM Identity Center 主控台的設定頁面上，選擇動作，然後選擇變更身分來源。
5. 針對選擇身分來源，將會選取 AWS Builder ID。選擇新的來源，然後選擇下一步。
6. 如果您要變更為 Active Directory，請從下一頁的選單中選擇可用的目錄。如果您要切換至外部身分提供者，建議您遵循[如何連線至外部身分提供者](#)中的步驟。
7. 檢閱並確認您的變更。您需要選取所有核取方塊，以確認您了解組織的變更。
8. 確認您的選擇，然後選擇變更身分來源。

這些步驟會示範如何先存取 AWS 設定來變更您的身分來源。不過，您可以使用 AWS 管理主控台委派管理員帳戶登入，並存取 IAM Identity Center 以變更您的身分來源。

移除組織政策

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

啟用進階功能之後，您可以修改資源控制政策 (RCPs) 和服務控制政策 (SCPs)，以變更 AWS 組織的控管。當您啟用進階功能時，會移除某些 AWS 受管組織政策。如需詳細資訊，請參閱[組織的受管政策](#)。以下資訊僅適用於 AWS 使用 AWS Builder ID 做為身分來源的組織。如果您使用其他來源，請遵循[更新政策](#)中的步驟。

修改服務控制政策 (SCP)

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇專案。
3. 在管理此組織中，選擇管理政策。

這會開啟 AWS Organizations 主控台。

4. 選擇服務控制政策頁面。
5. 選擇您要更新的政策名稱。
6. 在政策的詳細資訊頁面上，選擇 Edit policy (編輯政策)。
7. 進行下列任一或所有變更：
 - 您可以在 Policy name (政策名稱) 中輸入新名稱，來重新命名政策。
 - 您可以在 Policy description (政策描述) 輸入新文字，來變更描述。
 - 您可以在左側窗格中以 JSON 格式編輯政策，來編輯政策文字。或者，您可以在右側的編輯器中選擇陳述式，同時使用控制項來變更其元素。如需每個控制項的詳細資訊，請參閱本主題稍早介紹的建立 SCP 程序。
8. 完成時，請選擇儲存變更。

修改資源控制政策 (RCP)

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇專案。
3. 在管理此組織中，選擇管理政策。

這會開啟 AWS Organizations 主控台。

4. 選擇資源控制政策頁面。
5. 選擇您要更新的政策名稱。
6. 在政策的詳細資訊頁面上，選擇 Edit policy (編輯政策)。
7. 進行下列任一或所有變更：
 - 您可以在 Policy name (政策名稱) 中輸入新名稱，來重新命名政策。
 - 您可以在 Policy description (政策描述) 輸入新文字，來變更描述。
 - 您可以在左側窗格中以 JSON 格式編輯政策，來編輯政策文字。或者，您可以在右側的編輯器中選擇陳述式，同時使用控制項來變更其元素。如需每個控制項的詳細資訊，請參閱本主題稍早的建立 RCP 程序。
8. 完成時，請選擇儲存變更。

這些步驟說明如何透過 AWS 設定修改組織政策。不過，您可以使用 AWS 管理主控台 您的管理帳戶登入，AWS Organizations 並存取 主控台來修改這些政策。

在 AWS 設定中關閉您的帳戶

Warning

我們目前正在向有限數量的客戶發佈新體驗。您可能還無法存取此體驗。

如果您不再需要組織和其中存放的所有專案，您可以關閉您的專案、關閉您的管理帳戶，並刪除您的 AWS 建置器 ID。

為了確保您不再需要支付任何使用 AWS 資源的費用，您必須關閉專案並關閉組織的管理帳戶，但不必關閉 AWS 設定檔。與之相關聯的 AWS 建置器 ID 是免費的。

關閉管理帳戶後，您可以在關閉管理帳戶的 90 天內重新開啟管理帳戶。您關閉管理帳戶當天到 AWS 永久關閉管理帳戶之間的時間是關閉後期間。

關閉管理帳戶之前需要知道什麼

在關閉您的管理帳戶之前，您應該考慮下列事項：

- 當您關閉專案時，請考慮 中的考量事項 [關閉專案之前您需要知道什麼](#)。

- 您必須先關閉所有專案，才能關閉管理帳戶。
- 您必須先關閉管理帳戶，才能刪除 AWS Builder ID。
- 關閉管理帳戶後，您可以在關閉管理帳戶的 90 天內重新開啟管理帳戶。您關閉管理帳戶當天到永久關閉管理帳戶之間的 AWS 時間是關閉後期間。
- 您可以在關閉後期間重新開啟您的帳戶。
- 您無法使用與關閉時向組織註冊的相同電子郵件地址，做為另一個組織的主要電子郵件。如果您想要在使用註冊 AWS（新）時為不同的組織使用相同的電子郵件地址，建議您在關閉之前更新。如需詳細資訊，請參閱[在 AWS 設定中變更您的電子郵件地址](#)。
- 如果您已在管理帳戶上啟用多重要素驗證 (MFA) 並設定 MFA 裝置，則當您關閉管理帳戶時，不會自動移除 MFA。如果您選擇在關閉後 90 天內開啟 MFA，請保持 MFA 裝置處於作用中狀態，直到關閉後期間過期為止，以防您需要在此期間存取帳戶。請注意，在永久關閉您的帳戶之後，硬體 TOTP 字符裝置無法與其他使用者建立關聯。如果稍後想要將硬體 TOTP 字符用於其他使用者，您可以選擇在關閉管理帳戶之前停用硬體 MFA 裝置。

關閉專案

若要關閉您的專案，請參閱 [在 AWS 設定中關閉專案](#)。

關閉您的管理帳戶

關閉您的管理帳戶

1. 在 <https://settings.aws.com> 開啟 AWS 設定。
2. 在主要導覽窗格中，選擇專案。
3. 針對動作，選擇關閉管理帳戶。
4. 確認您的選擇，然後選擇關閉管理帳戶。

刪除您的 AWS 建置器 ID

刪除您的 AWS 建置器 ID 將導致下列情況：

- 無法存取：除了您的專案和組織之外，您無法再存取先前透過 AWS Builder ID 存取的任何 AWS 工具和服務。
- 刪除內容：將刪除僅與您的 AWS 建置器 ID 相關聯的任何剩餘內容，您將無法再使用 AWS 建置器 ID 從應用程式存取或復原內容。

- 個人資訊刪除：您在建立和管理 AWS 建置器 ID 時提供的任何個人資訊都會遭到刪除，但 AWS 可能會依法律要求或允許保留個人資訊，例如您刪除請求的記錄，或以無法識別您身分的形式保留資料。

您可以在 AWS 隱私權通知中進一步了解我們如何處理您的資訊。您可以前往 AWS AWS 通訊偏好設定中心，更新您的通訊偏好設定或取消訂閱。

現有的登入保持不變 – 如果您使用 Google 或 Apple 等登入，刪除您的 AWS 建置器 ID 不會刪除任何與您的登入帳戶相關的內容。

刪除您的 AWS 建置器 ID

1. 在 <https://settings.aws.com> 開啟 AWS 設定。

即使您已刪除管理帳戶，您仍然可以登入。

2. 在主導覽窗格中，選擇管理設定檔。
3. 針對設定檔資訊，選擇管理設定檔。

系統會將您重新導向至 AWS 您的建置器 ID 設定檔。

4. 在主要導覽窗格中，選擇隱私權與資料。
5. 針對刪除 AWS 建置器 ID，選擇刪除您的 AWS 建置器 ID。
6. 確認您的選項後，再選擇刪除。

註冊 AWS（進階）

如果您是初次使用 AWS，第一步是註冊 AWS 帳戶。當您遵循註冊 AWS（進階）的資訊時，會 AWS 建立一個帳戶，您可以在其中完全控制帳戶組態，以及儲存內容的位置。如果您有受管制的工作負載，例如 HIPAA、FedRAMP，請使用此選項。

若要將此註冊與註冊 AWS（新）進行比較，請參閱 [比較註冊選項](#)。

若要註冊 AWS 帳戶，您需要提供下列資訊：

- 根使用者電子郵件地址 – 電子郵件地址用作[根使用者的](#)登入名稱，是帳戶復原的必要項目。您必須能夠接收傳送到此地址的電子郵件訊息。您必須先驗證您有權存取傳送到此地址的電子郵件，才能執行特定任務。
- AWS 帳戶名稱 – 帳戶名稱會出現在數個位置，例如發票上，以及帳單與成本管理儀表板和 AWS Organizations 主控台等主控台中。我們建議您使用標準方法來命名您的帳戶，以便提供易於辨識的帳戶名稱。對於公司帳戶，請考慮使用命名標準，例如 organization-purpose-environment（例如 AnyCompany-audit-prod）。對於個人帳戶，請考慮使用命名標準，例如 first name-last name-purpose（例如 paulo-santos-testaccount）。
- 地址 – 如果您的聯絡地址和帳單地址位於印度，您帳戶的使用者協議是與印度當地 AWS 賣方 Amazon Web Services India Private Limited (AWS India) 簽訂的。在驗證過程中您必須提供您的 CVV。視您的銀行而定，您可能也必須輸入一次性密碼。AWS 做為驗證程序的一部分，印度會向您的付款方式收取 2 盧比的費用。AWS 驗證完成後，印度會退還 2 盧比。
- 電話號碼 – 此號碼用於身分驗證目的，並確認帳戶的所有權。您必須能夠使用此電話號碼接收通話和簡訊。

Important

如果此帳戶是針對企業，請使用公司電話號碼，讓您的公司即使員工變更職位或離開公司 AWS 帳戶，也可以保留對的存取權。

步驟 1：建立您的帳戶

這些指示適用於在印度 AWS 帳戶 外部建立。如需在印度建立帳戶，請參閱 [AWS 帳戶 使用 AWS 印度建立](#)。如需建立屬於管理組織一部分的帳戶 AWS Organizations，請參閱 AWS Organizations 《使用者指南》中的[在組織中建立成員帳戶](#)。

AWS 管理主控台

建立 AWS 帳戶

1. 開啟[註冊頁面 AWS](#)。
2. 輸入根使用者電子郵件地址和 AWS 帳戶 名稱，然後選擇驗證電子郵件地址。這會將驗證碼傳送至您的電子郵件地址。

Important

如果此帳戶是針對企業，請使用安全的公司分發清單（例如 `it.admins@example.com`），讓您的公司即使員工變更職位或離開公司 AWS 帳戶，也可以保留對 的存取權。由於電子郵件地址可用來重設帳戶的根使用者登入資料，因此請保護此分發清單或地址的存取權。

3. 輸入您的驗證碼，然後選擇驗證。
4. 為您的根使用者輸入高強度密碼，進行確認，然後選擇繼續。AWS 需要您的密碼符合下列條件：
 - 它必須至少有 8 個字元，最多 128 個字元。
 - 它至少混用 3 種下列類型字元：大寫、小寫、數字和 `!@#$%^&*()<>[]{}|_+~=` 符號。
 - 它不能與 AWS 帳戶 您的姓名或電子郵件地址相同。
5. 選擇您的帳戶計劃。如需詳細資訊，請參閱 [免費方案](#)。
6. 輸入您的聯絡資訊，然後閱讀並接受[AWS 客戶協議](#)。請務必先了解條款，再接受。

Important

如果此帳戶是針對企業，最佳實務是輸入公司電話號碼，而不是個人電話的號碼。使用個別電子郵件地址或個人電話號碼設定帳戶的根使用者可能會使您的帳戶變得不安全。

7. 輸入您的帳單資訊。如果您想要為帳單資訊使用不同的 AWS 帳單地址，請選擇使用新的地址。

您必須先新增有效的付款方式，才能繼續註冊程序。

8. 您可能需要確認您的身分：
 - a. 針對國家/地區或區域代碼，輸入可在幾分鐘內撥打的電話號碼。

- b. 針對電話號碼，輸入可在幾分鐘內撥打的電話號碼。
 - c. 選擇傳送簡訊。
 - d. 當自動化系統與您聯絡時，輸入您收到的代碼，然後選擇繼續。
9. 選擇其中一個可用的 AWS 支援計劃。如需可用支援計劃及其優點的描述，請參閱[比較 支援計劃](#)。
10. 選擇完成註冊。出現確認頁面，指出您的帳戶正在啟用。
11. 檢查您的電子郵件和垃圾郵件資料夾是否有電子郵件訊息，確認您的帳戶已啟用。啟用通常需要幾分鐘的時間，但有時可能需要長達 24 小時。
12. 收到啟用訊息後，您可以登入 [AWS 管理主控台](#) 以開始使用 AWS 服務。如需如何管理帳戶設定的一般資訊，請參閱 [設定您的 AWS 帳戶](#)。

對於透過 AWS 帳戶 管理的多個 AWS Organizations，請將管理存取權指派給 IAM Identity Center 中的管理使用者。如需說明，請參閱《[IAM Identity Center 使用者指南](#)》中的設定 [IAM Identity Center 管理使用者的 AWS 帳戶 存取權](#)。

AWS CLI & SDKs

您可以在由 AWS Organizations 管理的組織中建立成員帳戶，方法是在登入組織的管理帳戶時執行 [CreateAccount](#) 操作。

您無法使用 AWS Command Line Interface (AWS CLI) 或 AWS API 操作在組織 AWS 帳戶 外部建立獨立。

步驟 2：（建議）安裝 AWS CLI

AWS CLI 按照安裝 中的指示[安裝 AWS CLI](#)。您需要 2.32.0 版或更新版本。

您可以使用 AWS CLI 讓代理程式代表您管理 AWS 資源。

安裝 之後 AWS CLI，請使用下列命令以程式設計方式登入：

```
aws login
```

這會每 15 分鐘自動輪換您的登入資料，讓您的工作階段有效長達 12 小時，無需手動介入。

使用下列命令來驗證您的登入資料是否正常運作：

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

如需存取 的詳細資訊 AWS 帳戶，請參閱 [存取您的 AWS 帳戶](#)。

步驟 3：（建議）設定 AWS MCP 伺服器

AWS MCP 伺服器是受管伺服器，可讓客服人員 AWS 透過模型內容通訊協定 (MCP) 存取。客服人員可以搜尋 AWS 文件並擷取服務資訊，無需身分驗證。若要執行 AWS API 呼叫、在沙盒環境中執行 Python 指令碼，或遵循精心策劃的技能，客服人員會透過您現有的 IAM 登入資料進行驗證。如需詳細資訊，請參閱[什麼是 AWS 客服人員工具組？](#)

完成註冊程序後，請參閱下列主題：

- [相關 AWS 服務](#)
- [使用 AWS 帳戶根使用者](#)
- [存取您的 AWS 帳戶](#)
- [規劃您的 AWS 帳戶 控管結構](#)
- [設定您的 AWS 帳戶](#)
- [故障診斷您的 AWS 帳戶](#)
- [管理印度的帳戶](#)
- [關閉 AWS 帳戶](#)
- [重新開啟 AWS 帳戶](#)

相關 AWS 服務

視您註冊的方式而定 AWS，您可以存取 AWS 帳戶 或 專案。專案包含與其他協作者共用的 AWS 帳戶 和 設定。如需詳細資訊，請參閱[比較註冊選項](#)。在本節中，我們會說明如何使用註冊 AWS（進階）建立 AWS 帳戶 與下列服務無縫搭配運作：

- IAM

您的 AWS 帳戶 與 AWS Identity and Access Management (IAM) 緊密整合。您可以將 IAM 與您的帳戶搭配使用，以確保在帳戶中工作的其他人員擁有完成其任務所需的足夠存取權。您也可以使用 IAM 來控制對所有 AWS 資源的存取，而不只是帳戶特定資訊。在設定 的結構之前，請務必先熟悉 IAM 的主要概念和最佳實務 AWS 帳戶。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 中的安全性最佳實務](#)。

- AWS Organizations

如果您的公司規模較大或可能成長，您可能想要設定多個 AWS 反映公司特定結構的帳戶。AWS Organizations 為您提供基礎基礎設施和功能，以建置和管理多帳戶環境。您可以將現有帳戶合併為可讓您集中管理帳戶的組織。您可以建立自動成為您組織一部分的帳戶，也可以邀請其他帳戶加入您的組織。您也可以連接會影響您的部分或所有帳戶的政策。如需詳細資訊，請參閱[使用時機 AWS Organizations](#)。

下列與帳戶相關的 API 動作是 AWS Organizations API 的一部分，而非 AWS Account Management API。我們在此處包含它們，因為客戶通常會在帳戶管理文件中尋找這些操作，但它們是在 AWS Organizations 命名空間中定義。

- [CreateAccount](#)
- [CreateGovCloudAccount](#)
- [DescribeAccount](#)
- AWS Control Tower

AWS Control Tower 提供一種簡化的方式來設定和管理安全的多帳戶 AWS 環境。會使用 AWS Control Tower 自動建立您的多帳戶環境 AWS Organizations，執行個體化一組初始帳戶，並使用環境的一些預設護欄和組態。您可以使用在幾個步驟 AWS 帳戶中 AWS Control Tower 佈建新的，同時確保帳戶符合您的組織政策。如需詳細資訊，請參閱[使用時機 AWS Control Tower](#)。

使用 AWS 帳戶根使用者

視您註冊的方式而定 AWS，您可以存取 AWS 帳戶或專案。專案包含與其他協作者共用的 AWS 帳戶和設定。如需詳細資訊，請參閱[比較註冊選項](#)。在本節中，我們會說明如何在您使用註冊 AWS（進階）建立 AWS 帳戶的中使用根使用者。AWS Builder ID 擁有每個專案帳戶，而不是根使用者電子郵件地址，因此您無法在專案帳戶中使用根使用者，包括在啟用進階功能之後。

當您建立時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務和資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的[需要根使用者憑證的任務](#)。

若要避免將根使用者用於日常任務，請了解如何在[中設定管理使用者 AWS IAM Identity Center](#)。如需更多根使用者安全建議，請參閱[適用於 AWS 帳戶的根使用者最佳實務](#)。

 Important

擁有您 根使用者登入資料的任何人 AWS 帳戶 都可以不受限制地存取您帳戶中的所有資源，包括帳單資訊。

您可以變更或重設根使用者密碼，並建立或刪除根使用者的存取金鑰（存取金鑰 IDs 和私密存取金鑰）。如需使用根使用者登入的說明，請參閱 [登入使用者指南中的以根使用者 AWS 管理主控台身分登入](#)。AWS

存取您的 AWS 帳戶

如果您 AWS 使用註冊 AWS（進階）AWS 帳戶 或啟用帳戶的進階功能，此資訊就是存取。若要比較註冊選項，請參閱 [比較註冊選項](#)。

您可以透過下列 AWS 帳戶 任何方式存取您的：

AWS 管理主控台

[AWS 管理主控台](#) 是以瀏覽器為基礎的界面，可用來管理 AWS 帳戶 設定和資源 AWS。

AWS 命令列工具

使用 AWS 命令列工具，您可以在系統的命令列發出命令，以執行 AWS 帳戶 和 AWS 任務。使用命令列比使用主控台更快、更方便。如果您想要建置執行 AWS 任務的指令碼，命令列工具也很有用。AWS 提供兩組命令列工具：

- [AWS Command Line Interface](#) (AWS CLI)。如需安裝和使用的詳細資訊 AWS CLI，請參閱 [AWS Command Line Interface 使用者指南](#)。
- [AWS Tools for Windows PowerShell](#)。如需安裝和使用 Tools for Windows PowerShell 的詳細資訊，請參閱 [AWS Tools for PowerShell 使用者指南](#)。

AWS SDKs

AWS SDKs 包含適用於各種程式設計語言和平台（例如 Java、Python、Ruby、.NET、iOS 和 Android）的程式庫和範本程式碼。SDK 會負責的工作諸如以密碼演算法簽署請求、管理錯誤以及自動重試請求。如需 AWS SDKs 的詳細資訊，包括如何下載和安裝，請參閱 [適用於 Amazon Web Services 的工具](#)。

AWS 帳戶管理 HTTPS 查詢 API

AWS 帳戶管理 HTTPS 查詢 API 可讓您以程式設計方式存取 AWS 帳戶 和 AWS。HTTPS 查詢 API 可讓您直接向該服務發出 HTTPS 請求。當您使用 HTTPS API 時，必須包含使用您的登入資料來數位簽署請求的程式碼。如需詳細資訊，請參閱[透過提出 HTTP 查詢請求呼叫 API](#)。

規劃您的 AWS 帳戶 控管結構

此資訊是關於如果您 AWS 使用註冊 AWS（進階）註冊，或如果您為帳戶啟用進階功能，規劃您的 AWS 帳戶 控管結構。若要比較註冊選項，請參閱[比較註冊選項](#)。

雖然您可能已使用單一帳戶開始 AWS 旅程，但 AWS 建議您隨著工作負載的大小和複雜性增加而設定多個帳戶。無論您是中型企業還是大型企業，您都需要建立控管結構計劃，以確保您的資料和工作負載需求得到滿足。

本節涵蓋 中可用的優點和控管服務 AWS，以協助啟用多帳戶控管結構。

主題

- [使用多個 的優點 AWS 帳戶](#)
- [使用時機 AWS Organizations](#)
- [使用時機 AWS Control Tower](#)
- [了解 API 操作模式](#)

使用多個 的優點 AWS 帳戶

如果您使用註冊 AWS（進階）AWS 帳戶 或啟用帳戶的進階功能，此資訊是關於 AWS 使用多個 的好處。若要比較註冊選項，請參閱[比較註冊選項](#)。

AWS 帳戶 在 中形成基礎安全界限 AWS 雲端。它們可作為資源的容器，提供關鍵的隔離層，對於建立安全、妥善管理的環境至關重要。如需詳細資訊，請參閱[什麼是 AWS 帳戶？](#)。

將您的資源分成不同的 AWS 帳戶，可協助您在雲端環境中支援下列原則：

- 安全控制 – 不同的應用程式可以有不同的安全設定檔，需要不同的控制政策和機制。例如，與稽核人員交談會更輕鬆，而且能夠指向單一 AWS 帳戶，以託管受[支付卡產業 \(PCI\) 安全標準](#)規範之工作負載的所有元素。

- 隔離 – AWS 帳戶 是安全保護的單位。應將潛在風險和安全威脅包含在 中，AWS 帳戶 而不會影響其他人。由於不同的團隊或不同的安全性設定檔，可能會有不同的安全性需求。
- 許多團隊 – 不同的團隊有不同的責任和資源需求。您可以將團隊移至不同的位置，以防止團隊互相干擾 AWS 帳戶。
- 資料隔離 – 除了隔離團隊之外，將資料存放區隔離到 帳戶也很重要。這有助於限制可存取和管理該資料存放區的人數。這有助於抑制對高度私有資料的暴露，因此有助於遵守 [歐盟一般資料保護法規 \(GDPR\)](#)。
- 業務流程 – 不同的業務單位或產品可能有完全不同的目的和流程。使用多個 AWS 帳戶，您可以支援業務單位的特定需求。
- 帳單 – 帳戶是在帳單層級分隔項目的唯一真實方式。多個帳戶可協助跨業務單位、職能團隊或個別使用者在帳單層級區隔項目。您仍可將所有帳單合併到單一付款人（使用 AWS Organizations 和 合併帳單），同時將明細項目分開 AWS 帳戶。
- 配額分配 – AWS 服務配額會針對每個配額分別強制執行 AWS 帳戶。將工作負載分成不同的 AWS 帳戶，可防止它們互相消耗配額。

本文件中所述的所有建議和程序都符合 [AWS Well-Architected Framework](#)。此架構旨在協助您設計靈活、有彈性且可擴展的雲端基礎設施。即使您開始很小，仍建議您繼續遵循架構中的本指南。這樣做可協助您安全地擴展環境，而不會在您成長時影響持續的操作。

管理多個 AWS 帳戶

在您開始新增多個帳戶之前，您會想要制定計劃來管理這些帳戶。為此，我們建議您使用 [AWS Organizations](#)，這是免費 AWS 服務，用於管理組織中的所有 AWS 帳戶。

AWS 也提供 AWS Control Tower，可將多層 AWS 受管自動化新增至 Organizations，並自動將其與其他 AWS 服務整合 AWS CloudTrail AWS Config，例如 AWS Service Catalog Amazon CloudWatch 等。這些服務可能會產生額外費用。如需詳細資訊，請參閱 [AWS Control Tower 定價](#)。

另請參閱

- [使用時機 AWS Organizations](#)
- [使用時機 AWS Control Tower](#)

使用時機 AWS Organizations

此資訊是關於您 AWS Organizations 何時使用註冊 AWS（進階）註冊 AWS，或是否已啟用帳戶的進階功能。若要比較註冊選項，請參閱 [比較註冊選項](#)。

AWS Organizations 是一項 AWS 服務，可讓您以群組 AWS 帳戶 身分管理。這提供合併帳單等功能，其中您帳戶的所有帳單都會分組在一起，並由單一付款人處理。您也可以使用以政策為基礎的控制項，集中管理組織的安全性。如需的詳細資訊 AWS Organizations，請參閱[AWS Organizations 《使用者指南》](#)。

受信任的存取權

當您使用 AWS Organizations 以群組形式管理帳戶時，組織的大多數管理任務只能由組織的管理帳戶執行。根據預設，這只包含與管理組織本身相關的操作。您可以透過啟用 Organizations 與該 AWS 服務之間的受信任存取，將此額外功能擴展到其他服務。受信任存取會授予指定 AWS 服務的許可，以存取組織及其包含的帳戶的相關資訊。當您啟用 Account Management 的受信任存取時，帳戶管理服務會授予 Organizations 及其管理帳戶存取所有組織成員帳戶的中繼資料的許可，例如主要或替代聯絡資訊。

如需詳細資訊，請參閱[啟用 AWS 帳戶管理的受信任存取](#)。

委派管理員

啟用受信任存取後，您也可以選擇將其中一個成員帳戶指定為 AWS 帳戶管理的委派管理員帳戶。這可讓委派的管理員帳戶為您組織中的成員帳戶執行先前只有管理帳戶可以執行的相同帳戶管理中繼資料管理任務。委派的管理員帳戶只能存取帳戶管理服務的管理任務。委派的管理員帳戶沒有管理帳戶對組織的所有管理存取權。

如需詳細資訊，請參閱[啟用 AWS 帳戶管理的委派管理員帳戶](#)。

服務控制政策

當您 AWS 帳戶 是 管理的組織的一部分時 AWS Organizations，組織的管理員可以套用[服務控制政策 \(SCPs\)](#)，以限制成員帳戶中的主體可以執行的操作。SCP 永遠不會授予許可；而是會限制成員帳戶可以使用哪些許可的篩選條件。成員帳戶中的使用者或角色 (委託人) 只能執行與套用至帳戶的 SCPs 和連接至委託人的 IAM 許可政策相交的操作。例如，您可以使用 SCPs 來防止帳戶中的任何委託人修改其帳戶的替代聯絡人。

如需適用於 SCPs 範例 AWS 帳戶，請參閱[使用 AWS Organizations 服務控制政策限制存取](#)。

啟用 AWS 帳戶管理的受信任存取

這些指示說明如何在使用 AWS 註冊 AWS (進階) 註冊或啟用帳戶的進階功能時，啟用 AWS 帳戶管理的受信任存取。若要比較註冊選項，請參閱[比較註冊選項](#)。

啟用 AWS Account Management 的受信任存取權可讓管理帳戶的管理員修改每個成員帳戶的特定資訊和中繼資料 (例如，主要或替代聯絡人詳細資訊) AWS Organizations。如需詳細資訊，請參閱AWS

Organizations 《使用者指南》中的[AWS 帳戶管理和 AWS Organizations](#)。如需受信任存取如何運作的一般資訊，請參閱[搭配使用 AWS Organizations 與其他服務](#)。

啟用受信任存取後，您可以在支援它的[帳戶管理 API 操作](#)中使用 `accountID` 參數。只有在使用來自管理帳戶的登入資料呼叫操作，或啟用組織的委派管理員帳戶時，才能成功使用此參數。如需詳細資訊，請參閱[啟用 AWS 帳戶管理的委派管理員帳戶](#)。

使用下列程序為組織中的帳戶管理啟用受信任存取。

最低許可

若要執行這些任務，您必須符合下列要求：

- 您只能從組織的管理帳戶執行此操作。
- 您的組織必須[啟用所有功能](#)。

AWS 管理主控台

啟用 AWS Account Management 的受信任存取

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在導覽窗格中選擇服務。
3. 在服務清單中選擇 AWS 帳戶管理。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在啟用 AWS 帳戶管理的受信任存取對話方塊中，輸入啟用以確認，然後選擇啟用受信任存取。

AWS CLI & SDKs

啟用 AWS Account Management 的受信任存取

執行下列命令後，您可以使用組織的管理帳戶中的登入資料來呼叫 Account Management API 操作，這些操作使用 `--accountID` 參數來參考組織中的成員帳戶。

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

下列範例會啟用呼叫 AWS 帳戶組織中帳戶管理的受信任存取。

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

此命令如果成功就不會產生輸出。

啟用 AWS 帳戶管理的委派管理員帳戶

這些指示說明如何在使用 AWS 註冊 AWS（進階）註冊或啟用帳戶的進階功能時，啟用 AWS 帳戶管理的委派管理員帳戶。若要比較註冊選項，請參閱 [比較註冊選項](#)。

您可以為每個組織註冊帳戶管理服務的委派管理員 AWS 帳戶。註冊此帳戶後，該帳戶中的使用者和角色可以透過支援選用AccountId參數，在 Organizations 模式中運作的account命名空間中呼叫 AWS CLI 和 AWS SDK 操作。這可讓委派的管理員呼叫 中其他成員帳戶 AWS 的帳戶管理 API 操作 AWS Organizations。

若要將組織中的成員帳戶註冊為委派的管理員帳戶，請使用下列程序。

AWS CLI & SDKs

註冊 Account Management 服務的委派管理員帳戶

您可以使用下列命令來啟用帳戶管理服務的委派管理員。

最低許可

若要執行這些任務，您必須符合下列要求：

- 您只能從組織的管理帳戶執行此操作。
- 您的組織必須[啟用所有功能](#)。
- 您必須為[組織中的帳戶管理啟用受信任存取](#)。

您必須指定下列服務主體：

```
account.amazonaws.com
```

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

下列範例會將組織的成員帳戶註冊為帳戶管理服務的委派管理員。

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

此命令如果成功就不會產生輸出。

執行此命令後，您可以使用帳戶 123456789012 的登入資料來呼叫帳戶管理和 AWS CLI SDK API 操作，這些操作使用 `--account-id` 參數來參考組織中的成員帳戶。

AWS 管理主控台

AWS 帳戶管理管理主控台不支援此任務。您只能使用其中一個 AWS SDKs 的 AWS CLI 或 API 操作來執行此任務。

使用 AWS Organizations 服務控制政策限制存取

如果您使用註冊 AWS（進階）註冊或為您的帳戶啟用進階功能，此資訊是關於 AWS 使用 AWS Organizations 服務控制政策來限制存取。若要比較註冊選項，請參閱 [比較註冊選項](#)。

本主題提供範例，示範如何在 中使用服務控制政策 (SCPs) AWS Organizations 來限制組織中帳戶中的使用者和角色可執行的操作。如需服務控制政策的詳細資訊，請參閱 AWS Organizations 《使用者指南》中的下列主題：

- [建立 SCPs](#)
- [將 SCPs 連接至 OUs 和帳戶](#)
- [SCPs 的策略](#)
- [SCP 政策語法](#)

Example 範例 1：防止帳戶修改自己的替代聯絡人

下列範例會拒絕任何成員帳戶在 [獨立帳戶模式下](#) 呼叫 `PutAlternateContact` 和 `DeleteAlternateContact` API 操作。這可防止受影響帳戶中的任何主體變更自己的替代聯絡人。

JSON

```
{
```

```

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

```

Example 範例 2：防止任何成員帳戶修改組織中任何其他成員帳戶的替代聯絡人

下列範例會將 Resource 元素一般化為「*」，這表示它同時適用於[獨立模式請求](#)和[組織模式請求](#)。這表示即使帳戶管理的委派管理員帳戶適用，如果 SCP 也無法變更組織中任何帳戶的任何替代聯絡人。

JSON

```

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

```

Example 範例 3：防止 OU 中的成員帳戶修改自己的替代聯絡人

下列範例 SCP 包含的條件會將帳戶的組織路徑與兩個 OUs 的清單進行比較。這會導致封鎖指定 OUs 中任何帳戶中的委託人修改自己的替代聯絡人。

使用時機 AWS Control Tower

此資訊是關於您 AWS Control Tower 何時使用註冊 AWS（進階）註冊 AWS，或是否已啟用帳戶的進階功能。若要比較註冊選項，請參閱 [比較註冊選項](#)。

AWS Organizations 是基礎服務，可讓您集中管理和保護整個 AWS 環境。以此 AWS Organizations 為中心方法的關鍵元件是 AWS Control Tower。充 AWS Control Tower 當 Organizations 內的管理主控台，透過套用規範性最佳實務，提供簡化的方式來設定和管理安全、多帳戶 AWS 環境。

提供的這種安全最佳實務方法 AWS Control Tower 擴展了 的核心功能 AWS Organizations。會 AWS Control Tower 套用一組預防性和偵測性護欄，以協助確保您的組織和帳戶符合建議的安全和合規標準。

透過使用 建立架構良好的 AWS Organizations 結構 AWS Control Tower，您可以快速部署可擴展、安全且合規 AWS 的環境。這種集中式雲端管理和控管方法對於希望充分利用 功能的企業來說至關重要，AWS 雲端 同時保持最高標準的安全性和合規。

如需詳細資訊，請參閱《AWS Control Tower使用者指南》中的[什麼是AWS Control Tower？](#)。

了解 API 操作模式

此資訊是關於了解如果您 AWS 使用註冊 AWS（進階）註冊，或如果您為帳戶啟用進階功能的操作 API 模式。若要比較註冊選項，請參閱 [比較註冊選項](#)。

使用 的屬性 AWS 帳戶的 API 操作一律以兩種操作模式之一運作：

- 獨立內容 – 當帳戶中的使用者或角色存取或變更相同帳戶中的帳戶屬性時，就會使用此模式。當您呼叫其中一個帳戶管理 AWS CLI 或 AWS SDK 操作時，未包含 AccountId 參數時，會自動使用獨立內容模式。
- 組織內容 – 當組織中某個帳戶中的使用者或角色存取或變更同一組織中不同成員帳戶中的帳戶屬性時，就會使用此模式。當您呼叫其中一個帳戶管理 AWS CLI 或 AWS SDK 操作時，當您包含 AccountId 參數時，會自動使用組織內容模式。您只能從組織的管理帳戶或帳戶管理的委派管理員帳戶呼叫此模式中的操作。

AWS CLI 和 AWS SDK 操作可以在獨立或組織環境中運作。

- 如果您未包含 AccountId 參數，則操作會在獨立內容中執行，並自動將請求套用至您用來提出請求的帳戶。無論帳戶是否為組織的成員，都是如此。

- 如果您包含 `AccountId` 參數，則操作會在組織內容中執行，而操作會在指定的 Organizations 帳戶中運作。
- 如果呼叫操作的帳戶是帳戶管理服務的管理帳戶或委派管理員帳戶，則您可以在 `AccountId` 參數中指定該組織的任何成員帳戶，以更新指定的帳戶。
- 組織中唯一可以呼叫其中一個替代聯絡操作並在 `AccountId` 參數中指定自己的帳戶號碼的帳戶，是指定為帳戶管理服務的委派管理員帳戶的帳戶。任何其他帳戶，包括管理帳戶，都會收到 `AccessDenied` 例外狀況。
- 如果您以獨立模式執行操作，則必須允許您使用包含 `Resource` 元素的 IAM 政策來執行操作 "*"，以允許所有資源，或使用獨立帳戶語法的 ARN。
- 如果您在組織模式下執行操作，則必須允許您使用包含 `Resource` 元素的 IAM 政策來執行操作 "*"，以允許所有資源，或使用組織中成員帳戶語法的 ARN。

授予更新帳戶屬性的許可

與大多數 AWS 操作一樣，您可以使用 IAM AWS 帳戶許可政策授予新增、更新或刪除帳戶屬性的許可。https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html 當您將 IAM 許可政策連接至 IAM 主體（使用者或角色）時，您可以指定主體可以對哪些資源執行哪些動作，以及在哪些條件下執行哪些動作。

以下是建立許可政策的一些帳戶管理特定考量。

的 Amazon Resource Name 格式 AWS 帳戶

- 您可以 AWS 帳戶 包含在政策陳述式 `resource` 元素中的 [Amazon Resource Name \(ARN\)](#)，會根據您要參考的帳戶是獨立帳戶還是組織中的帳戶，以不同的方式建構。請參閱上一節[了解 API 操作模式](#)。

獨立帳戶的帳戶 ARN：

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

當您在獨立模式下執行帳戶屬性操作時，如果不包含 `AccountID` 參數，則必須使用此格式。

組織中成員帳戶的帳戶 ARN：

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

當您在組織模式下執行帳戶屬性操作時，必須包含 AccountID 參數，才能使用此格式。

IAM 政策的內容索引鍵

Account Management 服務也提供數個 [Account Management 服務特定條件金鑰](#)，可讓您精細控制您授予的許可。

account:AccountResourceOrgPaths

內容索引鍵 `account:AccountResourceOrgPaths` 可讓您透過組織的階層指定通往特定組織單位 (OU) 的路徑。只有該 OU 包含的成員帳戶符合條件。下列範例程式碼片段會限制政策僅套用至位於兩個指定 OUs 其中之一的帳戶。

由於 `account:AccountResourceOrgPaths` 是多值字串類型，您必須使用 [ForAnyValue](#) 或 [ForAllValues](#) 多值字串運算子。此外，請注意，即使您參考組織中 OUs 路徑 `account`，條件索引鍵上的字首為。

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

account:AccountResourceOrgTags

內容索引鍵 `account:AccountResourceOrgTags` 可讓您參考可連接到組織中帳戶的標籤。標籤是金鑰/值字串對，可用來分類和標記帳戶中的資源。如需標記的詳細資訊，請參閱 AWS Resource Groups 《使用者指南》中的 [標籤編輯器](#)。如需有關在屬性型存取控制策略中使用標籤的資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC for AWS](#)。下列範例程式碼片段會限制政策僅套用至組織中具有 金鑰標籤 `project` 且值為 `blue` 或 `red` 的帳戶。

由於 `account:AccountResourceOrgTags` 是多值字串類型，您必須使用 [ForAnyValue](#) 或 [ForAllValues](#) 多值字串運算子。此外，請注意，即使您參考組織成員帳戶上的標籤 `account`，條件索引鍵上的字首為。

```
"Condition": {
```

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

Note

您只能將標籤連接到組織中的帳戶。您無法將標籤連接至獨立 AWS 帳戶。

設定您的 AWS 帳戶

這些指示說明如何在使用 AWS 註冊 AWS (進階) 註冊 AWS 帳戶，或啟用帳戶的進階功能時設定。若要比較註冊選項，請參閱 [比較註冊選項](#)。

本節包含描述如何管理的主題 AWS 帳戶。

Note

如果您的 AWS 帳戶 是使用 Amazon Web Services India Private Limited (AWS 印度) 在印度建立的，則還有其他考量。如需詳細資訊，請參閱[管理印度的帳戶](#)。

主題

- [建立 AWS 帳戶 別名](#)
- [AWS 區域 在您的帳戶中啟用或停用](#)
- [更新 的帳單 AWS 帳戶](#)
- [更新根使用者電子郵件地址](#)
- [更新根使用者密碼](#)
- [更新 AWS 帳戶 名稱](#)
- [更新 的替代聯絡人 AWS 帳戶](#)
- [更新 的主要聯絡人 AWS 帳戶](#)
- [檢視 AWS 帳戶 識別符](#)

建立 AWS 帳戶 別名

這些指示說明如何在使用 AWS 註冊 AWS（進階）AWS 帳戶註冊，或啟用帳戶的進階功能時建立別名。若要比較註冊選項，請參閱 [比較註冊選項](#)。

如果您希望 IAM 使用者的 URL 包含您的公司名稱（或其他 easy-to-remember 識別符），而不是 AWS 帳戶 ID，您可以建立帳戶別名。

若要了解如何建立或更新帳戶別名，請參閱《IAM 使用者指南》中的 [為您的 AWS 帳戶 ID 使用別名](#)。

AWS 區域 在您的帳戶中啟用或停用

如果您 AWS 使用註冊 AWS（進階）AWS 區域 AWS 帳戶註冊，或者您為帳戶啟用進階功能，則此資訊與啟用或停用 相關。若要比較註冊選項，請參閱 [比較註冊選項](#)。

AWS 區域 是世界上 AWS 具有多個可用區域的實體位置。可用區域由一或多個離散 AWS 資料中心組成，每個資料中心都具有備援電源、聯網和連線能力，並存放在不同的設施中。這表示每個 AWS 區域都是實體隔離的，並且獨立於其他 區域。區域提供容錯能力、穩定性和恢復能力，也可降低延遲。在 AWS 區域 較接近最終使用者的位置執行工作負載，可以改善效能並降低延遲。如需可用和近期區域的地圖，請參閱 [區域和可用區域](#)。若要進一步了解工作負載的 AWS 區域 和 彈性架構，請造訪 [AWS 多區域基本概念](#)。

AWS 區域 大體上可分為兩類帳戶的可用性：

- 預設區域 – 預設會啟用 2019 年 3 月 20 日之前啟動的區域。您可以在帳戶啟用後立即在這些預設區域中建立和管理資源。預設區域無法啟用或停用。
- 選擇加入區域 – 2019 年 3 月 20 日之後啟動的區域預設為停用，稱為選擇加入區域。停用的選擇加入區域不會顯示在主控制台導覽列中，而且在啟用之前，您無法使用這些區域來建立工作負載。若要使用這些選擇加入區域，您必須先在中啟用這些區域 AWS 帳戶。啟用選擇加入區域之後，您可以在導覽列中選取該區域，並在該區域中建立和管理資源。若要為獨立帳戶啟用選擇加入區域，請參閱 [啟用或停用獨立帳戶的 區域](#)和 [為您的成員帳戶啟用選擇加入區域](#)，請參閱 [啟用或停用組織中的 區域](#)。

當您註冊時 AWS 帳戶，會根據您的聯絡地址國家/地區為您 AWS 建議選擇加入區域。在 AWS 選擇加入區域的國家/地區中，客戶會在聯絡資訊頁面上看到啟用該國家/地區選擇加入區域的建議。在同時具有選擇加入區域和預設區域的國家/地區中，例如印度、澳洲或加拿大，如果選擇加入區域比預設區域更接近，請參閱選擇加入區域的建議。帳戶啟用後，您可以在帳戶中啟用其他 AWS 選擇加入區域，或選擇停用您在註冊期間啟用的選擇加入區域。

當您建立時 AWS 帳戶，您的 IAM 資料和登入資料會自動設定為在所有預設區域中運作，允許具有適當許可的根使用者和 IAM 身分使用其現有的登入資料存取這些區域中 AWS 的服務。在預設情況下 AWS，選擇加入區域會停用，且這些區域中一開始無法使用 IAM 資料和登入資料，以防止存取該區域中 AWS 的服務。當您選擇啟用選擇加入區域時，會將您的 IAM 資料和登入資料 AWS 傳播至該區域。一旦傳播完成且啟用了選擇加入區域，根使用者和 IAM 身分就可以使用他們在預設區域中使用的相同 IAM 登入資料來存取新啟用選擇加入區域中 AWS 的服務。

當您停用選擇加入區域時，您的 IAM 登入資料會停用，而您會失去該選擇加入區域中資源的 IAM 存取權。停用選擇加入區域不會刪除該區域中的資源，而且該停用選擇加入區域中的資源（如果有的話）費用會繼續以標準費率累積。

Important

停用區域會停用 區域中資源的 IAM 存取。這不會刪除有問題的資源，這會持續產生費用。在停用區域之前移除任何剩餘的資源。

AWS 將區域分組為[分割區](#)。每個區域都只有一個分割區，而且每個分割區都有一或多個區域。分割區具有獨立的 AWS Identity and Access Management (IAM) 執行個體，並在不同 partitions. AWS commercial 區域中的區域位於aws分割區中、中國區域位於aws-cn分割區中，以及 AWS GovCloud (US) 區域位於aws-us-gov分割區中之間提供硬邊界。根據您建立的分割區 AWS 帳戶，您可以在該分割區 AWS 區域內使用。

- aws 分割區中的帳戶可讓您存取商業分割區中的多個區域，以便在符合您的需求的位置啟動 AWS 資源。例如，您可能想要在歐洲啟動 Amazon EC2 執行個體，以便更接近您的歐洲客戶或符合法律要求。
- aws-us-gov 分割區中的帳戶可讓您存取 AWS GovCloud（美國西部）區域和 AWS GovCloud（美國東部）區域。如需詳細資訊，請參閱[AWS GovCloud \(US\)](#)。
- aws-cn 分割區中的帳戶只會讓您存取北京和寧夏區域。如需詳細資訊，請參閱 [Amazon Web Services in China](#) (Amazon Web Services (中國))。

主題

- [區域可用性參考](#)
- [啟用和停用區域前的考量事項](#)
- [處理時間和請求限制](#)
- [啟用或停用獨立帳戶的 區域](#)

- [啟用或停用組織中的區域](#)

區域可用性參考

下表 AWS 區域 依可用性類型列出。預設區域會自動啟用且無法停用，而選擇加入區域必須先手動啟用，才能使用它們：

Opt-in Regions

下列區域是選擇加入區域，您必須先啟用，才能使用它們：

名稱	Code	狀態
非洲 (開普敦)	af-south-1	GA
亞太地區 (香港)	ap-east-1	GA
亞太區域 (台北)	ap-east-2	GA
亞太地區 (海德拉巴)	ap-south-2	GA
亞太地區 (雅加達)	ap-southeast-3	GA
亞太地區 (墨爾本)	ap-southeast-4	GA
亞太地區 (馬來西亞)	ap-southeast-5	GA
亞太區域 (紐西蘭)	ap-southeast-6	GA
亞太區域 (泰國)	ap-southeast-7	GA
加拿大西部 (卡加利)	ca-west-1	GA
歐洲 (蘇黎世)	eu-central-2	GA
歐洲 (米蘭)	eu-south-1	GA
歐洲 (西班牙)	eu-south-2	GA
以色列 (特拉維夫)	il-central-1	GA

名稱	Code	狀態
中東 (阿拉伯聯合大公國)	me-central-1	GA
Middle East (Bahrain)	me-south-1	GA
墨西哥 (中部)	mx-central-1	GA

Default Regions

下列區域預設為啟用，且無法停用：

名稱	Code
亞太地區 (東京)	ap-northeast-1
亞太地區 (首爾)	ap-northeast-2
亞太地區 (大阪)	ap-northeast-3
亞太地區 (孟買)	ap-south-1
亞太地區 (新加坡)	ap-southeast-1
亞太地區 (雪梨)	ap-southeast-2
加拿大 (中部)	ca-central-1
歐洲 (法蘭克福)	eu-central-1
歐洲 (斯德哥爾摩)	eu-north-1
歐洲 (愛爾蘭)	eu-west-1
歐洲 (倫敦)	eu-west-2
Europe (Paris)	eu-west-3
南美洲 (聖保羅)	sa-east-1

名稱	Code
美國東部 (維吉尼亞北部)	us-east-1
美國東部 (俄亥俄)	us-east-2
美國西部 (加利佛尼亞北部)	us-west-1
美國西部 (奧勒岡)	us-west-2

如需區域名稱及其對應代碼的清單，請參閱《AWS 一般參考指南》中的[區域端點](#)。如需每個區域（不含端點）支援的 AWS 服務清單，請參閱[AWS 區域服務清單](#)。

Important

AWS 建議您使用 regional AWS Security Token Service (AWS STS) 端點，而不是全域端點來減少延遲。區域 AWS STS 端點的工作階段權杖在所有區域中都有效 AWS。如果您使用區域 AWS STS 端點，則不需要進行任何變更。不過，來自全域 AWS STS 端點 (<https://sts.amazonaws.com>) 的工作階段字符僅在您啟用 AWS 區域的 中有效，或預設啟用的 中有效。如果您想要為帳戶啟用新的區域，您可以使用區域 AWS STS 端點的工作階段字符，或啟用全域 AWS STS 端點來發出在所有 中有效的工作階段字符 AWS 區域。在所有區域中皆有效的工作階段字符較大。如果您儲存工作階段字符，則這些較大的字符可能會影響您的系統。如需 AWS STS 端點如何使用 AWS 區域的詳細資訊，請參閱[在 AWS STSAWS 區域中管理](#)。

啟用和停用區域前的考量事項

在您啟用或停用區域之前，請務必考慮下列事項：

- 無論區域選擇狀態為何，您都可以在跨區域推論地理位置中使用所有目的地區域 – 某些 AWS 生成式 AI 服務，包括 Amazon Bedrock（請參閱[使用跨區域推論增加輸送量](#)）和 Amazon Q Developer（請參閱[Amazon Q Developer 中的跨區域處理](#)）使用跨區域推論。如果您使用這些服務，它們會自動在您選擇的地理位置內選取最佳 AWS 區域- 包括您尚未為資源和 IAM 資料啟用的區域。這可透過最大化可用的運算和模型可用性來改善客戶體驗。
- 您可以使用 IAM 許可來控制區域存取 – AWS Identity and Access Management (IAM) 包含四個許可，可讓您控制哪些使用者可以啟用、停用、取得和列出區域。如需詳細資訊，請參閱《IAM 使用者指南》中的[AWS 允許啟用和停用 AWS 區域](#)。您也可以使用 [aws:RequestedRegion](#) 條件金鑰來控制對 AWS 服務的存取 AWS 區域。

- 啟用和停用區域是免費的 – 啟用或停用區域無需付費。您只需為在新區域中建立的資源付費。
- Amazon EventBridge 整合 – 您可以在 EventBridge 中訂閱區域選項狀態更新通知。系統會為每個狀態變更建立 EventBridge 通知，讓客戶能夠自動化工作流程。
- 表達式區域選項狀態 – 由於啟用/停用選擇加入區域的非同步性質，區域選項請求有四種潛在狀態：
 - ENABLING
 - DISABLING
 - ENABLED
 - DISABLED

當選擇加入或選擇退出處於 ENABLING 或 DISABLING 狀態時，您無法取消。否則，ConflictException 將會擲回。已完成（啟用/停用）區域選項請求取決於金鑰基礎 AWS 服務的佈建。即使狀態為，有些 AWS 服務仍無法立即使用 ENABLED。

處理時間和請求限制

啟用或停用區域時，請注意下列時間和請求限制：

- 在某些情況下，啟用區域需要幾分鐘到幾個小時 – 當您啟用區域時，AWS 會執行動作來準備您在該區域中的帳戶，例如將您的 IAM 資源分發到該區域。大多數帳戶需要幾分鐘的時間，但有時可能需要幾個小時。直到此過程完成之前，您都無法使用區域。
- 停用區域不一定會立即顯示 – 停用區域後，服務和主控台可能會暫時顯示。停用區域可能需要幾分鐘到幾個小時才會生效。
- 單一帳戶在任何指定時間都可以有 6 個進行中的區域選擇請求 – 一個請求等於對一個帳戶啟用或停用一個特定區域。
- 組織可以在 AWS 組織的指定時間開啟 50 個區域選擇請求 - 管理帳戶可以隨時有 50 個待處理請求等待組織完成。一個請求等於啟用或停用一個帳戶的特定區域。

啟用或停用獨立帳戶的 區域

若要更新 AWS 帳戶可存取的區域，請執行下列程序中的步驟。下列 AWS 管理主控台 程序一律只能在獨立內容中運作。您可以使用 AWS 管理主控台 檢視或僅更新您用來呼叫 操作之帳戶中的可用區域。

AWS 管理主控台

啟用或停用獨立 的區域 AWS 帳戶

最低許可

若要執行下列程序中的步驟，IAM 使用者或角色必須具有下列許可：

- `account:ListRegions` (需要檢視 的清單，AWS 區域 以及它們目前是否啟用或停用)。
- `account:EnableRegion`
- `account:DisableRegion`

1. [AWS 管理主控台](#) 以具有最低許可的 AWS 帳戶根使用者 或 IAM 使用者或角色身分登入。
2. 選擇視窗右上角的帳戶名稱，然後選擇帳戶。
3. 在[帳戶頁面上](#)，向下捲動至區段 AWS 區域。
4. 選擇您要啟用或停用的區域，然後選擇所需的動作啟用或停用。您會看到確認提示。
5. 如果您選擇啟用選項，請檢閱顯示的文字，然後選擇啟用區域。

如果您選擇停用選項，請檢閱顯示的文字，輸入 **disable** 進行確認，然後選擇停用區域。

啟用選擇加入區域後，您可以從區域導覽列中選取該區域。如需選取區域的步驟，請參閱 [中的從導覽列中選擇 AWS 管理主控台](#) 區域，以及 帳戶中的區域特定主控台設定，請參閱 [中的設定預設區域 AWS 管理主控台](#)。

AWS CLI & SDKs

您可以使用下列 AWS CLI 命令或其 AWS SDK 對等操作來啟用、停用、讀取和列出區域選擇狀態：

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

最低許可

若要執行下列步驟，您必須擁有對應至該操作的許可：

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

如果您使用這些個別許可，您可以授予某些使用者僅讀取區域選擇資訊的能力，並授予其他人同時讀取和寫入的能力。

下列範例會為組織中指定的成員帳戶啟用區域。使用的登入資料必須來自組織的管理帳戶，或來自帳戶管理的委派管理員帳戶。

請注意，您也可以使用相同的命令停用區域，然後使用 取代 `enable-region` `disable-region`。

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

此命令如果成功就不會產生輸出。

操作是非同步的。下列命令可讓您查看請求的最新狀態。

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

啟用或停用組織中的區域

若要更新 成員帳戶已啟用的區域 AWS Organizations，請執行下列程序中的步驟。

Note

AWS Organizations 受管政策 `AWSOrganizationsReadOnlyAccess` 或 `AWSOrganizationsFullAccess` 已更新，以提供存取 AWS 帳戶管理 APIs 許可，以便

您可以從 AWS Organizations 主控台存取帳戶資料。若要檢視更新的受管政策，請參閱 [Organizations AWS 受管政策的更新](#)。

Note

在您可以從管理帳戶或組織中的委派管理員帳戶執行這些操作，以便與成員帳戶搭配使用之前，您必須：

- 啟用組織中的所有功能，以管理成員帳戶的設定。這可讓管理員控制成員帳戶。這會在您建立組織時預設為。如果您的組織設定為僅合併帳單，且您想要啟用所有功能，請參閱[啟用組織中的所有功能](#)。
- 啟用 AWS Account Management 服務的受信任存取。若要設定此項目，請參閱 [啟用 AWS 帳戶管理的受信任存取](#)。

AWS 管理主控台

啟用或停用組織中的區域

1. 使用組織的管理帳戶登入資料登入 AWS Organizations 主控台。
2. 在頁面上AWS 帳戶，選取您要更新的帳戶。
3. 選擇帳戶設定索引標籤。
4. 在區域下，選取您要啟用或停用的區域。
5. 選擇動作，然後選擇啟用或停用選項。
6. 如果您選擇啟用選項，請檢閱顯示的文字，然後選擇啟用區域。
7. 如果您選擇停用選項，請檢閱顯示的文字，輸入停用進行確認，然後選擇停用區域。

AWS CLI & SDKs

您可以使用下列 AWS CLI 命令或其 AWS SDK 對等操作來啟用、停用、讀取和列出組織成員帳戶的區域選擇狀態：

- EnableRegion
- DisableRegion
- GetRegionOptStatus

- ListRegions

 最低許可

若要執行下列步驟，您必須擁有對應至該操作的許可：

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

如果您使用這些個別許可，您可以授予某些使用者僅讀取區域選擇資訊的能力，並授予其他人同時讀取和寫入的能力。

下列範例會為組織中指定的成員帳戶啟用區域。使用的登入資料必須來自組織的管理帳戶，或來自帳戶管理的委派管理員帳戶。

請注意，您也可以使用相同的命令停用區域，然後使用 取代 `enable-region` `disable-region`。

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

此命令如果成功就不會產生輸出。

 Note

組織在特定時間最多只能有 20 個區域請求。否則，您會收到 `TooManyRequestsException`。

操作是非同步的。下列命令可讓您查看請求的最新狀態。

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

```
}
```

更新的帳單 AWS 帳戶

這些指示旨在說明 AWS 帳戶 如果您 AWS 使用註冊 AWS（進階）註冊，或如果您為 帳戶啟用進階功能，如何更新 的帳單。若要比較註冊選項，請參閱 [比較註冊選項](#)。

您可以使用 AWS Billing 和 Cost Management 主控台來更新所有 AWS 帳戶 帳單偏好設定。若要了解如何更新帳戶的帳單相關設定，請參閱 [AWS 帳單與成本管理 使用者指南](#)：

更新根使用者電子郵件地址

這些指示旨在說明如果您 AWS 使用註冊 AWS（進階）註冊或啟用帳戶的進階功能，如何更新根使用者電子郵件地址。若要比較註冊選項，請參閱 [比較註冊選項](#)。

基於各種商業原因，您可能需要更新根使用者電子郵件地址 AWS 帳戶。例如，安全與管理彈性。本主題會逐步引導您更新獨立和成員帳戶的根使用者電子郵件地址。

Note

變更 最多 AWS 帳戶 可能需要四個小時才能傳播到任何地方。

您可以根據帳戶是否為獨立帳戶或組織的一部分，以不同的方式更新根使用者電子郵件：

- 獨立帳戶 AWS 帳戶 或管理帳戶 – 對於 AWS 帳戶 未與組織建立關聯或組織的管理帳戶，您可以使用 AWS 管理主控台更新根使用者電子郵件。若要了解如何執行此操作，請參閱[更新獨立 AWS 帳戶 或管理帳戶的根使用者電子郵件](#)。
- 在 AWS 帳戶 組織中 – 對於屬於 AWS 組織的成員帳戶，管理帳戶或委派管理員帳戶中的使用者可以從 AWS Organizations 主控台集中更新成員帳戶的根使用者電子郵件，或透過 CLI AWS 和 SDKs 以程式設計方式更新成員帳戶的電子郵件。若要了解如何執行此操作，請參閱[更新 AWS 帳戶 組織中任何 的根使用者電子郵件](#)。

主題

- [更新獨立 AWS 帳戶 或管理帳戶的根使用者電子郵件](#)
- [更新 AWS 帳戶 組織中任何 的根使用者電子郵件](#)

更新獨立 AWS 帳戶 或管理帳戶的根使用者電子郵件

若要編輯獨立 AWS 帳戶 或管理帳戶的根使用者電子郵件地址，請執行下列程序的步驟。

AWS 管理主控台

Note

您必須以 身分登入 AWS 帳戶根使用者，這不需要額外的 IAM 許可。您無法以 IAM 使用者或角色的身分執行這些步驟。

1. 使用 AWS 帳戶您的電子郵件地址和密碼，以您的[AWS 管理主控台](#)身分登入 AWS 帳戶根使用者。
2. 在主控台的右上角，選擇您的帳戶名稱或號碼，然後選擇帳戶。
3. 在[帳戶頁面](#)的帳戶詳細資訊旁，選擇動作，然後選取更新電子郵件地址和密碼。
4. 在帳戶詳細資訊頁面上，選擇編輯。
5. 在編輯帳戶電子郵件頁面上，填寫新電子郵件地址、確認新電子郵件地址和確認目前密碼的欄位。然後，選擇儲存並繼續。驗證碼會從 傳送至您的新電子郵件地址no-reply@verify.signin.aws。
6. 在編輯帳戶電子郵件頁面的驗證碼下，輸入您從電子郵件收到的代碼，然後選擇確認更新。

Note

驗證碼最多可能需要 5 分鐘才會送達。如果您在收件匣中沒有看到電子郵件，請檢查您的垃圾郵件資料夾。

AWS CLI & SDKs

中 AWS CLI 或其中一個 AWS SDKs API 操作不支援此任務。您只能使用 來執行此任務 AWS 管理主控台。

更新 AWS 帳戶 組織中任何 的根使用者電子郵件

若要使用 AWS Organizations 主控台編輯組織中任何成員帳戶的根使用者電子郵件地址，請執行下列程序的步驟。

Note

在您更新成員帳戶的根使用者電子郵件地址之前，建議您了解此操作的影響。如需詳細資訊，請參閱AWS Organizations 《使用者指南》中的[使用 更新成員帳戶的根使用者電子郵件地址AWS Organizations](#)。

您也可以在以根使用者身分登入後，直接從 中的帳戶頁面更新成員帳戶的根使用者電子郵件地址。AWS 管理主控台 如需step-by-step說明，請遵循 中提供的步驟[更新獨立 AWS 帳戶 或管理帳戶的根使用者電子郵件](#)。

Note

您無法更新專案帳戶的根使用者電子郵件地址，這是在 AWS 設定中建立做為專案的成員帳戶。AWS Builder ID 擁有每個專案帳戶，而不是根使用者電子郵件地址，這不會在您啟用進階功能時變更。如需詳細資訊，請參閱[啟用進階功能之後的專案帳戶](#)。

AWS Management Console

備註

- 若要從管理帳戶或組織中的委派管理員帳戶針對成員帳戶執行此程序，您必須[啟用帳戶管理服務的信任存取](#)。
- 您無法使用此程序來存取與您用來呼叫 操作的不同組織中的帳戶。

使用 AWS Organizations 主控台更新成員帳戶的根使用者電子郵件地址

1. 登入 [AWS Organizations 主控台](#)。您必須以 IAM 使用者身分登入，或以組織的管理帳戶中的根使用者身分登入 ([不建議](#))。
2. 在AWS 帳戶頁面上，選擇要更新根使用者電子郵件地址的成員帳戶。
3. 在帳戶詳細資訊區段中，選擇動作按鈕，然後選擇更新電子郵件地址。
4. 在電子郵件下，輸入根使用者的新電子郵件地址，然後選擇儲存。這會將一次性密碼 (OTP) 傳送至新的電子郵件地址。

Note

如果您在等待程式碼時需要在 Organizations 主控台中關閉此頁面，您可以在程式碼傳送後的 24 小時內傳回並完成 OTP 程序。若要這樣做，請在帳戶詳細資訊頁面上選擇動作按鈕，然後選擇完成電子郵件更新。

5. 在驗證碼下，輸入在上一個步驟中傳送到新電子郵件地址的代碼，然後選擇確認。這會將更新遞交給帳戶的根使用者。

AWS CLI & SDKs

您可以使用下列 AWS CLI 命令或其 AWS SDK 對等操作來擷取或更新根使用者電子郵件地址（也稱為主要電子郵件地址）：

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

備註

- 若要從管理帳戶或組織中的委派管理員帳戶對成員帳戶執行這些操作，您必須[啟用帳戶管理服務的信任存取](#)。
- 您無法存取與您用來呼叫 操作的 不同組織中的帳戶。
- 對於專案帳戶，AccessDeniedException即使您具有必要的許可，StartPrimaryEmailUpdate 也會AcceptPrimaryEmailUpdate失敗並發生錯誤。

最低許可

對於每個操作，您必須擁有映射到該操作的許可：

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

如果您使用這些個別許可，您可以授予一些使用者僅讀取根使用者電子郵件地址 資訊的能力，並授予其他人同時讀取和寫入的能力。

若要完成根使用者電子郵件地址程序，您必須依照下列範例所示的順序，同時使用主要電子郵件 APIs。

Example **GetPrimaryEmail**

下列範例會從組織中指定的成員帳戶擷取根使用者電子郵件地址。使用的登入資料必須來自組織的管理帳戶，或來自帳戶管理的委派管理員帳戶。

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

Example **StartPrimaryEmailUpdate**

下列範例會啟動根使用者電子郵件地址更新程序、識別新的電子郵件地址，並將一次性密碼 (OTP) 傳送至組織中指定成員帳戶的新電子郵件地址。使用的登入資料必須來自組織的管理帳戶，或來自帳戶管理的委派管理員帳戶。

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

Example **AcceptPrimaryEmailUpdate**

下列範例接受 OTP 程式碼，並將新的電子郵件地址設定為組織中指定的成員帳戶。使用的登入資料必須來自組織的管理帳戶，或來自帳戶管理的委派管理員帳戶。

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

更新根使用者密碼

這些指示說明如何在使用 AWS 註冊 AWS（進階）註冊，或啟用帳戶的進階功能時更新根使用者密碼。若要比較註冊選項，請參閱 [比較註冊選項](#)。

若要編輯 AWS 帳戶您的根使用者密碼，請執行下列程序中的步驟。

AWS 管理主控台

編輯您的根使用者密碼

Note

您必須以 身分登入 AWS 帳戶根使用者，這不需要額外的 IAM 許可。您無法以 IAM 使用者或角色的身分執行這些步驟。

1. 使用 AWS 帳戶您的電子郵件地址和密碼，以您的[AWS 管理主控台](#)身分登入 AWS 帳戶根使用者。
2. 在主控台的右上角，選擇您的帳戶名稱或號碼，然後選擇帳戶。
3. 在[帳戶頁面](#)的帳戶詳細資訊旁，選擇動作，然後選取更新電子郵件地址和密碼。
4. 在帳戶詳細資訊頁面的密碼旁邊，選擇編輯。
5. 在編輯密碼頁面上，填寫目前密碼、新密碼和確認新密碼的欄位。然後，選擇更新密碼。如需其他指引，包括設定根使用者密碼的最佳實務，請參閱《IAM 使用者指南》中的[變更的密碼 AWS 帳戶根使用者](#)。

AWS CLI & SDKs

中 AWS CLI 或其中一個 AWS SDKs API 操作不支援此任務。您只能使用 執行此任務 AWS 管理主控台。

更新 AWS 帳戶 名稱

這些指示說明如何在使用 AWS 註冊 AWS（進階）註冊或啟用帳戶的進階功能時更新 AWS 帳戶 名稱。若要比較註冊選項，請參閱 [比較註冊選項](#)。

管理多個時 AWS 帳戶，請使用與業務單位和應用程式一致的清晰命名慣例來識別和組織。在重組、合併、取得或命名慣例更新期間，您可能需要重新命名帳戶，以維持一致的識別和管理標準。

帳戶的名稱會顯示在數個位置，例如您的發票和 主控台，例如 Billing and Cost Management 儀表板和 AWS Organizations 主控台。我們建議您使用標準方法來命名您的帳戶，以便識別您的帳戶名稱。對於公司帳戶，請考慮使用命名標準，例如 organization-purpose-environment（例如 sales-catalog-prod）。基於隱私權和安全考量，請避免使用反映個人身分識別資訊 (PII) 的帳戶名稱。

- 獨立帳戶 AWS 帳戶 或管理帳戶 – 對於 AWS 帳戶 未與組織建立關聯或組織的管理帳戶，您可以使用 AWS 管理主控台或 AWS CLI 和 SDKs 更新帳戶名稱。若要了解如何操作，請參閱 [更新獨立 AWS 帳戶 或管理帳戶的帳戶名稱](#)。
- 在 AWS 帳戶 組織內 – 對於屬於 的成員帳戶 AWS Organizations，管理帳戶或委派管理員帳戶中的使用者可以從 AWS Organizations 主控台集中更新組織中任何成員帳戶的帳戶名稱，或透過 AWS CLI 和 SDKs 以程式設計方式更新。若要了解如何操作，請參閱 [更新組織中任何 AWS 帳戶 的帳戶名稱](#)。

Note

變更 最多 AWS 帳戶 可能需要四個小時才能傳播到任何地方。

主題

- [更新獨立 AWS 帳戶 或管理帳戶的帳戶名稱](#)
- [更新組織中任何 AWS 帳戶 的帳戶名稱](#)

更新獨立 AWS 帳戶 或管理帳戶的帳戶名稱

若要變更獨立帳戶 AWS 帳戶 或管理帳戶的帳戶名稱，請執行下列程序中的步驟。

AWS 管理主控台

最低許可

您可以使用根使用者、IAM 使用者或 IAM 角色來更新帳戶名稱。如果您使用的是根使用者，則不需要額外的 IAM 許可來更新帳戶名稱。使用 IAM 使用者或 IAM 角色時，您至少必須擁有下列 IAM 許可：

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

更新獨立帳戶或管理帳戶的帳戶名稱

1. 使用 AWS 帳戶您的電子郵件地址和密碼，以您的 [AWS 管理主控台](#) 身分登入 AWS 帳戶根使用者。

2. 在主控台的右上角，選擇您的帳戶名稱或號碼，然後選擇帳戶。
3. 在[帳戶頁面](#)的帳戶詳細資訊旁，選擇動作，然後選取更新帳戶名稱。
4. 在名稱下，輸入您要更新的新帳戶名稱，然後選擇儲存。

AWS CLI & SDKs

最低許可

您可以使用根使用者、IAM 使用者或 IAM 角色來更新帳戶名稱。若要執行下列步驟，您的 IAM 使用者或 IAM 角色必須至少具有下列 IAM 許可：

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

更新獨立帳戶或管理帳戶的帳戶名稱

您可以使用下列其中一個操作：

- AWS CLI：[put-account-name](#)

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

- AWS SDKs：[PutAccountName](#)

更新組織中任何 AWS 帳戶 的帳戶名稱

在 AWS Organizations 中使用所有功能模式時，管理和委派管理員帳戶中的授權 IAM 使用者或 IAM 角色可以集中管理帳戶名稱。

若要變更組織中任何成員帳戶的帳戶名稱，請執行下列程序的步驟。

要求

若要使用 AWS Organizations 主控台更新帳戶名稱，您需要執行一些初步設定：

- 您的組織必須啟用所有功能，才能管理成員帳戶的設定。這可讓管理員控制成員帳戶。這會在您建立組織時預設為。如果您的組織設定為僅合併帳單，且您想要啟用所有功能，請參閱[啟用組織的所有功能](#)。
- 您需要為 AWS 帳戶管理服務啟用受信任存取。若要設定此項目，請參閱[啟用 AWS 帳戶管理的受信任存取](#)。

AWS 管理主控台

最低許可

若要更新成員帳戶的帳戶名稱，您的 IAM 使用者或 IAM 角色必須具有下列許可：

- `organizations:DescribeOrganization` (僅限主控台)
- `account:PutAccountName`

更新成員帳戶的帳戶名稱

1. 在 <https://console.aws.amazon.com/organizations/> 開啟 Organizations 主控台。
2. 在主導覽窗格中，選擇 AWS 帳戶。
3. 在 AWS 帳戶頁面上，選擇您要更新的成員帳戶，選擇動作下拉式功能表，然後選擇更新帳戶名稱。
4. 在名稱下，輸入更新的名稱，然後選擇儲存。

AWS CLI & SDKs

最低許可

若要更新成員帳戶的帳戶名稱，您的 IAM 使用者或 IAM 角色必須具有下列許可：

- `organizations:DescribeOrganization` (僅限主控台)
- `account:PutAccountName`

更新成員帳戶的帳戶名稱

您可以使用下列其中一個操作：

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

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

- AWS SDKs : [PutAccountName](#)

更新的替代聯絡人 AWS 帳戶

這些指示旨在說明 AWS 帳戶 如果您 AWS 使用註冊 AWS（進階）註冊或啟用帳戶的進階功能，如何更新的替代聯絡人。若要比較註冊選項，請參閱 [比較註冊選項](#)。

替代聯絡人允許 AWS 最多聯絡三個與帳戶相關聯的替代聯絡人。替代聯絡人不必要是特定人員。如果您的團隊負責管理帳單、操作和安全相關問題，您可以改為新增電子郵件分佈清單。這些是與帳戶[根使用者](#)相關聯的電子郵件地址以外的地址。[主要帳戶聯絡人](#)將繼續接收傳送到根帳戶電子郵件的所有電子郵件通訊。

您只能指定下列其中一個與 帳戶相關聯的聯絡類型。

- 帳單聯絡人
- 操作聯絡人
- 安全聯絡人

您可以根據帳戶是否為獨立帳戶或組織的一部分，以不同的方式新增或編輯替代聯絡人：

- 獨立 AWS 帳戶 – 對於 AWS 帳戶 未與組織建立關聯的，您可以使用 AWS 管理主控台或透過 CLI 和 SDKs AWS 更新您自己的替代聯絡人。若要了解如何執行此操作，請參閱[更新獨立的替代聯絡人 AWS 帳戶](#)。
- 在 AWS 帳戶 組織中 – 對於屬於 AWS 組織的成員帳戶，管理帳戶或委派管理員帳戶中的使用者可以從 AWS Organizations 主控台集中更新組織中的任何成員帳戶，或透過 CLI 和 SDKs AWS 以程式設計方式更新。若要了解如何執行此操作，請參閱[更新 AWS 帳戶 組織中任何的替代聯絡人](#)。

主題

- [電話號碼和電子郵件地址需求](#)
- [更新獨立的替代聯絡人 AWS 帳戶](#)

- [更新 AWS 帳戶 組織中任何 的替代聯絡人](#)
- [account : AlternateContactTypes 內容索引鍵](#)

電話號碼和電子郵件地址需求

在您繼續更新帳戶的替代聯絡人資訊之前，我們建議您在輸入電話號碼和電子郵件地址時先檢閱下列要求。

- 電話號碼只能包含數字、空格和下列字元："+-()"。
- 電子郵件地址的長度上限為 254 個字元，除了標準英數字元之外，還可以在電子郵件地址的本機部分包含下列特殊字元："+=.#!&-_"。

更新獨立的替代聯絡人 AWS 帳戶

若要新增或編輯獨立的替代聯絡人 AWS 帳戶，請執行下列程序中的步驟。下列 AWS 管理主控台程序一律僅適用於獨立內容。您可以使用 AWS 管理主控台 來存取或僅變更您用來呼叫 操作之帳戶中的替代聯絡人。

AWS 管理主控台

新增或編輯獨立的替代聯絡人 AWS 帳戶

最低許可

若要執行下列步驟，您至少必須擁有下列 IAM 許可：

- `account:GetAlternateContact`（查看替代聯絡詳細資訊）
- `account:PutAlternateContact`（設定或更新替代聯絡人）
- `account>DeleteAlternateContact`（刪除替代聯絡人）

1. 以具有最低許可的 IAM 使用者或角色[AWS 管理主控台](#)身分登入。
2. 選擇視窗右上角的帳戶名稱，然後選擇帳戶。
3. 在[帳戶頁面上](#)，向下捲動至替代聯絡人，然後在標題右側選擇編輯。

Note

如果您沒有看到編輯選項，則可能不是以您帳戶的根使用者或先前指定最低許可的人員身分登入。

- 變更任何可用欄位中的值。

Important

對於企業 AWS 帳戶，最佳實務是輸入公司電話號碼和電子郵件地址，而不是屬於個人的電話號碼和電子郵件地址。

- 完成所有變更後，請選擇更新。

AWS CLI & SDKs

您可以使用下列 AWS CLI 命令或其 AWS SDK 對等操作來擷取、更新或刪除替代聯絡資訊：

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

備註

- 若要針對成員帳戶從管理帳戶或組織中的委派管理員帳戶執行這些操作，您必須[啟用帳戶服務的信任存取](#)。

最低許可

對於每個操作，您必須擁有映射至該操作的許可：

- `GetAlternateContact`（查看替代聯絡詳細資訊）
- `PutAlternateContact`（設定或更新替代聯絡人）

- `DeleteAlternateContact` (刪除替代聯絡人)

如果您使用這些個別許可，您可以授予某些使用者僅讀取聯絡資訊的能力，並授予其他人同時讀取和寫入的能力。

Example

下列範例會擷取發起人帳戶的目前帳單替代聯絡人。

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

Example

下列範例會為發起人帳戶設定新的操作替代聯絡人。

```
$ 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"
```

此命令如果成功就不會產生輸出。

Example

Note

如果您對相同 AWS 帳戶 和相同的聯絡類型執行多個PutAlternateContact操作，則第一個 會新增新的聯絡案例，並且所有連續呼叫相同的 AWS 帳戶 和聯絡類型會更新現有的聯絡案例。

Example

下列範例會刪除發起人帳戶的安全替代聯絡人。

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

此命令如果成功就不會產生輸出。

Note

如果您嘗試多次刪除相同的聯絡人，第一個聯絡人會以無提示的方式成功。所有稍後的嘗試都會產生ResourceNotFound例外狀況。

更新 AWS 帳戶 組織中任何 的替代聯絡人

若要新增或編輯 AWS 帳戶 組織中任何 的替代聯絡人詳細資訊，請執行下列程序中的步驟。

要求

若要使用 AWS Organizations 主控台更新替代聯絡人，您需要執行一些初步設定：

- 您的組織必須啟用所有功能，才能管理成員帳戶的設定。這可讓管理員控制成員帳戶。這會在您建立組織時預設為 。如果您的組織設定為僅合併帳單，且您想要啟用所有功能，請參閱[啟用組織的所有功能](#)。
- 您需要為 AWS 帳戶管理服務啟用受信任存取。若要設定此項目，請參閱 [啟用 AWS 帳戶管理的受信任存取](#)。

 Note

AWS Organizations 受管政策 `AWSOrganizationsReadOnlyAccess` 或 `AWSOrganizationsFullAccess` 已更新，以提供存取 AWS 帳戶管理 APIs 許可，以便您可以從主控台存取帳戶資料 AWS Organizations。若要檢視更新的 受管政策，請參閱 [Organizations AWS 受管政策的更新](#)。

AWS 管理主控台

新增或編輯 AWS 帳戶 組織中任何 的替代聯絡人

1. 使用組織的管理帳戶登入資料登入 [AWS Organizations 主控台](#)。
2. 從 中 AWS 帳戶，選取要更新的帳戶。
3. 選擇聯絡資訊，然後在替代聯絡人下，找到聯絡人類型：帳單聯絡人、安全聯絡人或營運聯絡人。
4. 若要新增聯絡人，請選取新增，或選取編輯以更新現有聯絡人。
5. 變更任何可用欄位中的值。

 Important

對於企業 AWS 帳戶，最佳實務是輸入公司電話號碼和電子郵件地址，而不是屬於個人的電話號碼和電子郵件地址。

6. 完成所有變更後，請選擇更新。

AWS CLI & SDKs

您可以使用下列 AWS CLI 命令或其 AWS SDK 對等操作來擷取、更新或刪除替代聯絡資訊：

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

備註

- 若要針對成員帳戶從管理帳戶或組織中的委派管理員帳戶執行這些操作，您必須[啟用帳戶服務的信任存取](#)。
- 您無法存取與您用來呼叫 操作的 不同組織中的帳戶。

最低許可

對於每個操作，您必須擁有映射至該操作的許可：

- `GetAlternateContact` (查看替代聯絡詳細資訊)
- `PutAlternateContact` (設定或更新替代聯絡人)
- `DeleteAlternateContact` (刪除替代聯絡人)

如果您使用這些個別許可，您可以授予某些使用者僅讀取聯絡資訊的能力，並授予其他人同時讀取和寫入的能力。

Example

下列範例會擷取組織中發起人帳戶的目前帳單替代聯絡人。使用的登入資料必須來自組織的管理帳戶，或來自帳戶管理的委派管理員帳戶。

```
$ aws account get-alternate-contact \
  --alternate-contact-type=BILLING \
  --account-id 123456789012
{
  "AlternateContact": {
    "AlternateContactType": "BILLING",
    "EmailAddress": "saanvi.sarkar@amazon.com",
    "Name": "Saarvi Sarkar",
    "PhoneNumber": "+1(206)555-0123",
    "Title": "CF0"
  }
}
```

Example

下列範例會為組織中指定的成員帳戶設定操作替代聯絡人。使用的登入資料必須來自組織的管理帳戶，或來自帳戶管理的委派管理員帳戶。

```
$ 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"
```

此命令如果成功就不會產生輸出。

Note

如果您對相同 AWS 帳戶 和相同的聯絡類型執行多個PutAlternateContact操作，則第一個 會新增新的聯絡案例，並且所有連續呼叫相同的 AWS 帳戶 和聯絡類型會更新現有的聯絡案例。

Example

下列範例會刪除組織中指定成員帳戶的安全替代聯絡人。使用的登入資料必須來自組織的管理帳戶，或來自帳戶管理的委派管理員帳戶。

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

此命令如果成功就不會產生輸出。

Example

Note

如果您嘗試多次刪除相同的聯絡人，第一個聯絡人會以無提示的方式成功。所有稍後的嘗試都會產生ResourceNotFound例外狀況。

account : AlternateContactTypes 內容索引鍵

您可以使用內容索引鍵 `account:AlternateContactTypes` 來指定 IAM 政策允許（或拒絕）三種聯絡類型中的哪一種。例如，下列範例 IAM 許可政策使用此條件金鑰，允許連接的委託人擷取，但不能修改組織中特定帳戶的 BILLING 替代聯絡人。

由於 `account:AlternateContactTypes` 是多值字串類型，您必須使用 [ForAnyValue](#) 或 [ForAllValues](#) 多值字串運算子。

更新 的主要聯絡人 AWS 帳戶

這些指示旨在說明 AWS 帳戶 如果您 AWS 使用註冊 AWS（進階）註冊或啟用帳戶的進階功能，如何更新 的主要聯絡人。若要比較註冊選項，請參閱 [比較註冊選項](#)。

您可以更新與 帳戶相關聯的主要聯絡資訊，包括聯絡人的全名、公司名稱、郵寄地址、電話號碼和網站地址。

您也可以驗證主要聯絡電話號碼。如需詳細資訊，請參閱 [驗證主要聯絡人電話號碼](#)。

根據帳戶是否為獨立帳戶或組織的一部分，您可以以不同的方式編輯主要帳戶聯絡人：

- 獨立 AWS 帳戶 – 對於 AWS 帳戶 未與組織建立關聯的，您可以使用 AWS 管理主控台或透過 CLI 和 SDKs AWS 更新您自己的主要帳戶聯絡人。若要了解如何執行此操作，請參閱 [更新獨立 AWS 帳戶 主要聯絡人](#)。
- 在 AWS 帳戶 組織內 – 對於屬於 AWS 組織的成員帳戶，管理帳戶或委派管理員帳戶中的使用者可以從 AWS Organizations 主控台集中更新組織中的任何成員帳戶，或透過 CLI 和 SDKs AWS 以程式設計方式更新。若要了解如何執行此操作，請參閱 [更新組織中 AWS 帳戶 的主要聯絡人](#)。

主題

- [電話號碼和電子郵件地址需求](#)
- [更新獨立 AWS 帳戶 或管理帳戶的主要聯絡人](#)
- [更新組織中任何 AWS 成員帳戶的主要聯絡人](#)
- [驗證主要聯絡人電話號碼](#)

電話號碼和電子郵件地址需求

在您繼續更新帳戶的主要聯絡資訊之前，我們建議您在輸入電話號碼和電子郵件地址時先檢閱下列要求。

- 電話號碼應只包含數字。
- 電話號碼必須以 + 和國家/地區代碼開頭，且國家/地區代碼後面不得有任何前導零或其他空格。例如，+1（美國/加拿大）或 +44（英國）。
- 電話號碼不得在區域碼、交換碼和本機碼之間包含空格。例如，+12025550179。
- 基於安全考量，電話號碼必須能夠從接收簡訊 AWS。由於大多數不支援 SMS，因此不接受免付費電話號碼。
- 對於企業 AWS 帳戶，最佳實務是輸入公司電話號碼和電子郵件地址，而不是屬於個人的電話號碼和電子郵件地址。使用個人的電子郵件地址或電話號碼設定帳戶的[根使用者](#)，可能會讓您的帳戶在個人離開公司時難以復原。

更新獨立 AWS 帳戶 或管理帳戶的主要聯絡人

若要編輯獨立 AWS 帳戶 或管理帳戶的主要聯絡人詳細資訊，請執行下列程序中的步驟。下列 AWS 管理主控台 程序一律僅適用於獨立內容。您可以使用 AWS 管理主控台 來存取或僅變更您用來呼叫 操作之帳戶的主要聯絡資訊。

AWS 管理主控台

編輯獨立 AWS 帳戶 或管理帳戶的主要聯絡人

最低許可

若要執行下列步驟，您至少必須擁有下列 IAM 許可：

- `account:GetContactInformation`（查看主要聯絡人詳細資訊）
- `account:PutContactInformation`（更新主要聯絡人詳細資訊）

1. 以具有最低許可的 IAM 使用者或角色[AWS 管理主控台](#)身分登入。
2. 選擇視窗右上角的帳戶名稱，然後選擇帳戶。
3. 向下捲動至聯絡資訊區段，然後選擇編輯。
4. 變更任何可用欄位中的值。
5. 完成所有變更後，請選擇更新。

AWS CLI & SDKs

您可以使用下列 AWS CLI 命令或其 AWS SDK 對等操作來擷取、更新或刪除主要聯絡資訊：

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

備註

- 若要針對成員帳戶從管理帳戶或組織中的委派管理員帳戶執行這些操作，您必須[啟用帳戶服務的信任存取](#)。

最低許可

對於每個操作，您必須擁有映射到該操作的許可：

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

如果您使用這些個別許可，您可以授予某些使用者僅讀取聯絡資訊的能力，並授予其他人同時讀取和寫入的能力。

Example

下列範例會擷取發起人帳戶的目前主要聯絡資訊。

```
$ 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

下列範例會設定發起人帳戶的新主要聯絡資訊。

```
$ 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"}'
```

此命令如果成功就不會產生輸出。

更新組織中任何 AWS 成員帳戶的主要聯絡人

若要編輯組織中任何 AWS 成員帳戶中的主要聯絡人詳細資訊，請執行下列程序的步驟。

其他需求

若要更新與 AWS Organizations 主控台的主要聯絡人，您需要執行一些初步設定：

- 您的組織必須啟用所有功能，才能管理成員帳戶的設定。這可讓管理員控制成員帳戶。這會在您建立組織時預設為。如果您的組織設定為僅合併帳單，且您想要啟用所有功能，請參閱[啟用組織的所有功能](#)。
- 您需要為 AWS 帳戶管理服務啟用受信任存取。若要設定此項目，請參閱[啟用 AWS 帳戶管理的受信任存取](#)。

AWS 管理主控台

編輯組織中任何的主要聯絡人 AWS 帳戶

1. 使用組織的管理帳戶登入資料登入[AWS Organizations 主控台](#)。
2. 從 AWS 帳戶中選取您要更新的帳戶。
3. 選擇聯絡資訊，然後尋找主要聯絡人。
4. 選擇 Edit (編輯)。

5. 變更任何可用欄位中的值。
6. 完成所有變更後，請選擇儲存。

如果您變更電話號碼，當您選擇儲存時，我們會將驗證碼傳送至新號碼。您可以立即或稍後驗證號碼。如需詳細資訊，請參閱[驗證組織中成員帳戶的電話號碼](#)。

AWS CLI & SDKs

您可以使用下列 AWS CLI 命令或其 AWS SDK 對等操作來擷取、更新或刪除主要聯絡資訊：

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

備註

- 若要針對成員帳戶從管理帳戶或組織中的委派管理員帳戶執行這些操作，您必須[啟用帳戶服務的信任存取](#)。
- 您無法存取與您用來呼叫 操作的 不同組織中的帳戶。

最低許可

對於每個操作，您必須擁有映射到該操作的許可：

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

如果您使用這些個別許可，您可以授予某些使用者僅讀取聯絡資訊的能力，並授予其他人同時讀取和寫入的能力。

Example

下列範例會擷取組織中指定成員帳戶的目前主要聯絡資訊。使用的登入資料必須來自組織的管理帳戶，或來自帳戶管理的委派管理員帳戶。

```
$ 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

下列範例會設定組織中指定成員帳戶的主要聯絡資訊。使用的登入資料必須來自組織的管理帳戶，或來自帳戶管理的委派管理員帳戶。

```
$ 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"}'
```

此命令如果成功就不會產生輸出。

驗證主要聯絡人電話號碼

您可以在 的主要聯絡資訊中驗證電話號碼 AWS 帳戶。確認檔案中的電話號碼可以接收來自我們的簡訊。

當您開始驗證時，我們會透過 SMS 文字訊息將 6 位數驗證碼傳送至帳戶目前存檔的電話號碼。您不會輸入電話號碼來開始驗證。若要完成，請在程式碼過期之前輸入程式碼。

驗證電話號碼時，請記住下列事項：

- 程式碼會在我們傳送後 5 分鐘過期。
- 如果您請求新的程式碼，先前傳送的程式碼將無法再運作。

- 如果程式碼不正確或已過期，請請求新的程式碼，然後再試一次。
- 如果電話號碼在我們傳送代碼後變更，您就無法使用該代碼。請求目前號碼的新代碼。
- 驗證狀態一律會描述目前存檔的電話號碼。如果您變更電話號碼，狀態會說明新號碼。
- 對於組織中的成員帳戶，代碼會前往成員帳戶的主要聯絡電話號碼，而不是您的聯絡電話號碼。開始之前，請確定您可以從擁有該電話的任何人取得程式碼。

若要檢查驗證狀態，請使用 [GetContactInformation](#) 操作。回應中的 `VerificationStatus` 欄位具有下列其中一個值：

- VERIFIED – 已驗證檔案中的電話號碼。
- UNVERIFIED – 檔案上的電話號碼未驗證。
- NOT_SUPPORTED – 電話號碼驗證不適用於此帳戶。

驗證獨立或管理的電話號碼 AWS 帳戶

若要驗證您使用其登入資料的帳戶電話號碼，請使用下列 AWS CLI 命令或其 AWS SDK 對等操作：

- [SendPhoneNumberVerification](#)
- [VerifyPhoneNumber](#)

最低許可

對於每個操作，您必須擁有映射到該操作的許可：

- `account:SendPhoneNumberVerification`
- `account:VerifyPhoneNumber`

若要檢查驗證狀態，您也需要 `account:GetContactInformation`。

Example

下列 AWS CLI 範例會將驗證碼傳送至發起人帳戶的主要聯絡電話號碼：

```
$ aws account send-phone-number-verification  
{
```

```
"Status": "PENDING"
}
```

Example

下列 AWS CLI 範例會提交程式碼以完成驗證：

```
$ aws account verify-phone-number --otp 123456
{
  "Status": "VERIFIED"
}
```

Example

下列 AWS CLI 範例會擷取發起人主要聯絡電話號碼的驗證狀態：

```
$ aws account get-contact-information --query VerificationStatus
"VERIFIED"
```

驗證組織中成員帳戶的電話號碼

您可以使用 主控台 AWS CLI、或 AWS SDK 驗證成員帳戶 AWS Organizations 的電話號碼。開始之前，請先完成 中的步驟[其他需求](#)。

AWS 管理主控台

驗證成員帳戶的主要聯絡電話號碼

最低許可

若要執行下列步驟，您至少必須擁有下列 IAM 許可：

- `account:GetContactInformation` (查看電話號碼以及是否已驗證)
- `account:SendPhoneNumberVerification` (傳送驗證碼)
- `account:VerifyPhoneNumber` (提交程式碼)

`AWSOrganizationsFullAccess` 受管政策不包含 `account:SendPhoneNumberVerification` 或 `account:VerifyPhoneNumber`。如果您依賴該政策，請分別授予這些許可。

1. 使用組織的管理帳戶登入資料登入[AWS Organizations 主控台](#)。
2. 從 AWS 帳戶中選取成員帳戶。
3. 選擇聯絡資訊，然後尋找主要聯絡人。
4. 如果電話號碼未驗證，則會顯示警告。選擇電話號碼，然後選擇驗證電話號碼。我們會傳送 6 位數代碼到成員帳戶的電話號碼。
5. 在驗證碼中輸入程式碼，然後選擇驗證。

如果程式碼未送達，請在此選項可用時選擇重新傳送程式碼。

AWS CLI & SDKs

若要驗證成員帳戶的電話號碼，請使用下列 AWS CLI 命令或其 AWS SDK 對等操作，並指定成員帳戶 ID：

- [SendPhoneNumberVerification](#)
- [VerifyPhoneNumber](#)

備註

- 您使用的登入資料必須來自組織的管理帳戶或 AWS 帳戶管理的委派管理員帳戶。
- 您無法存取與您用來呼叫 操作的 不同組織中的帳戶。

最低許可

對於每個操作，您必須擁有映射到該操作的許可：

- `account:SendPhoneNumberVerification`
- `account:VerifyPhoneNumber`

若要檢查驗證狀態，您也需要 `account:GetContactInformation`。

Example

下列 AWS CLI 範例會將驗證碼傳送至指定成員帳戶的主要聯絡電話號碼：

```
$ aws account send-phone-number-verification --account-id 123456789012
{
  "Status": "PENDING"
}
```

Example

下列 AWS CLI 範例會提交我們傳送至成員帳戶電話號碼的程式碼：

```
$ aws account verify-phone-number --account-id 123456789012 --otp 123456
{
  "Status": "VERIFIED"
}
```

檢視 AWS 帳戶 識別符

如果您 AWS 使用註冊 AWS（進階）註冊，或如果您為帳戶啟用進階功能，則此資訊與檢視 AWS 帳戶 識別符有關。若要比較註冊選項，請參閱 [比較註冊選項](#)。

AWS 會為每個 指派下列唯一識別符 AWS 帳戶：

[AWS 帳戶 ID](#)

可唯一識別的 12 位數號碼，例如 012345678901 AWS 帳戶。許多 AWS 資源在其 [Amazon Resource Name \(ARNs\)](#) 中包含帳戶 ID。帳戶 ID 部分會將一個帳戶中的資源與另一個帳戶中的資源區分開來。如果您是 AWS Identity and Access Management (IAM) 使用者，您可以使用 AWS 管理主控台 帳戶 ID 或帳戶別名登入。雖然像任何識別資訊一樣，帳戶 IDs 應該謹慎使用和共用，但不會被視為秘密、敏感或機密資訊。

[正式使用者 ID](#)

英數字元識別符，例如

79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be，它是混淆形式的 AWS 帳戶 ID。您可以在使用 Amazon Simple Storage Service (Amazon S3) 授予儲存貯體和物件的跨帳戶存取權 AWS 帳戶 時，使用此 ID 來識別。您可以將 正式使用者 ID 擷取 AWS 帳戶 為 [根使用者](#) 或 IAM 使用者。

您必須使用 進行身分驗證 AWS，才能檢視這些識別符。

⚠ Warning

請勿將您的 AWS 登入資料（包括密碼和存取金鑰）提供給需要識別 AWS 帳戶符才能與您共用 AWS 資源的第三方。這樣做可讓他們存取您擁有 AWS 帳戶的。

尋找您的 AWS 帳戶 ID

您可以使用 AWS 管理主控台 或 AWS Command Line Interface () 尋找 AWS 帳戶 ID AWS CLI。在主控台中，帳戶 ID 的位置取決於您是以根使用者還是 IAM 使用者身分登入。無論您以根使用者或 IAM 使用者身分登入，帳戶 ID 都相同。

尋找您的帳戶 ID 做為根使用者

AWS 管理主控台

以根使用者身分登入時尋找您的 AWS 帳戶 ID

i 最低許可

若要執行下列步驟，您至少必須擁有下列 IAM 許可：

- 當您以根使用者身分登入時，您不需要任何 IAM 許可。

1. 在右上角的導覽列中，選擇您的帳戶名稱或號碼，然後選擇安全登入資料。

i Tip

如果您沒有看到安全登入資料選項，您可能會以 IAM 角色的聯合身分使用者身分登入，而不是以 IAM 使用者身分登入。在此情況下，請尋找項目帳戶及其旁邊的帳戶 ID 號碼。

2. 在帳戶詳細資訊區段下，帳戶號碼會顯示在 AWS 帳戶 ID 旁。

AWS CLI & SDKs

使用 尋找您的 AWS 帳戶 ID AWS CLI

i 最低許可

若要執行下列步驟，您至少必須擁有下列 IAM 許可：

- 當您以根使用者身分執行 命令時，您不需要任何 IAM 許可。

使用 [get-caller-identity](#) 命令，如下所示。

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

將您的帳戶 ID 尋找為 IAM 使用者

AWS 管理主控台

以 IAM 使用者身分登入時尋找您的 AWS 帳戶 ID

i 最低許可

若要執行下列步驟，您至少必須擁有下列 IAM 許可：

- `account:GetAccountInformation`

1. 在右上角的導覽列中，選擇您的使用者名稱，然後選擇安全登入資料。

i Tip

如果您沒有看到安全登入資料選項，您可能會以 IAM 角色的聯合身分使用者身分登入，而不是以 IAM 使用者身分登入。在此情況下，請尋找項目帳戶及其旁邊的帳戶 ID 號碼。

2. 在頁面頂端的帳戶詳細資訊下，帳戶號碼會顯示在 AWS 帳戶 ID 旁。

AWS CLI & SDKs

使用 尋找您的 AWS 帳戶 ID AWS CLI

最低許可

若要執行下列步驟，您至少必須擁有下列 IAM 許可：

- 當您以 IAM 使用者或角色身分執行命令時，您必須具有：
 - `sts:GetCallerIdentity`

使用 [get-caller-identity](#) 命令，如下所示。

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

尋找您的正式使用者 ID AWS 帳戶

您可以使用 AWS 帳戶 AWS 管理主控台 或 尋找 的正式使用者 ID AWS CLI。的正式使用者 ID AWS 帳戶 專屬於該帳戶。您可以將 正式使用者 ID 擷取 AWS 帳戶 為根使用者、聯合身分使用者或 IAM 使用者。

尋找正式 ID 做為根使用者或 IAM 使用者

AWS 管理主控台

以根使用者或 IAM 使用者身分登入主控台時，尋找您帳戶的正式使用者 ID

最低許可

若要執行下列步驟，您至少必須擁有下列 IAM 許可：

- 當您以根使用者身分執行 命令時，您不需要任何 IAM 許可。
- 當您以 IAM 使用者身分登入時，您必須擁有：
 - `account:GetAccountInformation`

1. 以根使用者或 IAM 使用者 AWS 管理主控台 身分登入。
2. 在右上角的導覽列中，選擇您的帳戶名稱或號碼，然後選擇安全登入資料。

 Tip

如果您沒有看到安全登入資料選項，您可能會以 IAM 角色的聯合身分使用者身分登入，而不是以 IAM 使用者身分登入。在此情況下，請尋找項目帳戶及其旁邊的帳戶 ID 號碼。

3. 在帳戶詳細資訊區段下，正式使用者 ID 會出現在正式使用者 ID 旁。您可以使用正式使用者 ID 來設定 Amazon S3 存取控制清單 ACLs)。

AWS CLI & SDKs

使用 尋找正式使用者 ID AWS CLI

相同的 AWS CLI 和 API 命令適用於 AWS 帳戶根使用者、IAM 使用者或 IAM 角色。

使用 [list-buckets](#) 命令，如下所示。

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

尋找正式 ID 做為具有 IAM 角色的聯合身分使用者

AWS 管理主控台

以具有 IAM 角色的聯合身分使用者身分登入主控台時，尋找您帳戶的正式 ID

 最低許可

- 您必須具有列出和檢視 Amazon S3 儲存貯體的許可。

1. 以 IAM 角色的聯合身分使用者 AWS 管理主控台 身分登入。

2. 在 Amazon S3 主控台中，選擇儲存貯體名稱以檢視儲存貯體的詳細資訊。
3. 選擇許可索引標籤。
4. 在存取控制清單區段的儲存貯體擁有者下，AWS 帳戶 會顯示您的正式 ID。

AWS CLI & SDKs

使用 尋找正式使用者 ID AWS CLI

相同的 AWS CLI 和 API 命令適用於 AWS 帳戶根使用者、IAM 使用者或 IAM 角色。

使用 [list-buckets](#) 命令，如下所示。

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

故障診斷您的 AWS 帳戶

如果您 AWS 使用註冊 AWS（進階）AWS 帳戶註冊，或如果您為帳戶啟用進階功能，此資訊會針對您的 進行故障診斷。若要比較註冊選項，請參閱 [比較註冊選項](#)。

使用下列主題中的資訊來協助您診斷和修正的問題 AWS 帳戶。如需根使用者的說明，請參閱《IAM 使用者指南》中的對[根使用者的問題進行故障診斷](#)。如需登入程序的協助，請參閱 [《AWS 帳戶 登入使用者指南》中的對登入問題進行故障診斷](#)。AWS

故障診斷主題

- [對 AWS 帳戶 建立的問題進行故障診斷](#)
- [對 AWS 帳戶 關閉問題進行故障診斷](#)
- [對的其他問題進行故障診斷 AWS 帳戶](#)

對 AWS 帳戶 建立的問題進行故障診斷

如果您 AWS 使用註冊 AWS（進階）註冊，或如果您為帳戶啟用進階功能，則此資訊會針對 AWS 帳戶 建立問題進行疑難排解。若要比較註冊選項，請參閱 [比較註冊選項](#)。

使用下表中的參考連結，協助您診斷和修正建立新的問題 AWS 帳戶。

問題	參考連結	來源
我不知道如何註冊或建立 帳戶	註冊 AWS (進階)	本指南
如果我沒有收到來自 的通話 AWS 來驗證我的新帳戶或我輸入的 PIN 碼無效，該怎麼辦？	https://repost.aws/knowledge-center/phone-verify-no-call	AWS re:Post
當我嘗試 AWS 帳戶 透過電話 驗證我的 時，如何解決「失敗 嘗試次數上限」錯誤？	https://repost.aws/knowledge-center/maximum-failed-attempts	AWS re:Post
已超過 24 小時且未啟用我的 帳戶	https://repost.aws/knowledge-center/create-and-activate-aws-account	AWS re:Post
新帳戶建立後就無法登入	https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html	AWS 登入使用者指南

如需其他協助，建議您[AWS re:Post](#)搜尋與特定問題相關的內容。如果您仍然需要協助，請聯絡 [AWS 支援](#)。

對 AWS 帳戶 關閉問題進行故障診斷

此資訊是關於使用 AWS 註冊 AWS (進階) 註冊或啟用帳戶的進階功能時，AWS 帳戶 對關閉問題進行故障診斷。若要比較註冊選項，請參閱 [比較註冊選項](#)。

使用以下資訊來協助您診斷和修正帳戶關閉程序期間發現的常見問題。如需帳戶關閉程序的一般資訊，請參閱 [關閉 AWS 帳戶](#)。

主題

- [我不知道如何刪除或取消我的 帳戶](#)
- [我在帳戶頁面上看不到關閉帳戶按鈕](#)
- [我已關閉我的帳戶，但仍未收到電子郵件確認](#)

- [我在嘗試關閉我的帳戶時收到「ConstraintViolationException」錯誤](#)
- [我在嘗試關閉成員帳戶時收到「CLOSE_ACCOUNT_QUOTA_EXCEEDED」錯誤](#)
- [在關閉管理帳戶之前，是否需要刪除我的 AWS 組織？](#)

我不知道如何刪除或取消我的 帳戶

若要關閉您的帳戶，請遵循 中的指示[關閉 AWS 帳戶](#)。

我在帳戶頁面上看不到關閉帳戶按鈕

如果您不是以根使用者身分登入，則不會在帳戶頁面上看到關閉帳戶按鈕。您必須[以根使用者 AWS 管理主控台 身分登入](#)，才能關閉您的帳戶。如果您無法登入，請參閱[對根使用者的問題進行故障診斷](#)。

我已關閉我的帳戶，但仍未收到電子郵件確認

此確認電子郵件只會傳送至 的根使用者電子郵件地址 AWS 帳戶。如果您在幾個小時內沒有收到此電子郵件，您可以[以根使用者的 AWS 管理主控台 身分登入](#)，以檢查您的帳戶是否已關閉。如果您的帳戶已成功關閉，您會看到顯示的訊息，指出您的帳戶已關閉。如果您關閉的帳戶是成員帳戶，您可以透過檢查已關閉的帳戶是否在 AWS Organizations 主控台CLOSED中標記為 來驗證成功關閉。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[關閉組織中的成員帳戶](#)。

如果您嘗試關閉管理帳戶，但未收到有關帳戶關閉的電子郵件確認，您的組織很可能有作用中的成員帳戶。只有在您的組織沒有任何作用中的成員帳戶時，才能關閉管理帳戶。若要驗證組織中沒有剩餘的作用中成員帳戶，請前往 AWS Organizations 主控台，並確認其帳戶名稱Closed旁顯示所有成員帳戶。之後，您可以關閉管理帳戶。

我在嘗試關閉我的帳戶時收到「ConstraintViolationException」錯誤

您正在嘗試使用 AWS Organizations 主控台關閉管理帳戶，這是不可能的。若要關閉管理帳戶，您需要以管理帳戶的[根使用者 AWS 管理主控台 身分登入](#)，並從帳戶頁面將其關閉。如需詳細資訊，請參閱AWS Organizations 《使用者指南》[中的關閉組織中的管理帳戶](#)。

我在嘗試關閉成員帳戶時收到「CLOSE_ACCOUNT_QUOTA_EXCEEDED」錯誤

您只能在滾動的 30 天內關閉 20% 的成員帳戶。此配額不受日曆月的約束，而是在您關閉帳戶時開始計算。在初始帳戶關閉的 30 天內，您無法超過 20% 的帳戶關閉限制。帳戶關閉下限為 250，帳戶關閉上限為 1000，即使 20% 的帳戶超過 1000。如需 Organizations 配額的詳細資訊，請參閱AWS Organizations 《使用者指南》中的 [的配額 AWS Organizations](#)。

在關閉管理帳戶之前，是否需要刪除我的 AWS 組織？

否，您不需要在關閉管理帳戶之前刪除您的 AWS 組織。不過，只有在您的組織沒有任何作用中的成員帳戶時，您才能關閉管理帳戶。若要驗證組織中沒有剩餘的作用中成員帳戶，請前往 AWS Organizations 主控台，並確認其帳戶名稱 Closed 旁顯示所有成員帳戶。之後，您可以關閉管理帳戶。

對的其他問題進行故障診斷 AWS 帳戶

如果您 AWS 使用註冊 AWS（進階）註冊 AWS 帳戶，或如果您為帳戶啟用進階功能，則此資訊與疑難排解的其他問題有關。若要比較註冊選項，請參閱 [比較註冊選項](#)。

使用此處的資訊來協助您疑難排解與相關的問題 AWS 帳戶。

問題

- [我需要變更我的信用卡 AWS 帳戶](#)
- [我需要報告詐騙 AWS 帳戶 活動](#)
- [我需要關閉我的 AWS 帳戶](#)
- [當我更新根使用者電子郵件地址AccessDeniedException時，會收到](#)

我需要變更我的信用卡 AWS 帳戶

若要變更的信用卡 AWS 帳戶，您必須能夠登入。AWS 有適當的保護，要求您證明您是帳戶擁有者。如需說明，請參閱AWS Billing 《使用者指南》中的[管理您的信用卡付款方式](#)。

我需要報告詐騙 AWS 帳戶 活動

如果您懷疑詐騙活動使用您的 AWS 帳戶 並想要進行報告，請參閱[如何報告資源濫用 AWS](#)。

如果您在 Amazon.com 上進行購買時遇到問題，請參閱 [Amazon 客戶服務](#)。

我需要關閉我的 AWS 帳戶

如需針對關閉的問題進行故障診斷的說明 AWS 帳戶，請參閱 [關閉 AWS 帳戶](#)。

當我更新根使用者電子郵件地址AccessDeniedException時，會收到

如果成員帳戶是專案帳戶，則無法更新其根使用者電子郵件地址。AWS Builder ID 擁有每個專案帳戶，而不是根使用者電子郵件地址。如需詳細資訊，請參閱[啟用進階功能之後的專案帳戶](#)。

管理印度的帳戶

如果您 AWS 使用註冊 AWS（進階）註冊，或啟用帳戶的進階功能，則此資訊與管理印度的帳戶有關。若要比較註冊選項，請參閱 [比較註冊選項](#)。

如果您註冊新的 AWS 帳戶，並為您的聯絡地址和帳單地址選擇印度，您的使用者協議是與 AWS Amazon Web Services India Private Limited (AWS India) 簽訂的。印度 AWS 管理您的帳單，您的發票總計以印度盧比 (INR) 而非美元 (USD) 列出。如需管理的資訊 AWS 帳戶，請參閱 [設定您的 AWS 帳戶](#)。

如果您的帳戶位於 AWS 印度，請遵循本主題中的程序來管理您的帳戶。本主題說明如何註冊 AWS 印度帳戶、編輯有關 AWS 印度帳戶的資訊、管理客戶驗證，以及新增或編輯您的永久帳戶號碼 (PAN)。

作為註冊期間信用卡驗證的一部分，AWS 印度會向您的信用卡收取 2 盧比的費用。AWS 印度會在驗證完成後退款 2 盧比。在驗證過程中您可能會跳轉至您的銀行。

主題

- [AWS 帳戶 使用 AWS 印度建立](#)
- [管理您的客戶驗證資訊](#)

AWS 帳戶 使用 AWS 印度建立

AWS 印度是印度 AWS 的本地賣方。如果您的聯絡人和帳單地址位於印度，而且您想要建立帳戶，請使用下列程序註冊 AWS 印度帳戶。

註冊 AWS 印度帳戶

1. 開啟 [Amazon Web Services 首頁](#)。
2. 選擇建立 AWS 帳戶。

Note

如果您 AWS 最近登入，該選項可能不存在。反之，選擇登入主控台。如果仍然看不到建立新 AWS 帳戶帳戶，請選擇登入不同的帳戶，然後選擇建立新 AWS 帳戶帳戶。

3. 輸入您的帳戶資訊、驗證您的電子郵件地址，並為您的帳戶選擇高強度密碼。
4. 選擇商務或個人。個人帳戶和企業帳戶具有相同的特性和功能。

5. 輸入您的公司或個人聯絡資訊。如果您的聯絡地址或帳單地址位於印度，且符合印度電腦緊急應變團隊 (CERT-In) 法規，AWS 則必須先收集並驗證您的身分資訊，才能授予您 AWS 服務的存取權。

您在聯絡或帳單資訊之間選擇的名稱，必須與計劃用於客戶驗證的文件上顯示的名稱完全相符。例如，如果您計劃使用公司註冊憑證來驗證企業帳戶，您必須提供文件上顯示的商業名稱。如需接受的證件類型清單，請參閱[the section called “用於客戶驗證的可接受印度證件”](#)。

6. 閱讀客戶協議後，選取條款和條件核取方塊，然後選擇繼續。
7. 在帳單資訊頁面上，輸入您要使用的付款方式。在驗證過程中您必須提供您的 CVV。
8. 在您是否有 PAN？下，如果您有想要顯示在稅務發票上的永久帳戶號碼 (PAN)，請選擇是，然後輸入您的 PAN。如果您沒有 PAN 或想要在註冊後新增，請選擇否。
9. 選擇驗證並繼續。AWS 印度會在驗證程序中向您的卡片收取 2 盧比的費用。AWS 印度會在驗證完成後退款 2 盧比。
10. 在確認您的身分頁面上，選取帳戶註冊的主要用途。
11. 選擇最能代表帳戶擁有者的所有權類型。如果您選擇公司、組織或合作夥伴關係做為所有權類型，請輸入關鍵管理人員的名稱。主要管理人員可以是主管、營運主管，或負責業務營運的人員。
12. 根據您選擇的所有權類型，選擇要用於驗證的已接受印度文件類型，並輸入您的文件資訊。

 Note

如果您有個人帳戶，並打算使用不是由印度聯發行的駕照，我們建議您使用不同的個人文件類型進行驗證。

13. 選擇您要用於客戶驗證的名稱。

如果帳單名稱和聯絡資訊與印度地址相關聯，則會顯示這些名稱以供選擇。請確定您選擇的名稱符合您計劃用於客戶驗證的文件類型名稱。如果您需要變更與帳單或聯絡地址相關聯的名稱，您可以在完成帳戶註冊後進行變更。

14. 同意提交資訊以供驗證，然後選擇繼續。

完成帳戶註冊後，系統會透過電子郵件通知您客戶驗證結果。您也可以在此帳戶設定中的客戶驗證頁面上或稍後 AWS 的運作狀態儀表板中檢查狀態。您必須通過客戶驗證才能存取 AWS 服務。

15. 選擇您要透過簡訊 (SMS) 或語音通話來驗證您的行動電話號碼。
16. 選取您的國家或地區代碼，然後輸入您的行動電話號碼。
17. 完成安全檢查。

18. 選擇傳送簡訊或立即呼叫我。幾分鐘後，您會在簡訊中收到四位數的 PIN 碼，或在行動電話上收到自動通話。
19. 在確認您的身分頁面上，輸入您收到的 PIN 碼，然後選擇繼續。
20. 在選取支援計劃頁面上，選取您的支援計劃，然後選擇完成註冊。驗證您的付款方式和客戶驗證後，您的帳戶將會啟用，而且您會收到一封電子郵件，確認啟用您的帳戶。

Note

如果您已完成客戶驗證，並編輯先前用於驗證身分的名稱、地址或文件，您可能需要再次更新並完成客戶驗證。如需詳細資訊，請參閱[the section called “編輯您的客戶驗證資訊”](#)。

管理您的客戶驗證資訊

為了符合印度電腦緊急回應團隊 (CERT-In) 法規，AWS 在授予您新的或繼續存取 AWS 服務之前，需要收集並驗證您的身分資訊。您的身分必須使用您提供的印度帳單或聯絡地址中的名稱進行驗證。在驗證期間，AWS 將檢查文件號碼是否有效，以及您提供的名稱是否與您用於客戶驗證的文件相關聯的名稱相符。您在聯絡或帳單資訊之間選擇的名稱必須與文件上顯示的名稱完全相符。

若要更新您的帳單名稱和地址，請參閱[付款偏好設定](#)頁面。若要更新您的聯絡人姓名和地址，請參閱[the section called “更新的主要聯絡人 AWS 帳戶”](#)。如果您編輯先前用於客戶驗證的任何資訊，例如帳單或聯絡資訊中的名稱或印度地址，您可能需要更新並重新提交客戶驗證資訊。

檢查您的客戶驗證狀態

您可以隨時在客戶驗證頁面上檢視您的客戶驗證狀態。如果您的驗證狀態為需要驗證或驗證失敗，請建立或更新客戶驗證資訊並提交以進行驗證。

如果您的管理帳戶已啟用客戶驗證繼承，則帳戶的驗證狀態會反映該帳戶的狀態。繼承作用中時，您不需要採取任何動作。

建立您的客戶驗證資訊

若要完成客戶驗證，您需要提供已接受印度文件的資訊。如需接受的證件類型清單，請參閱[the section called “用於客戶驗證的可接受印度證件”](#)。

1. 登入 [AWS 管理主控台](#)。

2. 在導覽列的右上角，選擇您的帳戶名稱（或別名），然後選擇帳戶。
3. 在其他設定中，選擇客戶驗證。

如果您之前尚未提供客戶驗證資訊，您會看到建立客戶驗證頁面。

4. 選擇與您計劃用於客戶驗證的文件名稱完全相符的名稱。例如，如果您計劃使用公司註冊憑證來驗證企業帳戶，您必須提供文件上顯示的商業名稱。
5. 提供頁面上請求的其餘資訊。根據您選擇的文件類型，您可能需要上傳文件正面和背面的副本。如果您上傳映像檔案，請確定文件中的所有資訊都可見且清晰。
6. 選擇提交。

您將透過電子郵件或在 AWS 運作狀態儀表板上收到客戶驗證結果和任何後續步驟的通知。

編輯您的客戶驗證資訊

您可以編輯客戶驗證資訊，例如帳戶註冊的主要用途、組織類型，以及您想要用於驗證的名稱、文件類型、文件上傳或文件資訊。

如果您編輯用於客戶驗證的名稱或文件類型，或更新任何文件資訊，則必須在儲存變更時再次驗證您的身分。

驗證繼承作用中

如果您的管理帳戶已啟用客戶驗證繼承，則您無法編輯或提交自己的客戶驗證資訊。您的驗證資訊會以唯讀模式顯示。

1. 登入 [AWS 管理主控台](#)。
2. 在導覽列的右上角，選擇您的帳戶名稱（或別名），然後選擇帳戶。
3. 在其他設定中，選擇客戶驗證。
4. 選擇編輯，然後更新您要變更的資訊。

當您更新資訊時，請注意下列指引：

- 如果您選擇不同的名稱，名稱必須與計劃用於客戶驗證的文件上的名稱完全相符。例如，如果您計劃使用公司註冊憑證來驗證企業帳戶，您必須提供文件上顯示的商業名稱。
- 如果您選擇不同的文件類型，您將需要上傳文件的正反面（如適用）的副本。文件上傳中的所有資訊都應清晰可見。

- 如果您有個人帳戶，並打算使用不是由印度聯發行的駕照，我們建議您使用不同的個人文件類型進行驗證。

如需接受的證件類型清單，請參閱[the section called “用於客戶驗證的可接受印度證件”](#)。

5. 選擇提交。

如果因為儲存的變更類型而必須再次驗證您的身分，您將會透過電子郵件收到客戶驗證結果和任何後續步驟的通知。您也可以返回客戶驗證頁面或在 AWS 運作狀態儀表板中檢視結果。

管理 AWS Organizations 的客戶驗證繼承

透過 [AWS Organizations](#)，您可以為組織啟用客戶驗證繼承。當您啟用繼承時，組織中以印度為基礎的成員帳戶會繼承管理帳戶的驗證狀態。他們不需要獨立完成客戶驗證。

您的管理帳戶必須先完成自己的客戶驗證，才能啟用繼承。啟用繼承之後，您不需要重新提交驗證文件。

當您的管理帳戶啟用客戶驗證繼承時，您的驗證狀態會延伸至組織中以印度為基礎的成員帳戶。對於這些成員帳戶，我們可能會使用或揭露您的驗證資訊，以回應執法或監管請求。

啟用或停用客戶驗證繼承

使用下列程序，為組織的印度成員帳戶開啟或關閉客戶驗證繼承。

1. AWS 管理主控台 在 開啟 [AWS 管理主控台](#)。
2. 在導覽列上，選擇您的帳戶名稱（或別名），然後選擇帳戶。
3. 在其他設定中，選擇客戶驗證。
4. 在客戶驗證設定下，開啟繼承切換以啟用繼承，或關閉以停用繼承。
5. 檢閱確認對話方塊，然後確認您的選擇。

當您啟用繼承時，組織中所有以印度為基礎的成員帳戶都會繼承您的驗證狀態。當您停用繼承時，我們會還原先前已完成其驗證之成員帳戶先前的驗證狀態。沒有事先驗證的成員帳戶必須獨立完成客戶驗證。

AWS Organizations 成員帳戶的客戶驗證

如果您的帳戶有印度聯絡人或帳單地址，您會繼承管理帳戶的驗證狀態。這適用於您的管理帳戶已啟用客戶驗證繼承的情況。您可以在客戶驗證頁面上看到確認此訊息。

當繼承處於作用中狀態時，您無法提交或編輯自己的客戶驗證資訊。您不需要採取任何動作。

如果您的管理帳戶停用繼承，您必須擁有自己的客戶驗證狀態。如果您的帳戶離開組織，或管理帳戶從組織中移除您的帳戶，則同樣適用。如果您先前已提交自己的驗證資訊，我們會還原您先前的驗證狀態。您不需要重複此程序。此還原僅適用於自上次驗證以來未變更的名稱和地址。

用於客戶驗證的可接受印度證件

接受以下列印度政府核發的證件類型進行客戶驗證。

Note

下列連結可能由政府變更。

- **PAN 卡** - 提供數位和實體格式，永久帳號 (PAN) 卡包含由印度稅務局核發給個人、公司和實體的唯一英數字元識別符。PAN 有十個字元，包括英文字母和數字，格式為 **AAAAA1111A**。若要使用此文件進行驗證，您還必須提供出現在 PAN 文件上的出生日期（個人）或成立日期（商業），並上傳卡片正面。您可以前往[收入稅部門的官方網站](#)，檢查 PAN 的有效性。
- **選民身分證/EPIC** - 選民身分證，也稱為選舉人照片身分證 (EPIC)，包含由印度選舉委員會核發給印度合格選民的唯一身分證號碼。選民 ID/EPIC 號碼包含十個字元，包括字母和數字。您可以前往[印度選舉委員會](#)的官方網站，檢查選民 ID 的有效性。若要使用此文件進行驗證，您必須同時上傳卡片的正面和背面。
- **駕照** - 如果您的駕照不是由印度聯邦核發，我們建議您使用不同的文件類型進行驗證。駕照號碼包含 12-16 個字元，包括字母、數字和空格或連字號。若要使用此文件進行驗證，您必須提供您的出生日期，並上傳卡片的正面和背面。您可以前往道路運輸和高速公路部的 [Parivahan Sewa 網站](#)，檢查駕照的有效性。
- **公司註冊憑證** - 公司註冊憑證是由公司事務部 (MCA) 發行的文件，該文件將企業註冊為法人實體。憑證用於唯一識別和追蹤在印度註冊的公司。每個憑證都包含企業識別號碼 (CIN)，這是由 21 個字元組成的唯一英數識別符，包括字母和數字。若要使用此文件進行驗證，您必須上傳公司註冊憑證文件。您可以前往[公司事務部入口網站](#)，檢查 CIN 的有效性。

個人和企業帳戶接受不同的印度證件類型：

- 對於個人帳戶 - PAN 卡、選民 ID 卡/EPIC 和駕照。
- 對於商業帳戶 - PAN 卡和公司註冊憑證。

管理您的 AWS 印度帳戶

除了下列任務之外，管理您帳戶的程序與在印度以外建立的帳戶相同。如需管理帳戶的一般資訊，請參閱 [the section called “設定您的帳戶”](#)。

使用 AWS 管理主控台 執行下列任務：

- [新增或編輯永久帳號](#)
- [編輯多個永久帳戶號碼](#)
- [the section called “管理您的客戶驗證資訊”](#)
- [編輯多個商品和服務稅號 \(GSTs\)](#)
- [檢視稅務發票](#)

關閉 AWS 帳戶

這些指示說明如何 AWS 帳戶 在使用 AWS 註冊 AWS（進階）註冊，或啟用帳戶的進階功能時關閉您的。若要比較註冊選項，請參閱 [比較註冊選項](#)。

如果您不再需要您的 AWS 帳戶，您可以隨時按照本節中的指示將其關閉。關閉帳戶後，您可以在關閉帳戶的 90 天內重新開啟它。您關閉帳戶當天到永久 AWS 關閉帳戶的期間稱為[關閉後期間](#)。

關閉帳戶之前您需要知道什麼

關閉您的 之前 AWS 帳戶，您應該考慮下列事項：

- 關閉您的帳戶將做為您終止此帳戶客戶 AWS 協議的通知。
- 您不需要先刪除 中的資源，AWS 帳戶 再關閉資源。不過，我們建議您備份任何要保留的資源或資料。如需有關如何備份特定資源的說明，請參閱該服務的適當[AWS 文件](#)。
- 您可以在[關閉後期間](#)重新開啟您的帳戶。如果您重新開啟服務，保留在帳戶中的服務費用將會重新啟動。您仍需對任何未支付發票和未完成[的預留執行個體](#)和 [Savings Plans](#) 負責。
- 您仍需負責帳戶關閉前所使用服務的所有未結費用。關閉帳戶後，您將在下個月收到 AWS 帳單。例如，如果您在 1 月 15 日關閉帳戶，您將在 2 月初收到從 1 月 1 日至 1 月 15 日產生的用量帳單。關閉帳戶後，您將繼續收到[預留執行個體](#)和 [Savings Plans](#) 的發票，直到過期為止。
- 您將無法再存取您帳戶中先前可用的 AWS 服務。不過，您只能在[關閉後期間](#)登入並存取已關閉 AWS 帳戶 的，以檢視過去的帳單資訊、存取帳戶設定或聯絡 [AWS 支援](#)。

- 您無法使用與關閉 AWS 帳戶時註冊到的相同電子郵件地址，做為另一個的主要電子郵件 AWS 帳戶。如果您想要對不同的使用相同的電子郵件地址 AWS 帳戶，建議您在關閉之前更新。如需詳細資訊，請參閱[更新根使用者電子郵件地址](#)。
- 您不能使用您在關閉另一個帳戶 AWS 帳戶時向註冊的相同帳戶別名 AWS 帳戶。若要重複使用不同別名 AWS 帳戶，請先刪除帳戶別名，再關閉帳戶。如需詳細資訊，請參閱《IAM 使用者指南》中的[為您的 AWS 帳戶 ID 使用別名](#)。
- 如果您已在 AWS 帳戶根使用者上[啟用多重驗證 \(MFA\)](#)，或在 [IAM 使用者上設定 MFA 裝置](#)，則當您關閉帳戶時，不會自動移除 MFA。如果您選擇在[關閉後](#) 90 天內開啟 MFA，請保持 MFA 裝置處於作用中狀態，直到關閉後期間過期為止，以防您需要在此期間存取帳戶。請注意，在永久關閉您的帳戶之後，硬體 TOTP 字符裝置無法與其他使用者建立關聯。如果稍後想要將硬體 TOTP 字符用於其他使用者，您可以選擇在關閉帳戶之前[停用硬體 MFA 裝置](#)。[IAM 使用者](#)的 MFA 裝置必須由帳戶管理員刪除。

成員帳戶的其他考量事項

- 當您關閉成員帳戶時，該帳戶在[關閉後期間](#)之前都不會從組織中移除。在關閉後期間，已關閉的成員帳戶仍會計入您在組織中的帳戶配額。若要避免帳戶計入配額，請參閱[在關閉之前從組織移除成員帳戶](#)。
- 您只能在連續 30 天的期間內關閉 20% 或 250 個成員帳戶，最多 1,000 個，以較高者為準。此配額不受日曆月的約束，而是在您關閉帳戶時開始計算。如需 Organizations 配額的詳細資訊，請參閱[配額 AWS Organizations](#)。
- 如果您使用 AWS Control Tower，則需要在嘗試關閉帳戶之前取消管理成員帳戶。請參閱「AWS Control Tower 使用者指南」中的[取消管理成員帳戶](#)。

服務特定考量事項

- AWS Marketplace 帳戶關閉時，訂閱不會自動取消。如果您有任何訂閱，請先[終止訂閱中軟體的所有執行個體](#)。然後，前往 AWS Marketplace 主控台的[管理訂閱](#)頁面並取消您的訂閱。
- 帳戶關閉後，AWS 會每天傳送電子郵件最多五天，然後再暫停網域。網域暫停之後，根據網域的註冊商，我們會在 30 天內刪除網域，或將網域釋出給其註冊商。如需詳細資訊，請參閱[我的 AWS 帳戶已關閉或永久關閉，且我的網域已向 Route 53 註冊](#)。

如果此帳戶根使用者的電子郵件地址使用此相同帳戶中透過 Route 53 註冊的網域，在完成下列其中一個動作之前，請勿關閉此帳戶：將網域轉移到不同的 AWS 帳戶，或更新根使用者電子郵件地址以使用未在此帳戶中註冊的網域。否則，關閉帳戶會暫停網域，這會中斷電子郵件交付到您的根使用者

地址。如果沒有電子郵件，您無法復原帳戶，如果沒有帳戶，則無法恢復網域。30 天後，Route 53 會永久刪除網域。這也適用於其根使用者電子郵件地址使用在此帳戶中註冊網域的成員帳戶。

- AWS CloudTrail 是基礎安全服務。這表示即使 AWS 帳戶 關閉，使用者建立的線索仍可繼續存在並交付事件，除非使用者在關閉線索 AWS 帳戶 之前明確刪除其中的線索。如需如何在關閉 AWS 帳戶 後請求刪除線索的詳細資訊，請參閱 CloudTrail 使用者指南中的[AWS 帳戶 關閉和線索](#)。

如何關閉您的帳戶

您可以使用 AWS 帳戶 下列程序關閉您的。請注意，根據您要關閉的帳戶類型【獨立、成員、管理和 AWS GovCloud (US)】，每個索引標籤都有不同的指引。

如果您在關閉帳戶的過程中遇到任何問題，請參閱 [對 AWS 帳戶 關閉問題進行故障診斷](#)。

Standalone account

獨立帳戶是不屬於 的個別受管帳戶 AWS Organizations。

從帳戶頁面關閉獨立帳戶

1. 以 AWS 帳戶 您要關閉的 中的[根使用者 AWS 管理主控台 身分登入](#)。以 IAM 使用者或角色身分登入時，您無法關閉帳戶。
2. 在右上角的導覽列上，選擇您的帳戶名稱或號碼，然後選擇帳戶。
3. 在[帳戶頁面上](#)，選擇關閉帳戶按鈕。
4. 輸入您的帳戶 ID（顯示在關閉對話方塊頂端），以確認您已閱讀並了解帳戶關閉程序。
5. 選擇關閉帳戶按鈕以啟動帳戶關閉程序。
6. 您應該會在幾分鐘內收到電子郵件確認，指出您的帳戶已關閉。

Note

中 AWS CLI 或其中一個 AWS SDKs API 操作不支援此任務。您只能使用 來執行此任務 AWS 管理主控台。

Member account

成員帳戶是 AWS 帳戶 的一部分 AWS Organizations。

從 AWS Organizations 主控台關閉成員帳戶

1. 登入 [AWS Organizations 主控台](#)。
2. 在 AWS 帳戶 頁面上，尋找並選擇您要關閉的成員帳戶名稱。您可以導覽 OU 階層，或查看沒有 OU 結構的帳戶平面清單。
3. 選擇頁面頂端帳戶名稱旁的關閉帳戶。只有在組織處於[所有功能](#)模式時，AWS 才能使用此選項。

Note

如果您的組織使用[合併帳單](#)模式，您將無法在主控台中看到關閉帳戶按鈕。若要以合併帳單模式關閉帳戶，請登入您要以根使用者身分關閉的帳戶。在帳戶頁面上，選擇關閉帳戶按鈕，輸入您的帳戶 ID，然後選擇關閉帳戶按鈕。

4. 閱讀並確保您了解帳戶關閉指引。
5. 輸入成員帳戶 ID，然後選擇關閉帳戶以啟動帳戶關閉程序。

Note

您關閉的任何成員帳戶都會在 AWS Organizations 主控台中在其帳戶名稱旁顯示CLOSED標籤，最長可達原始關閉日期後 90 天。90 天後，成員帳戶將不再顯示在 AWS Organizations 主控台中。

從帳戶頁面關閉成員帳戶

或者，您也可以直接從 中的帳戶頁面關閉 AWS 成員帳戶 AWS 管理主控台。如需step-by-step指引，請遵循獨立帳戶索引標籤中的指示。

此選項不適用於沒有根使用者的專案帳戶。從 AWS Organizations 主控台關閉專案帳戶。

使用 AWS CLI 和 SDKs 關閉成員帳戶

如需如何使用 AWS CLI 和 SDKs 關閉成員帳戶的說明，請參閱AWS Organizations 《使用者指南》中的[關閉組織中的成員帳戶](#)。

Management account

管理帳戶是 AWS 帳戶，可做為其父帳戶或根帳戶 AWS Organizations。

 Note

您無法直接從 AWS Organizations 主控台關閉管理帳戶。

從帳戶頁面關閉管理帳戶

1. 以您要關閉之管理帳戶的[根使用者 AWS 管理主控台 身分登入](#)。以 IAM 使用者或角色身分登入時，您無法關閉帳戶。
2. 確認您的組織中沒有剩餘的作用中成員帳戶。若要這樣做，請前往 [AWS Organizations 主控台](#)，並確定所有成員帳戶都顯示在其帳戶名稱Closed旁邊。如果您的成員帳戶仍處於作用中狀態，您將需要遵循成員帳戶索引標籤中提供的帳戶關閉指引，才能移至下一個步驟。
3. 在右上角的導覽列上，選擇您的帳戶名稱或號碼，然後選擇帳戶。
4. 在[帳戶頁面上](#)，選擇關閉帳戶按鈕。
5. 輸入您的帳戶 ID（顯示在關閉對話方塊頂端），以確認您已閱讀並了解帳戶關閉程序。
6. 選擇關閉帳戶按鈕以啟動帳戶關閉程序。
7. 您應該會在幾分鐘內收到電子郵件確認，指出您的帳戶已關閉。

 Note

中 AWS CLI 或其中一個 AWS SDKs API 操作不支援此任務。您只能使用 [AWS 管理主控台](#) 來執行此任務。

AWS GovCloud (US) account

AWS 帳戶 基於帳單和付款目的，AWS GovCloud (US) 帳戶一律會連結至單一標準。

關閉 AWS GovCloud (US) 帳戶

如果您有 AWS 帳戶 連結到 AWS GovCloud (US) 帳戶的，您需要先關閉標準帳戶，才能關閉帳戶 AWS GovCloud (US)。如需詳細資訊，包括如何備份資料和避免意外 AWS GovCloud (US) 費用，請參閱 AWS GovCloud (US) 《使用者指南》中的[關閉 AWS GovCloud \(US\) 帳戶](#)。

關閉帳戶後預期會發生的情況

關閉帳戶後，將立即發生下列情況：

- 您會收到一封電子郵件，確認帳戶關閉至根使用者的電子郵件地址。如果您在幾個小時內沒有收到此電子郵件，請參閱 [對 AWS 帳戶 關閉問題進行故障診斷](#)。
- 您關閉的任何成員帳戶都會在 AWS Organizations 主控台中在其帳戶名稱旁顯示CLOSED標籤，最長可達原始關閉日期後 90 天。90 天後，成員帳戶將不再顯示在 AWS Organizations 主控台中。
- 如果您已將存取 中服務的許可授予 AWS 帳戶 其他 帳戶，則從這些帳戶發出的任何存取請求都應在帳戶關閉後失敗。如果您重新開啟 AWS 帳戶，當您授予帳戶所需的許可時，其他 AWS 帳戶 可以再次存取帳戶的 AWS 服務和資源。

帳戶關閉可能不會在所有區域和服務中立即發生，可能需要數小時才能完成。

關閉後期間

關閉後期間是指您關閉帳戶當天到 AWS 永久關閉帳戶之間的時間長度 AWS 帳戶。關閉後期間為 90 天。在關閉後期間，您只能透過重新開啟 帳戶來存取您的內容 AWS 和服務。在關閉後期間之後，AWS 會永久關閉您的 AWS 帳戶，您無法再重新開啟它。AWS 也會刪除您帳戶中的內容和資源 (CloudTrail 追蹤除外)。帳戶永久關閉後，其 [AWS 帳戶 ID](#) 永遠無法重複使用。

重新開啟您的 AWS 帳戶

您的帳戶將在 90 天內永久關閉，之後您將無法重新開啟您的帳戶，AWS 並將刪除您帳戶中剩餘的內容。若要在永久關閉之前重新開啟您的帳戶，請參閱 [重新開啟 AWS 帳戶](#)。

Note

如果您重新開啟服務，保留在帳戶中的服務費用將會重新啟動。

重新開啟 AWS 帳戶

如果您關閉您的 AWS 帳戶 且沒有未結餘額，您可以在[關閉後期間](#)自行重新開啟。

您以根使用者身分登入並從帳戶頁面提交請求，以重新開啟帳戶。

重新開啟帳戶之前需要了解的事項

重新開啟您的 之前 AWS 帳戶，請注意下列事項：

- 自助式需求：只有在您自己關閉帳戶，且您的帳戶在帳戶關閉時沒有未結餘額時，才能使用此自助式程序。您必須以已關閉帳戶的根使用者身分登入；以 IAM 使用者或角色身分登入時，您無法重新開啟帳戶。您必須在關閉帳戶後的 90 天內在關閉後期間內提交重新開啟請求。
- 帳戶關閉者 AWS：如果 AWS 關閉您的帳戶，您無法自行重新開啟。在您的帳戶關閉後的 30 天內支付任何未結餘額，然後聯絡 [AWS 支援](#) 重新開啟您的帳戶。
- 付款和費用：您的帳戶必須具有有效、未過期的付款方式。由於上個月的帳單是在下個月初完成，因此即使您的帳戶在關閉時沒有餘額，在關閉之前，您可能仍有未結的餘額。若要檢閱或支付餘額，請參閱 [付款](#)。當您重新開啟帳戶時，會繼續針對其中仍在執行的任何服務收取費用。如果您在關閉帳戶之前未停止這些服務，您可能也會在關閉後期間產生費用。

如何重新開啟您的帳戶

請依照下列步驟重新開啟已關閉的帳戶。

Note

中 AWS CLI 或其中一個 AWS SDKs API 操作不支援此任務。您只能使用 來執行此任務 AWS 管理主控台。

從帳戶頁面重新開啟您的帳戶

1. 以您要重新開啟之已關閉 AWS 帳戶的 [根使用者 AWS 管理主控台 身分登入](#)。以 IAM 使用者或角色登入時，您無法重新開啟帳戶。
2. 開啟已關閉帳戶的帳戶頁面，如下所示：在關閉帳戶橫幅中，選擇重新開啟帳戶。
3. 在重新開啟帳戶對話方塊中，輸入對話方塊中顯示的帳戶 ID，以確認您想要重新開啟帳戶。
4. 選擇重新開啟帳戶以提交您的請求。訊息確認帳戶重新開啟已啟動。
5. 等待重新開啟完成。當您的帳戶再次處於作用中狀態時，會出現一則訊息，確認帳戶已成功重新開啟，且您的 AWS 服務和帳單已還原。

如果 AWS 無法重新開啟您的帳戶，您會收到主控台通知，說明原因和解決方法。

重新開啟帳戶後預期會發生的情況

提交重新開啟請求後，會發生下列情況：

- 若要檢查狀態，請重新整理帳戶頁面。重新開啟完成時，帳戶會顯示為作用中，且已關閉帳戶橫幅不會再顯示。
- 帳戶處於作用中狀態後，會 AWS 還原其服務和資源的存取權，然後繼續計費。

重新開啟後準備您的帳戶以供使用

有些資源和訂閱不會自動還原為執行中狀態。重新開啟帳戶後，您可能需要執行下列動作，才能繼續正常操作：

- 啟動帳戶關閉時停止的任何 Amazon EC2 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[啟動執行個體](#)。
- 從帳戶關閉時建立的快照還原 Amazon RDS 資料庫。
- 取消並重新訂閱任何 AWS Marketplace 訂閱。帳戶重新開啟時，訂閱不會自動還原。

區域可用性

自助式帳戶重新開啟適用於所有商業區域。

AWS 帳戶管理的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[共同責任模型](#)將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。AWS 也為您提供可安全使用的服務。在[AWS 合規計劃](#)中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於帳戶管理的合規計劃，請參閱[AWS 服務 合規計劃範圍內](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

共同的責任模型會針對所有 強制執行 AWS 帳戶。這包括 AWS 帳戶 您使用我們新的 AWS 體驗和您使用我們進階 AWS 體驗建立的帳戶來建立。

本文件可協助您了解如何在使用 AWS 帳戶管理時套用共同責任模型。它說明如何設定 Account Management 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護帳戶管理資源。其中一些文件僅與使用我們進階 AWS 體驗建立的帳戶相關。我們會識別文件何時僅與使用我們進階 AWS 體驗建立的帳戶相關。

主題

- [AWS Account Management 中的資料保護](#)
- [AWS PrivateLink 適用於 AWS 帳戶管理](#)
- [AWS 帳戶管理的 Identity and Access Management](#)
- [AWS AWS Account Management 的 受管政策](#)
- [AWS Account Management 的合規驗證](#)
- [AWS 帳戶管理中的彈性](#)
- [中的基礎設施安全 AWS 帳戶管理](#)

AWS Account Management 中的資料保護

下列資訊與所有 相關 AWS 帳戶。

AWS [共同責任模型](#)適用於 AWS 帳戶管理中的資料保護。如此模型所述，AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS

服務的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權常見問答集](#)。如需歐洲資料保護的詳細資訊，請參閱[一般資料保護規則 \(GDPR\) 中心](#)。

基於資料保護目的，我們建議您保護 AWS 帳戶登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱 AWS CloudTrail 《使用者指南》中的[使用 CloudTrail 追蹤](#)。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-3](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Account Management 或使用主控台、API AWS CLI 或其他 AWS 服務 AWS SDKs 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

AWS PrivateLink 適用於 AWS 帳戶管理

下列資訊與所有相關 AWS 帳戶。

如果您使用 Amazon Virtual Private Cloud (Amazon VPC) 託管 AWS 資源，您可以從 VPC 內存取 AWS 帳戶管理服務，而無需跨公有網際網路。

Amazon VPC 可讓您在自訂虛擬網路中啟動 AWS 資源。您可利用 VPC 來控制您的網路設定，例如 IP 地址範圍、子網路、路由表和網路閘道。如需有關 Amazon VPC 的詳細資訊，請參閱《[Amazon VPC 使用者指南](#)》。

若要將 Amazon VPC 連線至帳戶管理，您必須先定義介面 VPC 端點，以將您的 VPC 連線至其他 AWS 服務。端點可提供可靠、可擴展的連線能力，且不需要網際網路閘道、網路地址轉譯 (NAT) 執行個體或 VPN 連接。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[介面 VPC 端點 \(AWS PrivateLink\)](#)。

建立端點

您可以使用 AWS 管理主控台、(AWS CLI)、AWS SDK、AWS 帳戶管理 API 或在 AWS Command Line Interface VPC 中建立 AWS 帳戶管理端點 CloudFormation。

如需有關使用 Amazon VPC 主控台或 建立和設定端點的資訊 AWS CLI，請參閱《Amazon VPC 使用者指南》中的[建立界面端點](#)。

Note

當您建立端點時，請使用下列格式，將 Account Management 指定為您希望 VPC 連線的服務：

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

您必須完全依照所示方式使用字串，指定 us-east-1 區域。作為全球服務，帳戶管理僅託管在該 AWS 區域。

如需有關使用 建立和設定端點的資訊 CloudFormation，請參閱 CloudFormation 《使用者指南》中的[AWS::EC2::VPCEndpoint](#) 資源。

Amazon VPC 端點政策

您可以在建立 Amazon VPC 端點時連接端點政策，以控制可透過此服務端點執行的動作。您可以連接多個端點政策來建立複雜的 IAM 規則。如需詳細資訊，請參閱：

- [帳戶管理的 Amazon Virtual Private Cloud 端點政策](#)
- 《AWS PrivateLink 指南》中的[使用 VPC 端點控制對服務的存取](#)。

帳戶管理的 Amazon Virtual Private Cloud 端點政策

下列資訊與所有 相關 AWS 帳戶。

您可以為帳戶管理建立 Amazon VPC 端點政策，並在其中指定下列項目：

- 可執行動作的主體。
- 委託人可執行的動作。

- 可供執行動作的資源。

下列範例顯示 Amazon VPC 端點政策，允許帳戶 123456789012 中名為 Alice 的 IAM 使用者擷取和變更任何的替代聯絡資訊 AWS 帳戶，但拒絕所有 IAM 使用者刪除任何帳戶上任何替代聯絡資訊的許可。

如果您想要將屬於 AWS 組織一部分的帳戶存取權授予組織的其中一個成員帳戶中的委託人，則 Resource 元素必須使用下列格式：

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

如需建立端點政策的詳細資訊，請參閱《AWS PrivateLink 指南》中的[使用 VPC 端點控制對服務的存取](#)。

AWS 帳戶管理的 Identity and Access Management

AWS Identity and Access Management (IAM) 是 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證（登入）和授權（具有許可），以使用帳戶管理資源。IAM 是您可以免費使用 AWS 服務的。

下列資訊是關於 AWS 帳戶管理的 Identity and Access Management。此資訊與您使用進階 AWS 體驗時 AWS 帳戶，或是您為帳戶啟用進階功能時所建立的資訊最為相關。若要了解存取控制如何適用於我們的新 AWS 體驗，請參閱[比較存取管理](#)。

主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [AWS 帳戶管理如何與 IAM 搭配使用](#)
- [AWS Account Management 的身分型政策範例](#)
- [針對 AWS 帳戶管理使用身分型政策 \(IAM 政策\)](#)
- [故障診斷 AWS 帳戶管理身分和存取權](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 [故障診斷 AWS 帳戶管理身分和存取權](#))
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 [AWS 帳戶管理如何與 IAM 搭配使用](#))
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 [AWS Account Management 的身分型政策範例](#))

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的[如何登入您的 AWS 帳戶](#)。

對於程式設計存取，AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的[API 請求的AWS 第 4 版簽署程序](#)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務和資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的[需要根使用者憑證的任務](#)。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務使用臨時憑證存取。

聯合身分是來自您企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務憑證存取 Directory Service 的使用者。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[什麼是 IAM Identity Center ?](#)。

IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的[要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取](#)。

[IAM 群組](#)會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 使用者的使用案例](#)。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過[從使用者切換到 IAM 角色（主控台）](#)或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 中的快帳戶資源存取](#)。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS，會評估這些政策。大多數政策會以 JSON 文件 AWS 的形式存放在中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 [JSON 政策概觀](#)。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的[在受管政策與內嵌政策之間選擇](#)。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中[指定主體](#)。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 實體許可界限](#)。
- 服務控制政策 (SCP) — 為 AWS Organizations 中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的 [服務控制政策](#)。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的 [資源控制政策 \(RCP\)](#)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的 [工作階段政策](#)。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的 [政策評估邏輯](#)。

AWS 帳戶管理如何與 IAM 搭配使用

此資訊與您使用進階 AWS 體驗時 AWS 帳戶 建立的資訊最相關。若要了解存取控制如何適用於我們的新 AWS 體驗，請參閱 [比較存取管理](#)。

在您使用 IAM 管理帳戶管理的存取權之前，請先了解哪些 IAM 功能可與帳戶管理搭配使用。

您可以搭配 AWS Account Management 使用的 IAM 功能

IAM 功能	帳戶管理支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是

IAM 功能	帳戶管理支援
ACL	否
ABAC(政策中的標籤)	否
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	否

若要全面了解帳戶管理和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱 [《AWS IAM 使用者指南》中的與 IAM 搭配使用的服務](#)。

帳戶管理的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的[IAM JSON 政策元素參考](#)。

Account Management 的身分型政策範例

若要檢視帳戶管理身分型政策的範例，請參閱 [AWS Account Management 的身分型政策範例](#)。

Account Management 中的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下

執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 中的快帳戶資源存取](#)。

Account Management 的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

若要查看帳戶管理動作的清單，請參閱《服務授權參考》中的[AWS 帳戶管理定義的動作](#)。

Account Management 中的政策動作在動作之前使用以下字首。

```
account
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

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

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定使用 AWS 帳戶替代聯絡人的所有動作，請包含下列動作。

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

若要檢視帳戶管理身分型政策的範例，請參閱 [AWS Account Management 的身分型政策範例](#)。

Account Management 的政策資源

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

Account Management 服務支援 IAM 政策Resource元素中的下列特定資源類型，以協助您篩選政策並區分這些類型 AWS 帳戶：

- account

此resource類型僅比對非由 AWS Organizations 服務管理之組織中成員帳戶的獨立 AWS 帳戶。

- accountInOrganization

此resource類型僅符合服務所管理組織中 AWS 帳戶 的成員帳戶 AWS Organizations。

若要查看帳戶管理資源類型及其 ARNs 的清單，請參閱《服務授權參考》中的[AWS 帳戶管理定義的資源](#)。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱[AWS 帳戶管理定義的動作](#)。

若要檢視帳戶管理身分型政策的範例，請參閱 [AWS Account Management 的身分型政策範例](#)。

Account Management 的政策條件索引鍵

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用[條件運算子](#)的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的[AWS 全域條件內容索引鍵](#)。

Account Management 服務支援下列條件索引鍵，您可以使用這些索引鍵為您的 IAM 政策提供精細篩選：

- account : TargetRegion

此條件索引鍵採用由[AWS 區域代碼](#)清單組成的引數。它可讓您篩選政策，只影響套用至指定區域的這些動作。

- account : AlternateContactTypes

此條件索引鍵會取得替代聯絡類型的清單：

- 帳單
- 操作
- SECURITY

使用此金鑰可讓您篩選僅針對指定替代聯絡類型之動作的請求。

- account : AccountResourceOrgPaths

此條件索引鍵採用 引數，其中包含透過組織階層到特定組織單位 (OU) 的路徑清單。它可讓您篩選政策，只影響相符 OU 中的目標帳戶。

```
o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
```

- account : AccountResourceOrgTags

此條件索引鍵採用由標籤索引鍵和值清單組成的引數。它可讓您篩選政策，只影響那些屬於組織成員並以指定標籤索引鍵和值標記的帳戶。

- account : EmailTargetDomain

此條件索引鍵採用由電子郵件網域清單組成的引數。它可讓您篩選政策，只影響符合指定電子郵件網域的動作。此條件索引鍵區分大小寫。您應該在政策的條件區塊StringEquals中使用 StringEqualsIgnoreCase而非，以根據目標電子郵件地址網域來控制動作。以下是範例政策，當電子郵件網域包含 example.com、company.org或任何案例組合時，允許 account:StartPrimaryEmailUpdate動作完成，例如 EXAMPLE.COM。

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

```
        "example.com",  
        "company.org"  
    ]  
}  
}  
]  
}
```

若要查看帳戶管理條件索引鍵的清單，請參閱《服務授權參考》中的[AWS 帳戶管理的條件索引鍵](#)。若要了解您可以使用條件索引鍵的動作和資源，請參閱[AWS 帳戶管理定義的動作](#)。

若要檢視帳戶管理身分型政策的範例，請參閱 [AWS Account Management 的身分型政策範例](#)。

Account Management 中的存取控制清單

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Account Management 的屬性型存取控制

支援 ABAC (政策中的標籤)：否

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在 AWS 中，這些屬性稱為標籤。您可以將標籤連接至 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

對於 AWS 帳戶管理，僅透過 `account:AccountResourceOrgTags/key-name` 條件金鑰支援標籤型存取控制。帳戶命名空間中的 APIs 不支援標準 `aws:ResourceTag/key-name` 條件金鑰。

使用支援的條件金鑰的範例 JSON 政策

下列範例政策允許存取，以檢視組織中標記為金鑰 "CostCenter" 且值為 "12345" 或 "67890" 之帳戶的聯絡資訊。

JSON

```
{
```

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

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)和 [IAM 教學課程：根據標籤定義存取 AWS 資源的許可](#)。

搭配 Account Management 使用臨時登入資料

支援臨時憑證：是

臨時登入資料提供對 AWS 資源的短期存取，並在您使用聯合或切換角色時自動建立。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的臨時安全憑證](#)與[可與 IAM 搭配運作的 AWS 服務](#)。

Account Management 的跨服務主體許可

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫的委託人許可 AWS 服務，並結合 AWS 服務請求向下游服務提出請求。如需提出 FAS 請求時的政策詳細資訊，請參閱[轉發存取工作階段](#)。

Account Management 的服務角色

支援服務角色：否

服務角色是服務擔任的 [IAM 角色](#)，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[建立角色以委派許可給 AWS 服務](#)。

Account Management 的服務連結角色

支援服務連結角色：否

服務連結角色是連結至的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的中 AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服务連結角色的詳細資訊，請參閱[可搭配 IAM 運作的AWS 服務](#)。在資料表中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

AWS Account Management 的身分型政策範例

此資訊與您使用進階 AWS 體驗時 AWS 帳戶 建立的資訊最相關。若要了解存取控制如何適用於我們的新 AWS 體驗，請參閱 [比較存取管理](#)。

根據預設，使用者和角色沒有建立或修改帳戶管理資源的許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的[建立 IAM 政策 \(主控台\)](#)。

如需 Account Management 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱《服務授權參考》中的 [AWS Account Management 的動作、資源和條件索引鍵](#)。

主題

- [政策最佳實務](#)
- [使用 中的帳戶頁面 AWS 管理主控台](#)
- [提供 中帳戶頁面的唯讀存取權 AWS 管理主控台](#)
- [提供 中帳戶頁面的完整存取權 AWS 管理主控台](#)

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除帳戶管理資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#) 或 [任務職能的 AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [透過 MFA 的安全 API 存取](#)。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 [IAM 安全最佳實務](#)。

使用 中的帳戶頁面 AWS 管理主控台

若要存取 中的 [帳戶頁面](#) AWS 管理主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (IAM 使用者或角色) 而言，主控台就無法如預期運作。

為了確保使用者和角色可以使用帳戶管理主控台，您可以選擇將 `AWSAccountManagementReadOnlyAccess` 或 `AWSAccountManagementFullAccess` AWS 受管政策連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的 [新增許可到使用者](#)。

對於僅呼叫 CLI 或 AWS API AWS 的使用者，您不需要允許最低主控台許可。相反地，在許多情況下，您可以選擇僅允許存取與您嘗試執行之 API 操作相符的動作。

提供 中帳戶頁面的唯讀存取權 AWS 管理主控台

在下列範例中，您想要授予 中的 AWS 帳戶 IAM 使用者對 中帳戶頁面的唯讀存取權 AWS 管理主控台。附加此政策的使用者無法進行任何變更。

`account:GetAccountInformation` 動作授予檢視帳戶頁面上大部分設定的存取權。不過，若要檢視目前啟用 AWS 的區域，您還必須包含 `account:ListRegions` 動作。

JSON

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

提供中帳戶頁面的完整存取權 AWS 管理主控台

在下列範例中，您想要授予 IAM 使用者完整 AWS 帳戶存取中的帳戶頁面 AWS 管理主控台。連接此政策的使用者可以變更帳戶的設定。

此範例政策以上述範例政策為基礎，新增每個可用的寫入許可 (`CloseAccount` 除外)，允許使用者變更帳戶的大部分設定，包括 `account:EnableRegion` 和 `account:DisableRegion` 許可。

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": "*"
}
]
```

針對 AWS 帳戶管理使用身分型政策 (IAM 政策)

此資訊與您使用進階 AWS 體驗時 AWS 帳戶 建立的資訊最相關。若要了解存取控制如何適用於我們的新 AWS 體驗，請參閱 [比較存取管理](#)。

如需 AWS 帳戶 和 IAM 使用者的完整討論，請參閱 [什麼是 IAM？](#) IAM 使用者指南中的。

如需如何更新客戶受管政策的說明，請參閱《[IAM 使用者指南](#)》中的[編輯 IAM 政策](#)。

AWS 帳戶管理動作政策

此資料表摘要說明授予您帳戶設定存取權的許可。如需使用這些許可的政策範例，請參閱 [AWS Account Management 的身分型政策範例](#)。

Note

若要授予 IAM 使用者對 帳戶頁面中特定 [帳戶](#) 設定的寫入存取權 AWS 管理主控台，除了要用來修改該設定的許可（或許可）之外，您還必須允許 GetAccountInformation 許可。

許可名稱	存取層級	說明
account:ListRegions	清單	准許列出可用的區域。
account:GetAccountInformation	讀取	准許擷取 帳戶的帳戶資訊。
account:GetAlternateContact	讀取	准許擷取帳戶的替代聯絡人。

許可名稱	存取層級	說明
account:GetContactInformation	讀取	准許擷取帳戶的主要聯絡資訊。
account:GetPrimaryEmail	讀取	准許擷取帳戶的主要電子郵件地址。
account:GetRegionOptStatus	讀取	准許取得區域的選擇加入狀態。
account:AcceptPrimaryEmailUpdate	寫入	准許接受 AWS 組織中成員帳戶的主要電子郵件地址更新。
account:CloseAccount	寫入	准許關閉帳戶。 <div>  Note 此許可僅適用於主控台。此許可沒有可用的 API 存取權。 </div>
account>DeleteAlternateContact	寫入	准許刪除帳戶的替代聯絡人。
account:DisableRegion	寫入	准許停用區域。
account:EnableRegion	寫入	准許使用區域。
account:PutAccountName	寫入	准許更新帳戶的名稱。
account:PutAlternateContact	寫入	准許修改帳戶的替代聯絡人。
account:PutContactInformation	寫入	准許更新帳戶的主要聯絡資訊。

許可名稱	存取層級	說明
account:SendPhoneNumberVerification	寫入	准許將驗證碼傳送至 帳戶的主要聯絡電話號碼。
account:StartPrimaryEmailUpdate	寫入	准許啟動 AWS 組織中成員帳戶的主要電子郵件地址更新。
account:VerifyPhoneNumber	寫入	准許透過提交驗證碼來驗證帳戶的主要聯絡電話號碼。

故障診斷 AWS 帳戶管理身分和存取權

此資訊與您使用進階 AWS 體驗時 AWS 帳戶 建立的資訊最相關。若要了解存取控制如何適用於我們的新 AWS 體驗，請參閱 [比較存取管理](#)。

使用以下資訊來協助您診斷和修正使用帳戶管理和 IAM 時可能遇到的常見問題。

主題

- [我無權在帳戶頁面中執行動作](#)
- [我未獲得執行 iam:PassRole 的授權](#)
- [我想要允許 以外的人員 AWS 帳戶 存取我的帳戶詳細資訊](#)

我無權在帳戶頁面中執行動作

如果 AWS 管理主控台 告知您無權執行 動作，則必須聯絡您的管理員尋求協助。您的管理員是為您提供使用者名稱和密碼的人員。

當 mateojackson IAM 使用者嘗試使用主控台在 的帳戶頁面 AWS 帳戶 中檢視他的詳細資訊，AWS 管理主控台 但沒有 account:GetAccountInformation 許可時，會發生下列範例錯誤。



You Need Permissions

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

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 *my-example-widget* 動作存取 account:*GetWidget* 資源。

我未獲得執行 `iam:PassRole` 的授權

如果您收到錯誤，告知您無權執行 `iam:PassRole` 動作，您的政策必須更新，以允許您將角色傳遞給帳戶管理。

有些 AWS 服務可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 `iam:marymajor` 的使用者嘗試使用主控台在帳戶管理中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

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

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許以外的人員 AWS 帳戶 存取我的帳戶詳細資訊

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解帳戶管理是否支援這些功能，請參閱 [AWS 帳戶管理如何與 IAM 搭配使用](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《[IAM 使用者指南](#)》中的 [在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《[IAM 使用者指南](#)》中的 [將存取權提供給第三方 AWS 帳戶 擁有](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱《[IAM 使用者指南](#)》中的 [將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《[IAM 使用者指南](#)》中的 [IAM 中的跨帳戶資源存取](#)。

AWS AWS Account Management 的 受管政策

此資訊與您使用進階 AWS 體驗時 AWS 帳戶，或是您為帳戶啟用進階功能時所建立的資訊最為相關。若要了解存取控制如何適用於我們的新 AWS 體驗，請參閱 [比較存取管理](#)。

AWS Account Management 目前提供兩個可供您使用的 AWS 受管政策：

- [AWS 受管政策：AWSAccountManagementReadOnlyAccess](#)
- [AWS 受管政策：AWSAccountManagementFullAccess](#)
- [AWS 受管政策的帳戶管理更新](#)

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的[客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。AWS 服務當新的啟動或新的 API 操作可用於現有服務時，AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#)。

AWS 受管政策：AWSAccountManagementReadOnlyAccess

您可將 AWSAccountManagementReadOnlyAccess 政策連接到 IAM 身分。

此政策提供唯讀許可，只能檢視下列項目：

- 有關的中繼資料 AWS 帳戶
- 針對 AWS 區域 啟用或停用的 AWS 帳戶（您只能使用 AWS 主控台檢視帳戶中區域的狀態）

它透過授予執行任何 Get*或 List*操作的許可來執行此操作。它不提供修改帳戶中繼資料或 AWS 區域 啟用或停用帳戶的任何功能。

許可詳細資訊

此政策包含以下許可。

- **account** : 允許主體擷取其中繼資料資訊 AWS 帳戶。它還允許主體列出 AWS 區域 在 中為帳戶啟用的 AWS 管理主控台。

JSON

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

AWS 受管政策 : AWSAccountManagementFullAccess

您可將 AWSAccountManagementFullAccess 政策連接到 IAM 身分。

此政策提供檢視或修改下列項目的完整管理存取權：

- 有關 的中繼資料 AWS 帳戶
- 針對 AWS 區域 啟用或停用的 AWS 帳戶（您只能使用 AWS 主控台檢視帳戶的狀態，或是啟用或停用 區域）

它透過授予執行任何account操作的許可來執行此操作。

許可詳細資訊

此政策包含以下許可。

- **account** – 允許主體檢視或修改其中繼資料資訊 AWS 帳戶。它還允許主體列出為帳戶啟用 AWS 區域 的，並在 中啟用或停用它們 AWS 管理主控台。

JSON

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

AWS 受管政策的帳戶管理更新

檢視自此服務開始追蹤這些變更以來，帳戶管理 AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱帳戶管理文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AWS 使用新的 AWS 受管政策啟動帳戶管理，並開始追蹤變更	帳戶管理最初使用下列 AWS 受管政策啟動： <ul style="list-style-type: none">• AWSAccountManagementReadOnlyAccess• AWSAccountManagementFullAccess	2021 年 9 月 30 日

AWS Account Management 的合規驗證

我們的新 AWS 體驗無法用於任何受管制的工作負載。以下資訊僅與使用註冊 AWS（進階）時建立的帳戶相關。

第三方稽核人員會評估可在中作為多個合規計劃 AWS 帳戶一部分執行之 AWS 服務的安全性和 AWS 合規性。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需特定合規計劃範圍內 AWS 的服務清單，請參閱[AWS 服務 合規計劃範圍內](#)。如需一般資訊，請參閱 [AWS Compliance Programs](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱AWS Artifact 《使用者指南》中的在 [中下載報告 AWS Artifact](#)下載報告。

您在 中使用 服務的合規責任 AWS 帳戶 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源以協助合規：

- [安全與合規快速入門指南](#) – 這些部署指南討論架構考量，並提供在 上部署以安全與合規為重心 AWS 之基準環境的步驟。
- [Amazon Web Services 上的 HIPAA 安全與合規架構](#) – 本白皮書說明公司如何使用 AWS 來建立符合 HIPAA 資格的應用程式。

 Note

並非所有 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 [HIPAA 資格服務參照](#)。

- [AWS 合規資源](#) – 此工作手冊和指南集合可能適用於您的產業和位置。
- 《AWS Config 開發人員指南》中的[使用規則評估資源](#) – AWS Config 服務會評估資源組態符合內部實務、產業準則和法規的程度。
- [AWS Security Hub CSPM](#) – 這 AWS 服務 可讓您全面檢視 內的安全狀態 AWS ，協助您檢查是否符合安全產業標準和最佳實務。
- [AWS Audit Manager](#) – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和業界標準的方式。

AWS 帳戶管理中的彈性

下列資訊與所有 相關 AWS 帳戶。如果您使用我們的新 AWS 體驗，則適用其他區域考量。如需詳細資訊，請參閱[AWS 區域 您的專案](#)。

AWS 全球基礎設施是以 AWS 區域 和可用區域為基礎建置。區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

中的基礎設施安全 AWS 帳戶管理

下列資訊與所有 相關 AWS 帳戶。

作為受管服務，在 中執行 AWS 的服務 AWS 帳戶 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取帳戶設定。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以使用[AWS Security Token Service](#) (AWS STS) 以產生暫時安全憑證以簽署請求。

監控您的 AWS 帳戶

這包括 AWS 帳戶 您使用我們新的 AWS 體驗和您使用我們進階 AWS 體驗建立的帳戶來建立。若要比較註冊選項，請參閱 [比較註冊選項](#)。

監控是維護 AWS Account Management 和其他 AWS 解決方案的可靠性、可用性和效能的重要部分。AWS 提供下列監控工具來監看 Account Management、在發生錯誤時回報，以及適時採取自動動作：

- AWS CloudTrail 會擷取（日誌）API 呼叫，以及由 或代表您發出的相關事件，並將日誌檔案 AWS 帳戶 寫入您指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。這可讓您識別名為的使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱「[AWS CloudTrail 使用者指南](#)」。
- Amazon EventBridge 透過自動回應系統事件，例如應用程式可用性問題或資源變更，為您的 AWS 服務新增額外的自動化。來自 AWS 服務的事件會以近乎即時的方式交付至 EventBridge。您可編寫簡單的規則，來指示您在意的事件，以及當事件符合規則時所要自動執行的動作。如需詳細資訊，請參閱「[Amazon EventBridge 使用者指南](#)」。

使用 記錄 AWS 帳戶管理 API 呼叫 AWS CloudTrail

這包括 AWS 帳戶 您使用我們新的 AWS 體驗和您使用我們進階 AWS 體驗建立的帳戶來建立。若要比較註冊選項，請參閱 [比較註冊選項](#)。

AWS Account Management APIs 已與 整合 AWS CloudTrail，此服務提供由使用者、角色或呼叫 Account Management 操作 AWS 的服務所採取之動作的記錄。CloudTrail 會將所有帳戶管理 API 呼叫擷取為事件。擷取的呼叫包括對帳戶管理操作的所有呼叫。如果您建立追蹤，您可以開啟 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括帳戶管理操作的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷稱為帳戶管理操作的請求、用於提出請求的 IP 地址、提出請求的人員和時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「[AWS CloudTrail 使用者指南](#)」。

CloudTrail 中的帳戶管理資訊

當您建立帳戶 AWS 帳戶 時，CloudTrail 會在 中開啟。當帳戶管理操作發生活動時，CloudTrail 會記錄 CloudTrail 事件中的活動，以及事件歷史記錄中的其他 AWS 服務事件。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱《使用 CloudTrail 事件歷史記錄檢視事件》<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html>。

若要持續記錄 中的事件 AWS 帳戶，包括帳戶管理操作的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在 中建立線索時 AWS 管理主控台，線索會套用至所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中收集的事件資料。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [從多個區域接收 CloudTrail 日誌檔案](#)
- [從多個帳戶接收 CloudTrail 日誌檔案](#)

AWS CloudTrail 會記錄本指南的 API [參考區段中找到的所有帳戶管理 API](#) 操作。例如，對 CreateAccount、DeleteAlternateContact 和 PutAlternateContact 操作的呼叫都會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根使用者或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求
- 提出該請求時，是否使用了 IAM 角色或聯合身分使用者的暫時安全登入資料
- 請求是否由其他 AWS 服務提出

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

了解帳戶管理日誌項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件代表任何來源提出的單一請求，並包含所請求之操作的相關資訊、操作的日期和時間、請求參數等等。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

範例 1：下列範例顯示呼叫 GetAlternateContact 操作的 CloudTrail 日誌項目，以擷取帳戶的目前 OPERATIONS 替代聯絡人。操作傳回的值不會包含在記錄的資訊中。

Example 範例 1

```
{
```

```

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

```

範例 2：下列範例顯示呼叫 PutAlternateContact 操作的 CloudTrail 日誌項目，以將新的 BILLING 替代聯絡人新增至帳戶。

```
{
  "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"
}
```

```
}
```

範例 3：下列範例顯示呼叫 `DeleteAlternateContact` 操作以刪除目前 OPERATIONS 替代聯絡人的 CloudTrail 日誌項目。

```
{
  "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 EventBridge 監控帳戶管理事件

這包括 AWS 帳戶 您使用我們新的 AWS 體驗和您使用我們進階 AWS 體驗建立的帳戶來建立。若要比較註冊選項，請參閱 [比較註冊選項](#)。

先前稱為 CloudWatch Events 的 Amazon EventBridge 可協助您監控特定事件，並啟動使用其他 的目標動作 AWS 服務。來自 的事件 AWS 服務 會以近乎即時的方式交付至 EventBridge。

使用 EventBridge，您可以建立符合傳入事件的規則，並將其路由到目標以進行處理。

如需詳細資訊，請參閱 《Amazon EventBridge 使用者指南》中的 [Amazon EventBridge 入門](#)。

帳戶管理事件

下列範例顯示帳戶管理的事件。盡可能產生事件。

只有透過 CloudTrail 啟用和停用區域和 API 呼叫的特定事件，目前可供帳戶管理使用。

Event types (事件類型)

- [啟用和停用區域的事件](#)

啟用和停用區域的事件

當您從主控台或從 API 啟用或停用帳戶中的區域時，就會啟動非同步任務。初始請求將記錄為目標帳戶中的 CloudTrail 事件。此外，EventBridge 事件會在啟用或停用程序開始時傳送至呼叫帳戶，並在任一程序完成後再次傳送。

下列範例事件顯示如何傳送請求，指出 2020-09-30 ap-east-1 區域中的 是ENABLED針對帳戶 123456789012。

```
{
  "version": "0",
  "id": "11112222-3333-4444-5555-666677778888",
  "detail-type": "Region Opt-In Status Change",
  "source": "aws.account",
  "account": "123456789012",
```

```
{
  "time": "2020-09-30T06:51:08Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:account::123456789012:account"
  ],
  "detail": {
    "accountId": "123456789012",
    "regionName": "ap-east-1",
    "status": "ENABLED"
  }
}
```

有四種可能的狀態符合 GetRegionOptStatus 和 ListRegions APIs 傳回的狀態：

- ENABLED – 已成功為 accountId 指定的 啟用 區域
- ENABLING – 區域正在為 accountId 指定的 啟用
- DISABLED – 已成功停用 accountId 指定的 區域
- DISABLING – 區域正在為 accountId 指定的 停用

下列範例事件模式會建立擷取所有區域事件的規則。

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

下列範例事件模式會建立僅擷取 ENABLED 和 DISABLED 區域事件的規則。

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

```
        "DISABLED",  
        "ENABLED"  
    ]  
}
```

的配額 AWS 帳戶管理

您的 AWS 帳戶 具有每個 AWS 服務的預設配額，先前稱為限制。

下列配額資訊適用於您使用 建立的專案[註冊 AWS \(新\)](#)。若要調整配額，請建立支援票證。如需詳細資訊，請參閱[專案支援](#)。

資源	配額	可調整
您在 免費計劃中擁有的專案數量	29	否
您可以在付費計劃中擁有的專案數量	299	否
您可以與之共用專案的人數	500	否
您可以接受的專案邀請數量	100	否

如果您使用註冊（進階）註冊，以下配額資訊適用於 AWS 帳戶 您建立的。除非另有說明，否則每個配額都是 AWS 區域特定的。

資源	配額
每個目標帳戶的StartPrimaryEmailUpdate 請求數量上限	每 30 秒 3 次
中的替代聯絡人數量 AWS 帳戶	3 - BILLING、SECURITY和 各一個 OPERATIONS
每個帳戶的並行區域選項請求數量	6
每個組織的並行區域選項請求數量	50
每個呼叫者帳戶的AcceptPrimaryEmailUpdate 請求率	每秒 1 次，爆量至每秒 1 次

資源	配額
每個帳戶的DeleteAlternateContact 請求率	每秒 1 次，爆量至每秒 6 次
每個帳戶的DisableRegion 請求率	每秒 1 次，爆量至每秒 1 次
每個帳戶的EnableRegion 請求率	每秒 1 次，爆量至每秒 1 次
每個呼叫者帳戶的GetAccountInformation 請求率	每秒 3 次，爆量至每秒 3 次
每個帳戶的GetAlternateContact 請求率	每秒 10 次，爆量至每秒 15 次
每個帳戶的GetContactInformation 請求率	每秒 10 次，爆量至每秒 15 次
每個帳戶的GetGovCloudAccountInformation 請求率	每秒 3 次，爆量至每秒 5 次
每個呼叫者帳戶的GetPrimaryEmail 請求率	每秒 3 次，爆量至每秒 3 次
每個帳戶的GetRegionOptStatus 請求率	每秒 5 次，爆量至每秒 5 次
每個帳戶的ListRegions 請求率	每秒 5 次，爆量至每秒 5 次
每個呼叫者帳戶的PutAccountName 請求率	每秒 1 次，爆量至每秒 1 次
每個帳戶的PutAlternateContact 請求率	每秒 5 次，爆量至每秒 8 次
每個帳戶的PutContactInformation 請求率	每秒 5 次，爆量至每秒 8 次
每個呼叫者帳戶的StartPrimaryEmailUpdate 請求率	每秒 1 次，爆量至每秒 1 次

Account Management 使用者指南的文件歷史記錄

下表說明 AWS Account Management 的文件版本。

變更	描述	日期
新的電話號碼驗證 APIs	您可以使用新的 SendPhone NumberVerification 和 VerifyPhoneNumber APIs 來驗證主要聯絡電話號碼。GetContactInformation 回應也包含新的VerificationStatus 欄位。	2026 年 10 月 1 日
更新帳戶關閉配額值	在故障診斷主題中，將帳戶關閉配額百分比從 10% 更正為 20%，並將最小值從 10 更正為 250。	2026 年 6 月 23 日
新帳戶名稱 APIs	支援新的 GetAccountInformation 、和 PutAccountName API 來檢視或修改帳戶名稱。 APIs	2025 年 4 月 22 日
編輯安全挑戰問題的終止支援	從指南中移除編輯您的安全性挑戰問題主題，因為支援已結束。	2025 年 1 月 6 日
新的主要電子郵件 APIs	支援新的 StartPrimaryEmailUpdate 、 GetPrimaryEmail 和 AcceptPrimaryEmailUpdate APIs，以集中更新任何成員帳戶的根使用者電子郵件地址 AWS Organizations。如需詳細資訊，請參閱AWS	2024 年 6 月 6 日

	Organizations 《使用者指南》中的 更新成員帳戶的根使用者電子郵件地址 。	
重寫關閉帳戶主題	完全大修了整個關閉帳戶主題，包括新增如何關閉成員和管理帳戶的步驟。	2024 年 2 月 1 日
新增安全性挑戰問題的終止支援	新增了新內容，指出新增挑戰問題的選項已從帳戶頁面中移除。	2024 年 1 月 5 日
結束aws-portal 對命名空間的支援	AWS Identity and Access Management 先前用於管理您帳戶的 (IAM) 動作 (例如，aws-portal:ModifyAccount 和 aws-portal:ViewAccount) 已結束標準支援。	2024 年 1 月 1 日
重寫區域主題	完全大修了整個區域主題，包括新增展開和摺疊控制項。	2023 年 10 月 8 日
將根使用者主題重新配置到 IAM 使用者指南	將有關根使用者的討論合併為一個主題，新增根使用者主題的交叉參考連結，這些主題已移至 IAM 使用者指南。	2023 年 9 月 18 日
新增至主要帳戶聯絡人主題的新區段	已新增電話號碼和電子郵件地址需求區段。	2023 年 9 月 12 日
新的聯絡資訊 APIs	支援新的 GetContactInformation 和 PutContactInformation API。APIs	2022 年 7 月 22 日

[AWS Account Management](#)
[現在支援透過 AWS Organizations 主控台更新替代聯絡人。](#)

您現在可以使用更新的 AWS Organizations 受管政策提供的帳戶 API 許可，透過 AWS Organizations 主控台更新組織的替代聯絡人。

2022 年 2 月 8 日

[初始版本](#)

AWS 帳戶管理參考指南的初始版本

2021 年 9 月 30 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。