參考指南

AWS 帳戶管理

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 帳戶管理: 參考指南

Copyright © 2025 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
的功能 AWS 帳戶 2
您是第一次 AWS 使用嗎？ 3
相關 AWS 服務 3
使用根使用者 4
支援和意見回饋 4
其他 AWS 資源 5
開始使用您的帳戶 6
檢閱先決條件 6
步驟 1：建立您的帳戶 7
步驟 2：為您的根使用者啟用 MFA 9
步驟 3：建立管理員使用者 9
相關主題 10
存取您的帳戶 10
規劃您的控管結構 11
使用多個 的優點 AWS 帳戶 11
管理多個 AWS 帳戶 12
使用時機 AWS Organizations 12
啟用受信任存取 13
啟用委派的管理員帳戶 14
使用 SCPs 限制存取 15
使用時機 AWS Control Tower 17
了解 API 操作模式 18
授予更新帳戶屬性的許可 19
設定您的帳戶 21
建立或更新您的帳戶別名 21
在您的 AWS 區域 帳戶中啟用或停用 21
啟用和停用區域的考量事項 22
啟用或停用獨立帳戶的 區域 25
啟用或停用組織中的區域 27
更新 的帳單 AWS 帳戶 29
更新根使用者電子郵件 29
更新獨立 的根使用者電子郵件AWS 帳戶 30
更新 AWS 帳戶 組織中任何 的根使用者電子郵件 31

更新根使用者密碼 ... 33
更新 AWS 帳戶 名稱 ... 34
更新獨立 的帳戶名稱 AWS 帳戶 ... 35
更新組織中任何 的帳戶名稱 AWS 帳戶 ... 36
更新 的替代聯絡人 AWS 帳戶 ... 38
電話號碼和電子郵件地址需求 ... 39
更新獨立 的替代聯絡人 AWS 帳戶 ... 39
更新 AWS 帳戶 組織中任何 的替代聯絡人 ... 42
account：AlternateContactTypes 內容索引鍵 ... 46
更新 的主要聯絡人 AWS 帳戶 ... 46
電話號碼和電子郵件地址需求 ... 47
更新獨立的主要聯絡人 AWS 帳戶 ... 47
更新 AWS 帳戶 組織中任何 的主要聯絡人 ... 50
檢視您的帳戶識別碼 ... 52
尋找您的 AWS 帳戶 ID ... 53
尋找您 的正式使用者 ID AWS 帳戶 ... 55
保護您的帳戶 ... 58
資料保護 ... 58
AWS PrivateLink ... 59
建立端點 ... 59
Amazon VPC 端點政策 ... 60
端點政策 ... 60
身分和存取權管理 ... 61
目標對象 ... 62
使用身分驗證 ... 62
使用政策管理存取權 ... 65
AWS 帳戶管理和 IAM ... 67
身分型政策範例 ... 74
使用身分型政策 ... 76
故障診斷 ... 78
AWS 受管政策 ... 80
AWSAccountManagementReadOnlyAccess ... 80
AWSAccountManagementFullAccess ... 81
政策更新 ... 82
法規遵循驗證 ... 82
恢復能力 ... 83

基礎架構安全 ... 83
監控您的帳戶 ... 85
CloudTrail 日誌 ... 85
CloudTrail 中的帳戶管理資訊 ... 85
了解帳戶管理日誌項目 ... 86
使用 EventBridge 監控帳戶管理事件 ... 90
帳戶管理事件 ... 90
對您的帳戶進行故障診斷 ... 93
帳戶建立問題 ... 93
帳戶關閉問題 ... 94
我不知道如何刪除或取消我的 帳戶 ... 94
我在帳戶頁面上看不到關閉帳戶按鈕 ... 94
我已關閉我的帳戶，但尚未收到電子郵件確認 ... 94
我在嘗試關閉帳戶時收到「ConstraintViolationException」錯誤 ... 95
我在嘗試關閉成員帳戶時收到「CLOSE_ACCOUNT_QUOTA_EXCEEDED」錯誤 ... 95
在關閉管理帳戶之前，是否需要刪除我的 AWS 組織？ ... 95
其他問題 ... 95
我需要變更我的 的信用卡 AWS 帳戶 ... 95
我需要報告詐騙 AWS 帳戶 活動 ... 96
我需要關閉我的 AWS 帳戶 ... 96
關閉您的帳戶 ... 97
關閉帳戶之前需要知道的資訊 ... 97
如何關閉您的帳戶 ... 98
關閉帳戶後預期會發生的情況 ... 101
關閉後期間 ... 101
重新開啟您的 AWS 帳戶 ... 101
API 參考 ... 102
動作 ... 103
AcceptPrimaryEmailUpdate ... 105
DeleteAlternateContact ... 109
DisableRegion ... 113
EnableRegion ... 116
GetAccountInformation ... 119
GetAlternateContact ... 124
GetContactInformation ... 129
GetPrimaryEmail ... 133

GetRegionOptStatus 136
ListRegions 140
PutAccountName 144
PutAlternateContact 148
PutContactInformation 154
StartPrimaryEmailUpdate 157
相關動作 160
CreateAccount 160
CreateGovCloudAccount 160
DescribeAccount 160
資料類型 160
AlternateContact 162
ContactInformation 164
Region 168
ValidationExceptionField 169
常見參數 169
常見錯誤 171
提出 HTTP 查詢請求 173
端點 174
必要的 HTTPS 174
簽署 AWS 帳戶管理 API 請求 174
配額 175
管理印度的帳戶 177
AWS 帳戶 使用 AWS 印度建立 177
管理您的客戶驗證資訊 179
檢查您的客戶驗證狀態 179
建立您的客戶驗證資訊 179
編輯您的客戶驗證資訊 180
用於客戶驗證的可接受印度證件 180
管理您的 AWS 印度帳戶 182
文件歷史紀錄 183
..... clxxxv

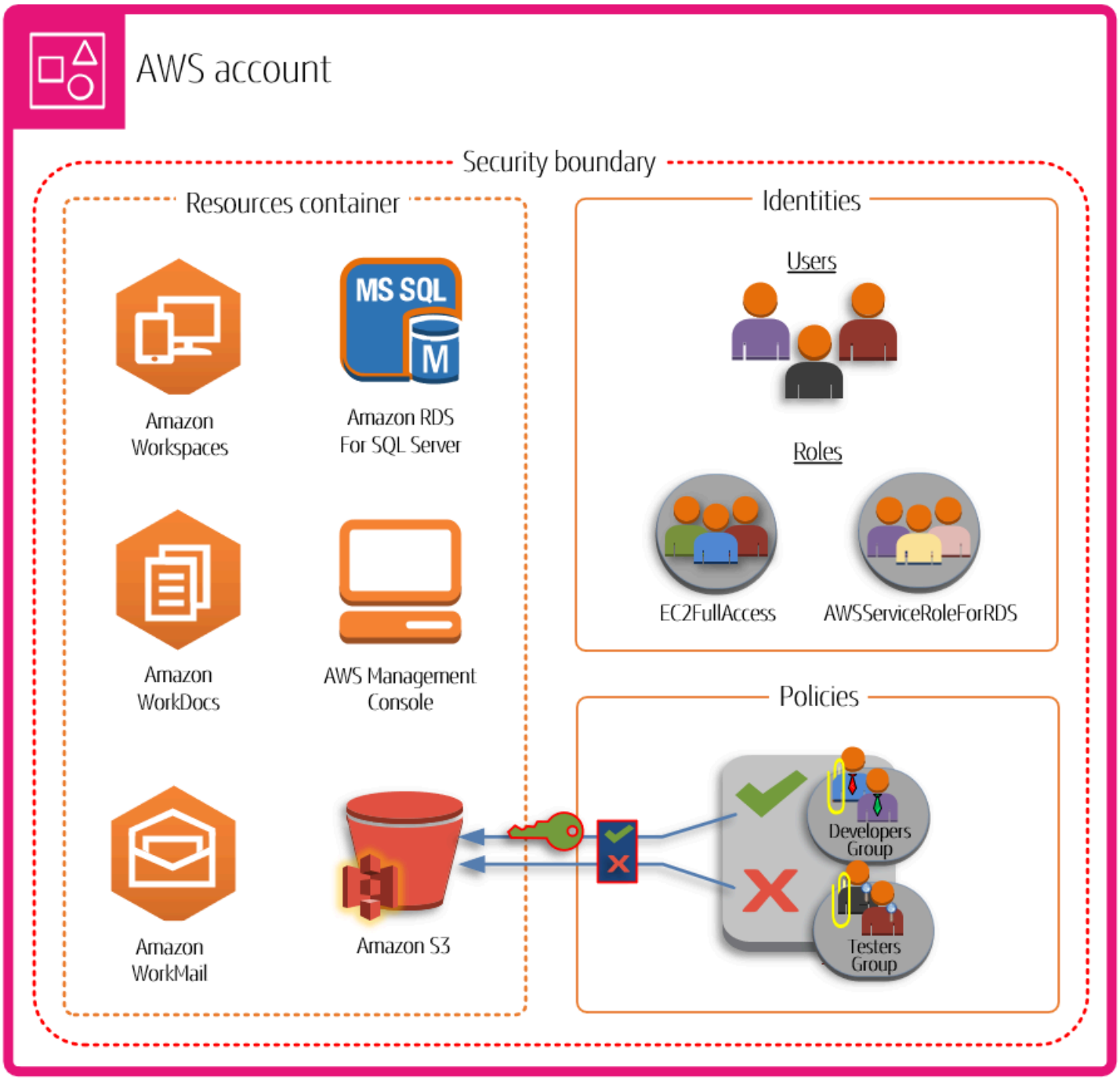
什麼是 AWS 帳戶？

AWS 帳戶 代表您建立的正式商業關係 AWS。您在 中建立和管理 AWS 資源 AWS 帳戶，而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，可區分它與其他 ID AWS 帳戶。

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生產和非生產資源和資料，則根據預設，這些環境之間不允許存取。

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 客戶身分建立的所有 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，而這些動作可能會嚴重影響您的 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、組態錯誤或惡意動作的風險。如果某個帳戶發生問題，則對其他帳戶中包含的工作負載的影響可以減少或消除。
- 鏡像您的業務工作負載 – 使用多個帳戶，將不同帳戶中具有常見業務目的的工作負載分組。因此，您可以讓擁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，讓這些單位的偏離更為容易。

您是第一次 AWS 使用嗎？

如果您是第一次使用 AWS，您的第一個步驟是註冊 AWS 帳戶。當您註冊時， 會使用您提供的詳細資訊 AWS 建立帳戶，並將帳戶指派給您。建立您的 後 AWS 帳戶，以根使用者身分登入，為根使用者啟用多重要素驗證 (MFA)，並將管理存取權指派給使用者。

如需如何設定新帳戶的step-by-step說明，請參閱 入門 AWS 帳戶。

相關 AWS 服務

AWS 帳戶 可無縫搭配下列 服務使用：

- IAM

  您的 AWS 帳戶 與 AWS Identity and Access Management (IAM) 緊密整合。您可以搭配 帳戶使用 IAM，確保在帳戶中工作的其他人員擁有所需的存取權，才能完成其任務。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反映公司特定結構 AWS 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到

可讓您集中管理帳戶的組織。您可以建立會自動成為組織一部分的帳戶，也可以邀請其他帳戶來加入您的組織。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。

- AWS Control Tower

  AWS Control Tower 提供一種簡化的方式來設定和管理安全、多帳戶 AWS 環境。 會使用 AWS Control Tower 自動建立多帳戶環境 AWS Organizations、執行個體化一組初始帳戶，以及環境的一些預設護欄和組態。您可以使用 AWS Control Tower ，在幾個步驟 AWS 帳戶 中佈建新的 ，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

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務 和 資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，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 ，皆可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 Management Console 身分登入 。 AWS

支援 AWS 帳戶管理

您可以使用AWS 帳戶管理支援論壇來發佈意見回饋和問題。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 Management Console。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 – 角色型和特殊課程的連結，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，以協助您使用 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、快速回應的支援管道，可協助您在雲端中建置和執行應用程式。
- 聯絡我們 – 有關 AWS 帳單、帳戶、事件、濫用和其他問題的查詢的中央聯絡窗口。
- 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。

入門 AWS 帳戶

如果您是初次使用 AWS，第一步是註冊 AWS 帳戶。當您這樣做時， AWS 將使用您提供的詳細資訊建立帳戶，並將其指派給您。

本節中的主題將協助您開始了解和設定新的 AWS 帳戶。

主題

- 建立新 的先決條件 AWS 帳戶
- 建立 AWS 帳戶
- 為您的根使用者啟用 MFA
- 建立管理員使用者
- 存取您的 AWS 帳戶

建立新 的先決條件 AWS 帳戶

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。

  > **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。

- AWS 帳戶名稱 – 帳戶的名稱會顯示在數個位置，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，請考慮使用組織用途環境等命名標準（例如 AnyCompany-audit-prod)。對於個人帳戶，請考慮使用命名標準，例如名字-姓氏-用途（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 作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。在驗證完成後， AWS 印度會退還 2 盧比。

- 電話號碼 – 此號碼可用來確認帳戶的所有權。您必須能夠以此電話號碼接聽通話。

> **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。

建立 AWS 帳戶

本主題說明如何建立非 管理 AWS 帳戶 的獨立 AWS Organizations。如果您想要建立屬於 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。

這些指示適用於在印度 AWS 帳戶 以外建立 。如需在印度建立帳戶，請參閱AWS 帳戶 使用 AWS 印度建立。

AWS Management Console

若要建立 AWS 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 ，則此選項可能不存在。反之，選擇登入主控台。然後，如果無法顯示建立新的 AWS 帳戶 ，請先選擇登入不同的 帳戶，然後選擇建立新的 AWS 帳戶。

3. 輸入您的帳戶資訊，然後選擇驗證電子郵件地址。這會將驗證碼傳送至您指定的電子郵件地址。

   > **Important**
   >
   > 由於 帳戶的根使用者具有關鍵性質，我們強烈建議您使用可由 群組存取的電子郵件地址，而非只有個人。如此一來，如果註冊 的人員 AWS 帳戶 離開公司， AWS 帳戶 仍然可以使用 ，因為電子郵件地址仍可存取。

如果您無法存取與 相關聯的電子郵件地址 AWS 帳戶，則如果您遺失密碼，將無法復原對 帳戶的存取權。

4. 輸入您的驗證碼，然後選擇驗證。
5. 為您的根使用者輸入強式密碼，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。
6. 選擇商務或個人。個人帳戶和企業帳戶具有相同的功能和功能。
7. 輸入您的公司或個人資訊。

> **Important**
>
> 對於企業 AWS 帳戶，最佳實務是輸入：
>
> - 公司電話號碼，而不是個人電話號碼。
> - 網域名稱屬於將使用帳戶之公司或組織的電子郵件地址。
>
> 使用個別電子郵件地址或個人電話號碼來設定帳戶的根使用者，可能會使您的帳戶變得不安全。

8. 閱讀並接受AWS 客戶協議。請務必閱讀並了解 AWS 客戶協議的條款。
9. 選擇繼續。此時，您將收到一封電子郵件，以確認您的 AWS 帳戶 已準備好使用。您可以使用您在註冊期間提供的電子郵件地址和密碼來登入您的新帳戶。不過，在完成啟用帳戶之前，您無法使用任何 AWS 服務。
10. 輸入付款方式的相關資訊，然後選擇驗證並繼續。如果您想要使用不同的帳單地址做為 AWS 帳單資訊，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。
11. 從清單中輸入您的國家或地區代碼，然後輸入電話號碼，即可在幾分鐘內聯絡您。
12. 輸入 CAPTCHA 中顯示的程式碼，然後提交。
13. 當自動化系統與您聯絡時，輸入您收到的 PIN，然後提交。

14. 選取其中一個可用的 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。
15. 選擇完成註冊。出現確認頁面，指出您的帳戶正在啟用。
16. 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。

    收到啟用訊息後，您可以完整存取所有 AWS 服務。

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。

您不能使用 AWS Command Line Interface (AWS CLI) 或 AWS API 操作在組織 AWS 帳戶 外部建立獨立 。

為您的根使用者啟用 MFA

我們強烈建議您為根使用者啟用 MFA。MFA 可大幅降低有人未經您的授權存取您帳戶的風險。

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS Management Console身分登入 。在下一頁中，輸入您的密碼。

   如需使用您的根使用者登入的協助，請參閱 登入使用者指南中的以根使用者 AWS Management Console 身分登入 。 AWS
2. 為您的根使用者開啟 MFA。

   如需說明，請參閱《IAM 使用者指南》中的為您的 AWS 帳戶 根使用者（主控台）啟用虛擬 MFA 裝置。

建立管理員使用者

由於您無法限制根使用者可執行的動作，我們強烈建議您不要將根使用者用於未明確要求根使用者的任何任務。相反地，在 IAM Identity Center 中將管理存取權指派給管理使用者，並以該管理使用者身分登入，以執行您的每日管理任務。

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。

相關主題

- 如需保護根使用者憑證的相關資訊，請參閱《IAM 使用者指南》中的保護根使用者的憑證。
- 如需需要根使用者的任務清單，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

存取您的 AWS 帳戶

您可以透過下列 AWS 帳戶 任何方式存取 ：

AWS Management Console

AWS Management Console 是以瀏覽器為基礎的介面，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來執行 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)。 如需有關安裝和使用 的資訊 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 Windows PowerShell 使用者指南。

AWS SDKs

AWS SDKs包含各種程式設計語言和平台 （例如 Java、Python、Ruby、.NET、iOS 和 Android) 的程式庫和範例程式碼。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。如需有關 AWS SDKs 的詳細資訊，包括如何下載和安裝它們，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

雖然您可能已經使用單一帳戶開始 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

AWS 帳戶 在 中形成基礎安全界限 AWS 雲端。它們可做為資源的容器，提供重要的隔離層，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？。

將資源分開， 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 來託管工作負載中受支付卡產業 (PCI) 安全標準規範的所有元素。
- 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設定檔，可能會有不同的安全需求。
- 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。這有助於控制對高度私有資料的暴露，因此有助於遵守歐盟的一般資料保護法規 (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程序。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的帳單層級分隔項目。您仍然可以在明細項目分隔時，將所有帳單合併到單一付款人（使用 AWS Organizations 和 合併帳單）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、彈性和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，而不會在成長時影響您的持續操作。

管理多個 AWS 帳戶

開始新增多個帳戶之前，您會想要開發管理帳戶的計劃。因此，我們建議您使用 AWS Organizations，這是免費 AWS 服務，可管理組織中的所有 AWS 帳戶 。

AWS 也提供 AWS Control Tower，可將受 AWS 管自動化層新增至 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

AWS Organizations 是一項 AWS 服務，可用來以群組 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。您也可以使用政策型控制項，集中管理組織的安全性。如需詳細資訊 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 和該 AWS 服務之間的信任存取，將此額外功能擴展到其他 服務。信任的存取會授予指定 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 的信任存取時，Account Management 服務會授予 Organizations 及其管理帳戶許可，以存取所有組織成員帳戶的中繼資料，例如主要或替代聯絡資訊。

如需詳細資訊，請參閱為 AWS 帳戶管理啟用受信任存取。

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擁有組織的所有管理存取權。

如需詳細資訊，請參閱為 AWS 帳戶管理啟用委派的管理員帳戶。

服務控制政策

當您的 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動作。SCP 永遠不會授予許可；而是會限制成員帳戶可使用之許可的篩選條件。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主體修改其帳戶的替代聯絡人。

如需適用於 SCPs AWS 帳戶，請參閱 使用 AWS Organizations 服務控制政策限制存取。

為 AWS 帳戶管理啟用受信任存取

啟用 AWS Account Management 的受信任存取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，主要或備用聯絡詳細資訊）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 。如需受信任存取的運作方式的一般資訊，請參閱搭配使用 AWS OrganizationsAWS 與其他 服務。

啟用受信任存取後，您可以在支援 參數的那些帳戶管理 API 操作中使用 `accountID` 參數。只有在您從 管理帳戶使用登入資料呼叫 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，請參閱為 AWS 帳戶管理啟用委派的管理員帳戶。

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 Management Console

啟用 AWS Account Management 的信任存取

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 帳戶管理的信任存取對話方塊中，輸入啟用以確認，然後選擇啟用信任存取。

AWS CLI & SDKs

啟用 AWS Account Management 的信任存取

執行下列命令之後，您可以使用組織的管理帳戶中的登入資料來呼叫帳戶管理 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

  下列範例為呼叫 AWS 帳戶組織中的帳戶管理啟用受信任存取。

  ```
  $ 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。

為 AWS 帳戶管理啟用委派的管理員帳戶

您可以啟用委派的管理員帳戶，以便呼叫其他成員帳戶 AWS 的帳戶管理 API 操作 AWS Organizations。在您為組織註冊委派的管理員帳戶之後，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。

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 Account Management 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。

  執行此命令之後，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 Management Console

AWS Account Management 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

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以執行的動作。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 `PutAlternateContact`和 `DeleteAlternateContact` API 操作在獨立帳戶模式下被任何成員帳戶呼叫。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。

```
{
    "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，如果 SCP 適用於該帳戶，也無法變更組織中任何帳戶的任何替代聯絡人。

```
{
    "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。這會導致指定 OUs 中任何帳戶中的委託人無法修改自己的替代聯絡人。

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

使用時機 AWS Control Tower

AWS Organizations 是基礎服務，可讓您集中管理和保護整個 AWS 環境。此以 AWS Organizations為中心方法的關鍵元件是 AWS Control Tower。 在 Organizations 中 AWS Control Tower 充當管理主控台，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。 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治理方法對於希望充分利用 的強大功能， AWS 雲端同時保持最高標準的安全性和合規的企業至關重要。

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

使用 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 Account Management AWS CLI 或 AWS SDK 操作時，當您不包含 `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相同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 Account Management 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，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，就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的語法的 ARN。

授予更新帳戶屬性的許可

與大多數 AWS 操作一樣，您授予 AWS 帳戶 使用 IAM 許可政策來新增、更新或刪除 帳戶屬性的許可。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時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 的 Amazon Resource Name (ARN)，會根據您想要參考的帳戶是獨立帳戶或組織中的帳戶而有不同的建構方式。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，您必須使用此格式，方法為不包含 `AccountID` 參數。
  - 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，您必須包含 `AccountID` 參數，以使用此格式。

IAM 政策的內容索引鍵

Account Management 服務也提供數個 Account Management 服務特有的條件金鑰，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兩個指定 OUs 之一的帳戶。

由於 `account:AccountResourceOrgPaths` 是多值字串類型，因此您必須使用 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。如需使用標籤做為屬性型存取控制策略一部分的資訊，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 標籤且 索引鍵`project`為 `blue`或 值的帳戶`red`。

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是 。

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

> **Note**
>
> 您只能將標籤連接至組織中的帳戶。您無法將標籤連接至獨立 AWS 帳戶。

設定您的 AWS 帳戶

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 India) 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
- 在您的 AWS 區域 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

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。

在您的 AWS 區域 帳戶中啟用或停用

AWS 區域 是全球的實體位置，我們擁有多個可用區域。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。如需可用和近期區域的地圖，請參閱 區域和可用區域。

除非您明確使用 AWS 服務提供的複寫功能，否則您在一個區域中建立的資源不存在於任何其他 區域。例如，Amazon S3 和 Amazon EC2 支援跨區域複寫。有些服務，例如 AWS Identity and Access Management (IAM) 沒有區域資源。

您的帳戶決定您可用的區域。

- AWS 帳戶 提供多個區域，讓您可以在符合您需求的位置啟動 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。
- An AWS GovCloud （美國西部） 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)。
- Amazon AWS （中國） 帳戶僅提供北京和寧夏區域的存取權。如需詳細資訊，請參閱 Amazon Web Services in China (Amazon Web Services (中國))。

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，而不是全域端點來降低延遲。區域 AWS STS 端點的工作階段權杖在所有 AWS 區域中都有效。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。如果您想要為您的帳戶啟用新的區域，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。在所有區域中有效的工作階段字符較大。如果您存放工作階段字符，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AWS STS 在 AWS 區域中管理 。

主題

- 啟用和停用區域的考量事項
- 啟用或停用獨立帳戶的 區域
- 啟用或停用組織中的區域

啟用和停用區域的考量事項

啟用或停用區域之前，請務必考量下列事項：

- 在 2019 年 3 月 20 日之前引進的區域預設為啟用 – AWS AWS 區域 最初預設會啟用所有新的，這表示您可以立即開始在這些區域中建立和管理資源。您無法啟用或停用預設啟用的區域。今天，當 AWS 新增區域時，預設會停用新區域。如果您希望使用者能夠在新區域中建立和管理資源，您首先需要啟用該區域。下列區域預設為啟用。

名稱	代碼
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
亞太區域 (東京)	ap-northeast-1
亞太區域 (首爾)	ap-northeast-2
亞太區域 (大阪)	ap-northeast-3
亞太區域 (孟買)	ap-south-1
亞太區域 (新加坡)	ap-southeast-1
亞太區域 (悉尼)	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

- 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，它們會自動選取所選地理位置中未針對資源和 IAM 資料啟用的最佳 AWS 區域區域。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。
- 啟用區域是免費的 – 啟用區域是免費的。您只需為在新區域中建立的資源付費。
- 停用區域會停用區域中資源的 IAM 存取 – 如果您停用仍包含 AWS 資源的區域，例如 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，您會失去該區域中資源的 IAM 存取。例如，您無法使用 AWS Management Console 來檢視或變更已停用區域中任何 EC2 執行個體的組態。
- 如果您停用區域，作用中資源的費用會繼續 – 如果您停用仍包含 AWS 資源的區域，則這些資源（如果有的話）的費用會以標準費率繼續累積。例如，若您停用的區域中含有 Amazon EC2 執行個體，即使您已無法存取該等執行個體，仍須為執行個體付費。
- 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。
- 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。
- 組織可以在整個 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。
- 單一帳戶在任何指定時間都可以有 6 個進行中的區域選項請求 – 一個請求等於對一個帳戶啟用或停用一個特定區域。
- Amazon EventBridge 整合 – 客戶可以在 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`

您無法在處於 或 DISABLING 狀態時取消選擇加入ENABLING或選擇退出。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 服務仍可能無法立即使用ENABLED。

- 與 完全整合 AWS Organizations – 管理帳戶可以修改或讀取該 AWS 組織任何成員帳戶的 region-opt。成員帳戶也可以讀取/寫入其區域狀態。

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。以下 AWS Management Console 程序一律僅適用於獨立內容。您可以使用 AWS Management Console 來僅檢視或更新您用來呼叫 操作之帳戶中的可用區域。

AWS Management Console

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 Management Console 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。

> **Note**
>
> 系統可能會提示您核准存取此資訊。 AWS 會傳送請求到與帳戶相關聯的電子郵件地址，以及主要聯絡電話號碼。選擇請求中的連結以在瀏覽器中開啟連結，並核准存取權。

4. 在動作欄中 AWS 區域 具有 選項的每個 旁邊，選擇啟用或停用，取決於您是否希望帳戶中的使用者能夠建立和存取該區域中的資源。
5. 如果出現提示，請確認您的選擇。
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，您必須具有映射至該操作的許可：
>
> - `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 為 AWS 帳戶管理啟用受信任存取。

AWS Management Console

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，您必須具有映射至該操作的許可：
>
> - `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

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

您可能需要更新根使用者電子郵件地址的商業原因有很多 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 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 的根使用者電子郵件AWS 帳戶。

- 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 主控台集中更新成員帳戶的根使用者電子郵件，或透過 CLI 和 SDKs AWS 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 的根使用者電子郵件AWS 帳戶
- 更新 AWS 帳戶 組織中任何 的根使用者電子郵件

更新獨立 的根使用者電子郵件AWS 帳戶

若要編輯獨立 的根使用者電子郵件地址 AWS 帳戶，請執行下列程序的步驟。

AWS Management Console

> **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 Management Console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，電子郵件地址旁選擇編輯。
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的欄位，並確認您目前的密碼。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 分鐘才能送達。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

AWS CLI 中或其中一個 AWS SDKs API 操作不支援此任務。您只能使用 來執行此任務 AWS Management Console。

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 的帳戶頁面更新成員帳戶的根使用者電子郵件地址。AWS Management Console 如需step-by-step說明，請遵循 中提供的步驟更新獨立 的根使用者電子郵件AWS 帳戶。

AWS Management Console

> **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此程序，您必須啟用帳戶管理服務的信任存取。
> - 您不能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，選擇您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，您可以在傳送程式碼後的 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。

> **最低許可**
>
> 對於每個操作，您必須擁有映射至該操作的許可：
>
> - `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的能力資訊，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

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 Management Console

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 Management Console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，於密碼旁邊選擇編輯。
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

AWS CLI 中或其中一個 AWS SDKs API 操作不支援此任務。您只能使用 來執行此任務 AWS Management Console。

更新 AWS 帳戶 名稱

管理多個時 AWS 帳戶，請使用與業務單位和應用程式一致的明確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，請考慮使用組織用途環境（例如 sales-catalog-prod) 等命名標準。基於隱私權和安全性考量，請避免使用反映個人身分識別資訊 (PII) 的帳戶名稱。

- 獨立 AWS 帳戶 – 對於 AWS 帳戶 未與組織相關聯的 ，您可以使用 AWS Management Console或 AWS CLI 和 SDKs來更新您的帳戶名稱。若要了解如何操作，請參閱 更新獨立 的帳戶名稱 AWS 帳戶。

- 在AWS 帳戶 組織中 – 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 的帳戶名稱 AWS 帳戶。

> **Note**
>
> 變更 最多 AWS 帳戶 可能需要四小時才能傳播到任何地方。

主題

- 更新獨立 的帳戶名稱 AWS 帳戶
- 更新組織中任何 的帳戶名稱 AWS 帳戶

更新獨立 的帳戶名稱 AWS 帳戶

若要變更獨立 的帳戶名稱 AWS 帳戶，請執行下列程序中的步驟。

AWS Management Console

> **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 Management Console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 的帳戶名稱 AWS 帳戶

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 為 AWS 帳戶管理啟用受信任存取。

AWS Management Console

> **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：//https://console.aws.amazon.com/organizations/ 開啟 Organizations 主控台。
2. 在左側導覽窗格中，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

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 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替代聯絡人 AWS 帳戶，請執行下列程序中的步驟。以下 AWS Management Console 程序一律僅適用於獨立內容。您可以使用 AWS Management Console 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 Management Console

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 Management Console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具有上述最低許可的人員身分登入。

4. 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。

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受信任存取。

> **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": "CFO"
    }
}
```

Example

下列範例會設定發起人帳戶的新操作替代聯絡人。

```
$ 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，而所有連續的對相同 的呼叫 AWS 帳戶 和聯絡類型都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 的替代聯絡詳細資訊，請執行下列程序的步驟。

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，才能管理成員帳戶上的設定。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 為 AWS 帳戶管理啟用受信任存取。

> **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 Management Console

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 AWS 帳戶中選取您要更新的帳戶。
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": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

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，而所有連續的對相同 的呼叫 AWS 帳戶 和聯絡類型都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）三種帳單類型中的哪一種。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，但不會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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "account:GetAlternateContact",
            "Resource": [
                "arn:aws:account::123456789012:account/o-aa111bb222/111111111111"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "account:AlternateContactTypes": [
                        "BILLING"
                    ]
                }
            }
        }
    ]
}
```

更新 的主要聯絡人 AWS 帳戶

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。

根據帳戶是否為獨立帳戶或組織的一部分，您可以不同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任何成員帳戶。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
- 更新獨立的主要聯絡人 AWS 帳戶
- 更新 AWS 帳戶 組織中任何 的主要聯絡人

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，且在國家/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連字號或空格 "-"。例如，+12025550179。
- 基於安全考量，電話號碼必須能夠從 接收簡訊 AWS。不接受免付費電話號碼，因為大多數不支援簡訊。
- 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根使用者，可能會讓您的帳戶難以復原，如果該個人離開公司。

更新獨立的主要聯絡人 AWS 帳戶

若要編輯獨立 的主要聯絡人詳細資訊 AWS 帳戶，請執行下列程序的步驟。以下 AWS Management Console 程序一律僅適用於獨立內容。您可以使用 AWS Management Console 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 Management Console

編輯獨立 的主要聯絡人 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: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 Management Console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，然後在其旁邊選擇編輯。
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受信任存取。

> **最低許可**
>
> 對於每個操作，您必須擁有映射至該操作的許可：
>
> - `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 AWS 帳戶 組織中任何 的主要聯絡人

若要編輯組織中任何 AWS 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

若要使用 AWS Organizations 主控台更新主要聯絡人，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 為 AWS 帳戶管理啟用受信任存取。

AWS Management Console

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 中AWS 帳戶，選取要更新的帳戶。
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受信任存取。

- 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：

- `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。

檢視 AWS 帳戶 識別符

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 Management Console 帳戶 ID 或帳戶別名登入 。雖然 帳戶 IDs 與任何識別資訊一樣，都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`，是混淆形式的 AWS 帳戶 ID。您可以使用此 ID 來識別 AWS 帳戶 ，使用 Amazon Simple Storage Service (Amazon S3) 授予儲存貯體和物件的跨帳戶存取權。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 AWS 帳戶 識別符才能與您共用 AWS 資源的第三方。這樣做會讓他們存取您擁有 AWS 帳戶 的 。

尋找您的 AWS 帳戶 ID

您可以使用 AWS Management Console 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。無論您是以根使用者或 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 Management Console

以根使用者身分登入時尋找您的 AWS 帳戶 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。

   > **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

> **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
```

尋找您的帳戶 ID 做為 IAM 使用者

AWS Management Console

以 IAM 使用者身分登入時尋找您的 AWS 帳戶 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：
>
> - `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。

   > **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 Management Console 或 找到 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 Management Console

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，您必須具備：
> - `account:GetAccountInformation`

1. 以根使用者或 IAM 使用者 AWS Management Console 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，請尋找其旁邊的項目帳戶和帳戶 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 Management Console

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 Management Console 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
```

AWS 帳戶管理中的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以從資料中心和網路架構中受益，該架構旨在滿足最安全敏感組織的需求。

安全性是 AWS 和 之間的共同責任。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。第三方稽核人員會定期測試和驗證我們安全的有效性，做為AWS 合規計畫的一部分。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。
- 雲端安全 – 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

本文件可協助您了解如何在使用 AWS 帳戶管理時套用共同的責任模型。其中說明如何設定 Account Management 以符合您的安全和合規目標。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。

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
- AWSAWS Account Management 的 受管政策
- AWS 帳戶管理的合規驗證
- AWS 帳戶管理中的彈性
- 中的基礎設施安全性 AWS 帳戶管理

AWS Account Management 中的資料保護

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。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

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 或其他 AWS 服務 使用主控台、API AWS CLI或 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

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，而不必跨公有網際網路。

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 連線至其他服務 AWS 。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》中的界面 VPC 端點 (AWS PrivateLink)。

建立端點

您可以使用 AWS Management Console、 (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 AWS 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》中的建立介面端點。

> **Note**
>
> 當您建立端點時，請使用下列格式，將帳戶管理指定為您希望 VPC 連線的服務：
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> 您必須完全如所示使用字串，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 AWS CloudFormation，請參閱AWS 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：

- 適用於帳戶管理的 Amazon Virtual Private Cloud 端點政策
- 使用 AWS PrivateLink 指南中的 VPC 端點控制對 服務的存取。

適用於帳戶管理的 Amazon Virtual Private Cloud 端點政策

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 使用者同時擷取和變更任何替代聯絡資訊 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。

```
{
```

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

如果您想要將屬於 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，則該`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 AWS 服務 您可以免費使用的 。

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) 會有所不同，取決於您在帳戶管理中所做的工作。

服務使用者 – 如果您使用帳戶管理服務來執行任務，管理員會為您提供所需的登入資料和許可。當您使用更多帳戶管理功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取帳戶管理中的功能，請參閱 故障診斷 AWS 帳戶管理身分和存取權。

服務管理員 – 如果您在公司負責帳戶管理資源，您可能擁有帳戶管理的完整存取權。您的任務是判斷服務使用者應存取的帳戶管理功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何透過帳戶管理使用 IAM，請參閱 AWS 帳戶管理如何與 IAM 搭配使用。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解如何撰寫政策以管理帳戶管理存取權的詳細資訊。若要檢視您可以在 IAM 中使用的帳戶管理身分型政策範例，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 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 （登入 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 《 使用者指南》中的如何登入您的 AWS 帳戶 。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需

使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重驗證 (MFA) 來提高帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的多重要素驗證和《IAM 使用者指南》中的 IAM 中的AWS 多重要素驗證。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務 和 資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，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

根據最佳實務， 要求人類使用者，包括需要管理員存取權的使用者，使用 聯合身分提供者 AWS 服務 來使用臨時憑證來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、 Identity Center 目錄或任何使用透過身分來源提供的登入資料 AWS 服務 存取的使用者。當聯合身分存取時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時登入資料。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，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 使用者是 中的身分 AWS 帳戶 ，具有單一人員或應用程式的特定許可。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色（主控台）。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。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。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在其中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。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》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。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權給 AWS 服務。

- 服務連結角色 – 服務連結角色是一種連結至 的服務角色。 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。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

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。政策是 中的物件， AWS 當與身分或資源相關聯時， 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

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。

預設情況下，使用者和角色沒有許可。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。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console AWS CLI、 或 API AWS 取得角色資訊。

身分型政策

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。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 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。

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。

存取控制清單 (ACL)

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。

Amazon S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個 的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，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) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括支援 RCPs AWS 服務 的 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 (RCPs)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作

階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。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

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
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 Account Management 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。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。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，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當委託人和資源位於不同位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體 （使用者或角色） 存取資源的許可。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。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。

帳戶管理的政策動作

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，哪個主體在什麼条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。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

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。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

Account Management 服務支援 IAM 政策`Resources`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 (或 `Condition` 區塊) 可讓您指定使陳述式生效的條件。`Condition` 元素是選用項目。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。

若您在陳述式中指定多個 `Condition` 元素，或是在單一 `Condition` 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值， 會使用邏輯`OR`操作 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定的條件金鑰。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：

  - 計費
  - 操作
  - SECURITY

  使用此金鑰可讓您篩選僅針對指定替代聯絡類型的動作的請求。

- 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。

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 中 AWS，這些屬性稱為標籤。您可以將標籤連接到 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索引鍵 "CostCenter" 且值為 "12345" 或 "67890" 之帳戶的聯絡資訊。

```
{
   "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

當您使用臨時登入資料登入時，有些 AWS 服務 無法運作。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的使用 IAM 的 。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則會使用暫時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取 時，該程序會自動建立臨時登入資料。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的從使用者切換至 IAM 角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 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 中的暫時性安全憑證。

Account Management 的跨服務主體許可

支援轉寄存取工作階段 (FAS)：是

當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。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權給 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。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在表格中尋找服務，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

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。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。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。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

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 Management Console
- 提供 中帳戶頁面的唯讀存取權 AWS Management Console
- 提供 中帳戶頁面的完整存取權 AWS Management Console

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 等使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 AWS 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》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html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 Management Console

若要存取 中的帳戶頁面 AWS Management Console，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。反之，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 Management Console

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 Management Console。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。

```
{
    "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 Management Console

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 Management Console。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。

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

針對 AWS 帳戶管理使用身分型政策 (IAM 政策）

如需 AWS 帳戶 和 IAM 使用者的完整討論，請參閱《IAM 使用者指南》中的什麼是 IAM？。

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 Management Console，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	描述
`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。
`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。 **Note** 此許可僅適用於主控台。此許可沒有可用的 API 存取權。

許可名稱	存取層級	描述
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。
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。

故障診斷 AWS 帳戶管理身分和存取權

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。

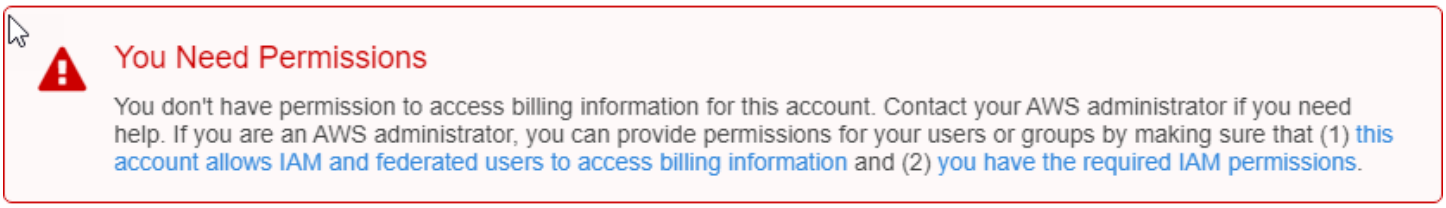
主題

- 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 Management Console 通知您未獲授權執行 動作，則您必須聯絡管理員尋求協助。您的管理員是提供您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 Management Console 但沒有 account:GetAccountInformation許可時，會發生下列範例錯誤。



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 的 IAM `marymajor` 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 沒有將角色傳遞至該服務的許可。

```
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。

AWSAWS Account Management 的 受管政策

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見使用案例提供許可，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。我們建議您定義使用案例專屬的客戶管理政策，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 受管政策中 AWS 定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。當新的 AWS 服務 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 Management Console。

```
{
    "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，或啟用或停用 區域的）

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 Management Console。

```
{
```

```
    "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，帳戶管理受 AWS 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 帳戶管理使用新的 AWS 受管政策啟動，並開始追蹤變更	帳戶管理最初使用下列 AWS 受管政策啟動： • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	2021 年 9 月 30 日

AWS 帳戶管理的合規驗證

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 依合規計劃清單。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。

您在 中使用 服務的合規責任 AWS 帳戶 取決於資料的敏感度、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，並提供以 AWS 安全與合規為重心的基準環境部署步驟。
- 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 – 此工作手冊和指南的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 – 這 AWS 服務 可讓您全面檢視 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，以及符合法規和產業標準的方式。

AWS 帳戶管理中的彈性

AWS 全域基礎設施是以 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。

中的基礎設施安全性 AWS 帳戶管理

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 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱 Security Pillar 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

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、報告錯誤，並在適當時採取自動動作：

- AWS CloudTrail 會擷取（日誌）API 呼叫，以及由 或代表您發出的相關事件， AWS 帳戶 並將日誌檔案寫入您指定的 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》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/。
- 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

AWS Account Management APIs 已與 整合 AWS CloudTrail，此服務提供使用者、角色或呼叫 Account Management 操作 AWS 的服務所採取動作的記錄。CloudTrail 會將所有 Account Management API 呼叫擷取為事件。擷取的呼叫包括所有對帳戶管理操作的呼叫。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 主控台中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。當使用 Account Management 操作進行活動時，CloudTrail 會記錄 CloudTrail 事件中的活動，以及事件歷史記錄中的其他服務 AWS 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 Management Console，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。您可以設定其他服務 AWS ，以進一步分析 CloudTrail 日誌中收集的事件資料並對其採取行動。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：

- 請求是使用根使用者還是 AWS Identity and Access Management (IAM) 使用者登入資料提出
- 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
- 該請求是否由其他 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，以擷取帳戶目前的`OPERATIONS`替代聯絡人。操作傳回的值不包含在記錄的資訊中。

Example 範例 1

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
```

```
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T19:25:53Z"
      }
    }
  },
  "eventTime": "2021-04-30T19:26:15Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "GetAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "SECURITY"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

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": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "PutAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "name": "*Alejandro Rosalez*",
    "emailAddress": "alrosalez@example.com",
    "title": "CFO",
    "alternateContactType": "BILLING"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

範例 3：下列範例顯示 CloudTrail 日誌項目，用於呼叫 `DeleteAlternateContact`操作以刪除目前的`OPERATIONS`替代聯絡人。


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "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

Amazon EventBridge，先前稱為 CloudWatch Events，可協助您監控特定於 的事件，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。

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，非同步任務會啟動。初始請求將記錄為目標帳戶中的 CloudTrail 事件。此外，當啟用或停用程序開始時，EventBridge 事件將傳送至呼叫帳戶，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`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"
      ]
   }
```

```
}
```

對 進行故障診斷 AWS 帳戶

使用下列主題中的資訊，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》中的根使用者問題故障診斷。如需登入程序的協助，請參閱 AWS 登入使用者指南中的對登入 AWS 帳戶 問題進行故障診斷。

故障診斷主題

- 對建立的問題 AWS 帳戶 進行故障診斷
- 對關閉問題 AWS 帳戶 進行故障診斷
- 對 的其他問題進行故障診斷 AWS 帳戶

對建立的問題 AWS 帳戶 進行故障診斷

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	建立 AWS 帳戶	本指南
如果我沒有收到來自 的呼叫 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，我的帳戶未啟用	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。

對關閉問題 AWS 帳戶 進行故障診斷

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，但尚未收到電子郵件確認
- 我在嘗試關閉帳戶時收到「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，則不會看到帳戶頁面上顯示的關閉帳戶按鈕。您必須以根使用者的 AWS Management Console 身分登入 ，才能關閉您的帳戶。如果您無法登入，請參閱疑難排解根使用者的問題。

我已關閉我的帳戶，但尚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 Management Console 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，您可以檢查關閉的帳戶是否在 AWS Organizations 主控台SUSPENDED中標記為 ，以確認成功關閉。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，並確定其帳戶名稱Suspended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 Management Console 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

在連續 30 天內，您僅可關閉 10% 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。在初次關閉帳戶後的 30 天內，不可超過 10% 的帳戶關閉限制。帳戶關閉下限為 10，帳戶關閉上限為 1000，即使 10% 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，並確定其帳戶名稱Suspended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

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 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

我需要變更我的 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 已具備保護，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

如果您懷疑使用 進行詐騙活動， AWS 帳戶 並想要提出報告，請參閱如何報告資源濫用 AWS。

如果您在 Amazon.com 上購買時遇到問題，請參閱 Amazon Customer Service。

我需要關閉我的 AWS 帳戶

如需關閉 時發生問題的故障診斷說明 AWS 帳戶，請參閱 關閉 AWS 帳戶。

關閉 AWS 帳戶

如果您不再需要您的 AWS 帳戶，您可以隨時遵循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。您關閉帳戶當日到 AWS 永久關閉帳戶之間的時間範圍稱為關閉後期間。

關閉帳戶之前需要知道的資訊

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 AWS 此帳戶客戶協議的通知。
- 關閉資源 AWS 帳戶 之前，您不需要刪除 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帳戶。如果您重新開啟帳戶，保留在帳戶中的服務費用將會重新啟動。您仍需負責任何未支付發票和未完成的預留執行個體和 Savings Plans。
- 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，則 2 月初將收到 1 月 1 日至 1 月 15 日期間產生的用量帳單。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和存取已關閉 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。
- 您不能使用與關閉 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。
- 如果您已在 AWS 帳戶 根使用者上啟用多重要素驗證 (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，硬體 TOTP 字符裝置無法在永久關閉您的帳戶後與其他使用者建立關聯。如果您想要稍後將硬體 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。

- 在連續 30 天內，您僅可關閉 10% 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。在初次關閉帳戶後的 30 天內，不可超過 10% 的帳戶關閉限制。帳戶關閉下限為 10，帳戶關閉上限為 1000，即使 10% 的帳戶超過 1000。如需 Organizations 配額的詳細資訊，請參閱 的配額 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

- AWS Marketplace 帳戶關閉時不會自動取消訂閱。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 會在暫停網域之前，傳送每日電子郵件最多五天。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，我的網域已向 Route 53 註冊。
- 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。如需有關如何在關閉 AWS 帳戶 後請求刪除追蹤的詳細資訊，請參閱《CloudTrail 使用者指南》中的AWS 帳戶 關閉和追蹤。

如何關閉您的帳戶

您可以使用 AWS 帳戶 下列程序來關閉您的 。請注意，根據您要關閉的帳戶類型 【獨立帳戶、成員帳戶、管理帳戶和 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 對關閉問題 AWS 帳戶 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 您要關閉之 中的根使用者 AWS Management Console 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），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的 API 操作不支援此任務。您只能使用 來執行此任務 AWS Management Console。

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 Close (關閉)。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會在其帳戶名稱旁，於 AWS Organizations 主控台中顯示SUSPENDED標籤，最長至原始關閉日期後 90 天。90 天後，成員帳戶將不再顯示在 中 AWS Organizations。

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 Management Console。 如需step-by-step指引，請遵循獨立帳戶索引標籤中的指示。

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 Management Console 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Suspended旁邊。如果您有仍在作用中的成員帳戶，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），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的 API 操作不支援此任務。您只能使用 來執行此任務 AWS Management Console。

AWS GovCloud (US) account

AWS GovCloud (US) 帳戶一律連結至單一標準 AWS 帳戶 ，用於計費和付款。

關閉 AWS GovCloud (US) 帳戶

如果您有 AWS 帳戶 連結至 AWS GovCloud (US) 帳戶的 ，則需要先關閉標準帳戶，再關閉帳戶 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 對關閉問題 AWS 帳戶 進行故障診斷。
- 您關閉的任何成員帳戶都會在 AWS Organizations 主控台中顯示其帳戶名稱旁的SUSPENDED標籤，最長可達原始關閉日期的 90 天後。90 天後，成員帳戶將不再顯示在 AWS Organizations 主控台中。
- 如果您已將 中的服務存取許可授予 AWS 帳戶 其他 帳戶，則從這些帳戶提出的任何存取請求在帳戶關閉後都應失敗。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，就無法重複使用其 AWS 帳戶 ID。

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。若要在帳戶永久關閉之前重新開啟您的帳戶，(1) 您必須AWS 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，保留在帳戶中的服務費用將會重新啟動。

API 參考

Account Management (`account`) 命名空間中的 API 操作可讓您修改您的 AWS 帳戶。

每個 都 AWS 帳戶 支援具有帳戶相關資訊的中繼資料，包括與帳戶相關聯的最多三個替代聯絡人的相關資訊。這些是與 帳戶根使用者相關聯的電子郵件地址之外的。您只能指定與 帳戶相關聯的下列任一聯絡類型。

- 帳單聯絡人
- 操作聯絡人
- 安全聯絡人

根據預設，本指南中討論的 API 操作會直接套用至呼叫操作的帳戶。呼叫 操作的帳戶中的身分通常是 IAM 角色或 IAM 使用者，且必須具有 IAM 政策套用的許可才能呼叫 API 操作。或者，您可以從 管理帳戶中的身分呼叫這些 API AWS Organizations 操作，並指定屬於組織成員的任何 AWS 帳戶 的帳戶 ID 號碼。

API 版本

此版本的帳戶 API 參考記錄了帳戶管理 API 2021-02-01 版。

> **Note**
>
> 除了直接使用 API 之外，您也可以使用其中一個 AWS SDKs，其中包含程式庫和範例程式碼，可用於各種程式設計語言和平台 (Java、Ruby、.NET、iOS、Android 等）。SDKs提供便捷的方式，以建立對 AWS Organizations 的程式設計存取。例如，SDKs會處理密碼編譯簽署請求、管理錯誤，以及自動重試請求。如需有關 AWS SDKs 的詳細資訊，包括如何下載和安裝它們，請參閱適用於 Amazon Web Services 的工具。

我們建議您使用 AWS SDKs 對帳戶管理服務進行程式設計 API 呼叫。不過，您也可以使用帳戶管理查詢 API 直接呼叫帳戶管理 Web 服務。若要進一步了解帳戶管理查詢 API，請參閱《帳戶管理使用者指南提出 HTTP 查詢請求以呼叫 API》中的 。Organizations 支援所有動作的 GET 和 POST 請求。也就是說，API 不會要求您在某些動作上使用 GET，在其他動作上使用 POST。不過，GET 請求受限於 URL 的限制大小。因此，對於需要較大大小的操作，請使用 POST 請求。

簽署請求

當您傳送 HTTP 請求至 時 AWS，您必須簽署請求，讓 AWS 可以識別傳送這些請求的對象。您可以使用 AWS 存取金鑰簽署請求，其中包含存取金鑰 ID 和私密存取金鑰。強烈建議您不要為根帳戶建立存取金鑰。擁有根帳戶存取金鑰的任何人，皆可不受限制地存取您帳戶中的所有資源。反之，請為具有管理權限的 IAM 使用者建立存取金鑰。另一個選項是使用 AWS Security Token Service 來產生臨時安全憑證，並使用這些憑證來簽署請求。

若要簽署請求，建議您使用 Signature 第 4 版。如果您有使用 Signature 第 2 版的現有應用程式，則不需要更新它即可使用 Signature 第 4 版。不過，有些操作現在需要 Signature 第 4 版。需要第 4 版的操作文件指出此需求。如需詳細資訊，請參閱《IAM 使用者指南》中的簽署 AWS API 請求。

當您使用 AWS 命令列界面 (AWS CLI) 或其中一個 AWS SDKs來向 發出請求時 AWS，這些工具會自動使用您在設定工具時指定的存取金鑰來簽署請求。

帳戶管理的支援和意見回饋

我們誠摯歡迎您提供意見回饋。將您的意見傳送至 feedback-awsaccounts@amazon.com，或在帳戶管理支援論壇中張貼您的意見回饋和問題。如需 AWS 支援論壇的詳細資訊，請參閱論壇說明。

範例的呈現方式

Account Management 傳回的 JSON 作為對請求的回應，會以單一長字串傳回，沒有換行或格式化空格。本指南中的範例會同時顯示換行和空格，以改善可讀性。當範例輸入參數也會導致長字串超出畫面時，我們會插入換行符號以增強可讀性。您應該一律以單一 JSON 文字字串的形式提交輸入。

記錄 API 請求

Account Management 支援 CloudTrail，這是一種記錄 AWS API 呼叫您的 AWS 帳戶 並將日誌檔案交付至 Amazon S3 儲存貯體的服務。透過使用 CloudTrail 所收集的資訊，您可以判斷哪些請求已成功向帳戶管理、提出請求的人員、提出時間等等提出。如需 Account Management 及其對 CloudTrail 支援的詳細資訊，請參閱使用 記錄 AWS 帳戶管理 API 呼叫 AWS CloudTrail。欲進一步了解 CloudTrail，包括如何將其開啟並尋找您的日誌檔案，請參閱《AWS CloudTrail 使用者指南》。

動作

支援以下動作：

- AcceptPrimaryEmailUpdate
- DeleteAlternateContact
- DisableRegion

- EnableRegion
- GetAccountInformation
- GetAlternateContact
- GetContactInformation
- GetPrimaryEmail
- GetRegionOptStatus
- ListRegions
- PutAccountName
- PutAlternateContact
- PutContactInformation
- StartPrimaryEmailUpdate

AcceptPrimaryEmailUpdate

接受來自 的請求StartPrimaryEmailUpdate，以更新指定帳戶的主要電子郵件地址（也稱為根使用者電子郵件地址）。

請求語法

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

{
   "AccountId": "string",
   "Otp": "string",
   "PrimaryEmail": "string"
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要透過此操作存取或修改之 AWS 帳戶 的 12 位數帳戶 ID 號碼。若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分。指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用受信任存取，並選擇性地指派委派的管理員帳戶。

此操作只能從成員帳戶的管理帳戶或組織的委派管理員帳戶呼叫。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`。

類型：字串

模式：`\d{12}`

必要：是

Otp

傳送至 `StartPrimaryEmailUpdate` API 呼叫上`PrimaryEmail`所指定 的 OTP 程式碼。

類型：字串

模式：`[a-zA-Z0-9]{6}`

必要：是

PrimaryEmail

用於指定帳戶的新主要電子郵件地址。這必須符合 `StartPrimaryEmailUpdate` API 呼叫`PrimaryEmail`中的 。

類型：字串

長度限制：長度下限為 5。長度上限為 64。

必要：是

回應語法

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

{
   "Status": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

Status

擷取已接受的主要電子郵件更新請求的狀態。

類型：字串

有效值:`PENDING | ACCEPTED`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

ConflictException

由於資源目前狀態發生衝突，無法處理請求。例如，如果您嘗試啟用目前正在停用的區域（處於 DISABLING 狀態），或嘗試將帳戶的根使用者電子郵件變更為已在使用的電子郵件地址，就會發生這種情況。

HTTP 狀態碼：409

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

ResourceNotFoundException

操作失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

DeleteAlternateContact

從 刪除指定的替代聯絡人 AWS 帳戶。

如需如何使用替代聯絡人操作的完整詳細資訊，請參閱更新您的替代聯絡人 AWS 帳戶。

> **Note**
> 您必須先啟用 AWS 帳戶管理和組織之間的整合 AWS Organizations，才能更新由 AWS 帳戶管理的 的替代聯絡資訊。如需詳細資訊，請參閱啟用 AWS 帳戶管理的受信任存取。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要使用此操作存取或修改之帳戶的 12 位數 AWS 帳戶 ID 號碼。

如果您未指定此參數，它會預設為用來呼叫 操作的身分 AWS 帳戶。

若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分，且指定的帳戶 ID 必須是同一組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用受信任存取，並可選擇指派委派管理員帳戶。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`；它必須藉由不包含 `AccountId` 參數，在獨立內容中呼叫 操作。

若要在非組織成員的帳戶上呼叫此操作，請不要指定此參數，並使用屬於您想要擷取或修改其聯絡人之帳戶的身分來呼叫操作。

類型：字串

模式：`\d{12}`

必要：否

AlternateContactType

指定要刪除的替代聯絡人。

類型：字串

有效值:`BILLING | OPERATIONS | SECURITY`

必要：是

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

ResourceNotFoundException

操作失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

範例

範例 1

下列範例會刪除登入資料用於呼叫 操作之帳戶的安全替代聯絡人。

請求範例

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

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

回應範例

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

範例 2

下列範例會刪除組織中指定成員帳戶的帳單替代聯絡人。您必須使用來自組織管理帳戶的登入資料，或來自帳戶管理服務的委派管理員帳戶。

請求範例

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

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

回應範例

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

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

DisableRegion

停用（選擇退出）帳戶的特定區域。

> **Note**
>
> 停用區域的行為會移除該區域中任何資源的所有 IAM 存取權。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要透過此操作存取或修改之 AWS 帳戶 的 12 位數帳戶 ID 號碼。如果您未指定此參數，它會預設為用於呼叫 操作之身分的 Amazon Web Services 帳戶。若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分。指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用受信任存取，並選擇性地指派委派的管理員帳戶。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`。它必須藉由不包含 `AccountId` 參數，在獨立內容中呼叫 操作。

若要在非組織成員的帳戶上呼叫此操作，請勿指定此參數。反之，使用屬於您想要擷取或修改其聯絡人之帳戶的身分來呼叫 操作。

類型：字串

模式：`\d{12}`

必要：否

RegionName

指定指定區域名稱的區域代碼（例如，`af-south-1`)。當您停用區域時， AWS 會執行動作來停用帳戶中的區域，例如銷毀區域中的 IAM 資源。對於大部分帳戶，這個過程需要幾分鐘的時間，但此帳戶可能需要數小時的時間。在停用程序完全完成之前，您無法啟用區域。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：是

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

ConflictException

由於資源目前狀態衝突，無法處理請求。例如，如果您嘗試啟用目前正在停用的區域（處於 DISABLING 狀態），或嘗試將帳戶的根使用者電子郵件變更為已在使用的電子郵件地址，就會發生這種情況。

HTTP 狀態碼：409

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

EnableRegion

為帳戶啟用（選擇加入）特定區域。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要透過此操作存取或修改之 AWS 帳戶 的 12 位數帳戶 ID 號碼。如果您未指定此參數，它會預設為用於呼叫 操作之身分的 Amazon Web Services 帳戶。若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分。指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用受信任存取，並選擇性地指派委派的管理員帳戶。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`。它必須藉由不包含 `AccountId` 參數，在獨立內容中呼叫 操作。

若要在非組織成員的帳戶上呼叫此操作，請勿指定此參數。反之，使用屬於您想要擷取或修改其聯絡人之帳戶的身分來呼叫 操作。

類型：字串

模式：`\d{12}`

必要：否

RegionName

指定指定區域名稱的區域代碼（例如，af-south-1)。在啟用區域時，AWS 會執行動作，以便在該區域中準備您的帳戶，例如將您的 IAM 資源分發至該區域。大多數帳戶需要幾分鐘的時間，但可能需要數小時的時間。直到此過程完成之前，您都無法使用區域。此外，在啟用程序完全完成之前，您無法停用區域。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：是

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

ConflictException

由於資源目前狀態衝突，無法處理請求。例如，如果您嘗試啟用目前正在停用的區域（處於 DISABLING 狀態），或嘗試將帳戶的根使用者電子郵件變更為已在使用的電子郵件地址，就會發生這種情況。

HTTP 狀態碼：409

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetAccountInformation

擷取指定帳戶的相關資訊，包括其帳戶名稱、帳戶 ID 和帳戶建立日期和時間。若要使用此 API，IAM 使用者或角色必須具有 IAM `account:GetAccountInformation` 許可。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要使用此操作存取或修改之帳戶的 12 位數 AWS 帳戶 ID 號碼。

如果您未指定此參數，它會預設為用來呼叫 操作的身分 AWS 帳戶。

若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分，而指定的帳戶 ID 必須是同一組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用信任存取，並可選擇指派委派管理員帳戶。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`；它必須藉由不包含 `AccountId` 參數，在獨立內容中呼叫 操作。

若要在非組織成員的帳戶上呼叫此操作，請不要指定此參數，並使用屬於您想要擷取或修改其聯絡人之帳戶的身分來呼叫操作。

類型：字串

模式：\d{12}

必要：否

回應語法

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

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

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AccountCreatedDate

建立帳戶的日期和時間。

類型：Timestamp

AccountId

指定您要透過此操作存取或修改之 AWS 帳戶 的 12 位數帳戶 ID 號碼。若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分。指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用受信任存取，並選擇性地指派委派的管理員帳戶。

此操作只能從成員帳戶的管理帳戶或組織的委派管理員帳戶呼叫。

> **Note**
>
> 管理帳戶無法指定自己的 AccountId。

類型：字串

模式：`\d{12}`

AccountName

帳戶的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

模式：`[ -;=?-~]+`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

範例

範例 1

下列範例會擷取登入資料用於呼叫 操作之帳戶的 帳戶資訊。

請求範例

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

{}
```

回應範例

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

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

範例 2

下列範例會擷取組織中指定成員帳戶的帳戶資訊。您必須使用來自組織管理帳戶的登入資料，或來自帳戶管理服務的委派管理員帳戶。

請求範例

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

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

回應範例

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

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

```
}
```

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetAlternateContact

擷取連接至 的指定替代聯絡人 AWS 帳戶。

如需如何使用替代聯絡人操作的完整詳細資訊，請參閱更新您的替代聯絡人 AWS 帳戶。

> **Note**
> 您必須先啟用 AWS 帳戶管理和組織之間的整合 AWS Organizations，才能更新由 AWS 帳戶管理的 的替代聯絡資訊。如需詳細資訊，請參閱啟用 AWS 帳戶管理的受信任存取。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要使用此操作存取或修改之帳戶的 12 位數 AWS 帳戶 ID 號碼。

如果您未指定此參數，它會預設為用來呼叫 操作的身分 AWS 帳戶。

若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分，而指定的帳戶 ID 必須是同一組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用信任存取，並可選擇指派委派管理員帳戶。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`；它必須藉由不包含 `AccountId` 參數，在獨立內容中呼叫 操作。

若要在非組織成員的帳戶上呼叫此操作，請不要指定此參數，並使用屬於您想要擷取或修改其聯絡人之帳戶的身分來呼叫操作。

類型：字串

模式：`\d{12}`

必要：否

AlternateContactType

指定您要擷取的替代聯絡人。

類型：字串

有效值:`BILLING | OPERATIONS | SECURITY`

必要：是

回應語法

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

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

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AlternateContact

包含指定替代聯絡人詳細資訊的結構。

類型：AlternateContact 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

ResourceNotFoundException

操作失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

範例

範例 1

下列範例會擷取其登入資料用於呼叫 操作之帳戶的安全替代聯絡人。

請求範例

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

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

回應範例

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

{
   "AlternateContact":{
      "Name":"Anika",
      "Title":"COO",
      "EmailAddress":"anika@example.com",
      "PhoneNumber":"206-555-0198",
      "AlternateContactType":"Security"
   }
}
```

範例 2

下列範例會擷取組織中指定成員帳戶的操作替代聯絡人。您必須使用來自組織管理帳戶的登入資料，或來自帳戶管理服務的委派管理員帳戶。

請求範例

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

{
   "AccountId":"123456789012",
```

```
   "AlternateContactType":"Operations"
}
```

回應範例

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

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

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetContactInformation

擷取 的主要聯絡資訊 AWS 帳戶。

如需如何使用主要聯絡人操作的完整詳細資訊，請參閱更新主要聯絡人 AWS 帳戶。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要透過此操作存取或修改之 AWS 帳戶 的 12 位數帳戶 ID 號碼。如果您未指定此參數，它會預設為用於呼叫 操作之身分的 Amazon Web Services 帳戶。若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分。指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用受信任存取，並可選擇指派委派的管理員帳戶。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`。它必須藉由不包含 `AccountId` 參數，在獨立內容中呼叫 操作。

若要在非組織成員的帳戶上呼叫此操作，請勿指定此參數。反之，使用屬於您想要擷取或修改其聯絡人之帳戶的身分來呼叫 操作。

類型：字串

模式：\d{12}

必要：否

回應語法

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

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

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

ContactInformation

包含與 相關聯的主要聯絡資訊的詳細資訊 AWS 帳戶。

類型：ContactInformation 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

ResourceNotFoundException

操作失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK

- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetPrimaryEmail

擷取指定帳戶的主要電子郵件地址。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要透過此操作存取或修改之 AWS 帳戶 的 12 位數帳戶 ID 號碼。若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分。指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用受信任存取，並選擇性地指派委派的管理員帳戶。

此操作只能從成員帳戶的管理帳戶或組織的委派管理員帳戶呼叫。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`。

類型：字串

模式：`\d{12}`

必要：是

回應語法

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

{
   "PrimaryEmail": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

PrimaryEmail

擷取與指定帳戶相關聯的主要電子郵件地址。

類型：字串

長度限制：長度下限為 5。長度上限為 64。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

ResourceNotFoundException

操作失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

GetRegionOptStatus

擷取特定區域的選擇加入狀態。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要透過此操作存取或修改之 AWS 帳戶 的 12 位數帳戶 ID 號碼。如果您未指定此參數，它會預設為用於呼叫 操作之身分的 Amazon Web Services 帳戶。若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分。指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用受信任存取，並選擇性地指派委派的管理員帳戶。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`。它必須藉由不包含 `AccountId` 參數，在獨立內容中呼叫 操作。

若要在非組織成員的帳戶上呼叫此操作，請勿指定此參數。反之，使用屬於您想要擷取或修改其聯絡人之帳戶的身分來呼叫 操作。

類型：字串

模式：`\d{12}`

必要：否

RegionName

指定指定區域名稱的區域代碼（例如，af-south-1)。此函數將傳回您傳遞至此參數的任何區域的狀態。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：是

回應語法

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

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

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

RegionName

傳入的區域碼。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

RegionOptStatus

區域可以經歷的其中一個潛在狀態（啟用、啟用、停用、停用、啟用_By_Default)。

類型：字串

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

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK

- AWS 適用於 Ruby V3 的 SDK

ListRegions

列出指定帳戶的所有區域及其個別選擇加入狀態。或者，可以依 `region-opt-status-contains` 參數篩選此清單。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要透過此操作存取或修改之 AWS 帳戶 的 12 位數帳戶 ID 號碼。如果您未指定此參數，它會預設為用於呼叫 操作之身分的 Amazon Web Services 帳戶。若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分。指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用受信任存取，並選擇性地指派委派的管理員帳戶。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`。它必須藉由不包含 `AccountId` 參數，在獨立內容中呼叫 操作。

若要在非組織成員的帳戶上呼叫此操作，請勿指定此參數。反之，使用屬於您想要擷取或修改其聯絡人之帳戶的身分來呼叫 操作。

類型：字串

模式：`\d{12}`

必要：否

MaxResults

命令輸出中要傳回的項目總數。如果可用的項目總數超過指定的值，`NextToken`則會在命令的輸出中提供 。若要繼續分頁，請在後續命令的 `starting-token` 引數中提供 `NextToken` 值。請勿在 CLI AWS 外部直接使用`NextToken`回應元素。如需使用範例，請參閱《 AWS 命令列界面使用者指南》中的分頁。

類型：整數

有效範圍：最小值為 1。最大值為 50。

必要：否

NextToken

用於指定在何處開始分頁的字符。這是先前截斷的回應`NextToken`中的 。如需使用範例，請參閱《 AWS 命令列界面使用者指南》中的分頁。

類型：字串

長度限制：長度下限為 0。長度上限為 1000。

必要：否

RegionOptStatusContains

區域狀態清單（啟用、啟用、停用、停用、啟用、by_default)，可用來篩選指定帳戶的區域清單。例如，傳入 ENABLING 值只會傳回區域狀態為 ENABLING 的區域清單。

類型：字串陣列

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

必要：否

回應語法

```
HTTP/1.1 200
```

```
Content-type: application/json

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

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

如果要傳回更多資料，則會填入此項目。它應該傳遞到 的`next-token`請求參數`list-regions`。

類型：字串

Regions

這是指定帳戶的 區域清單，或者如果使用篩選過的參數，則為符合 `filter` 參數中所設定篩選條件的區域清單。

類型：Region 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

PutAccountName

更新指定帳戶的帳戶名稱。若要使用此 API，IAM 主體必須具有 IAM `account:PutAccountName` 許可。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要使用此操作存取或修改之帳戶的 12 位數 AWS 帳戶 ID 號碼。

如果您未指定此參數，它會預設為用來呼叫 操作的身分 AWS 帳戶。

若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分，而指定的帳戶 ID 必須是同一組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用信任存取，並可選擇指派委派管理員帳戶。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`；它必須藉由不包含 `AccountId` 參數，在獨立內容中呼叫 操作。

若要在非組織成員的帳戶上呼叫此操作，請不要指定此參數，並使用屬於您想要擷取或修改其聯絡人之帳戶的身分來呼叫操作。

類型：字串

模式：`\d{12}`

必要：否

AccountName

帳戶的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

模式：`[ -;=?-~]+`

必要：是

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

範例

範例 1

下列範例會更新其登入資料用於呼叫 操作的帳戶名稱。

請求範例

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

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

回應範例

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

範例 2

下列範例會更新組織中指定成員帳戶的帳戶名稱。您必須使用來自組織管理帳戶的登入資料，或來自帳戶管理服務的委派管理員帳戶。

請求範例

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

{
   "AccountId": "123456789012",
   "AccountName": "MyMemberAccount"
```

```
}
```

回應範例

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

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

PutAlternateContact

修改連接至 的指定替代聯絡人 AWS 帳戶。

如需如何使用替代聯絡人操作的完整詳細資訊，請參閱更新您的替代聯絡人 AWS 帳戶。

> **Note**
> 您必須先啟用 AWS 帳戶管理和組織之間的整合 AWS Organizations，才能更新 AWS 帳戶 管理的替代聯絡資訊。如需詳細資訊，請參閱啟用 AWS 帳戶管理的受信任存取。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要使用此操作存取或修改之帳戶的 12 位數 AWS 帳戶 ID 號碼。

如果您未指定此參數，它會預設為用來呼叫 操作的身分 AWS 帳戶。

若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分，且指定的帳戶 ID 必須是同一組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用信任存取，並選擇性地指派委派管理員帳戶。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`；它必須藉由不包含 `AccountId` 參數，在獨立內容中呼叫 操作。

若要在非組織成員的帳戶上呼叫此操作，請不要指定此參數，並使用屬於您想要擷取或修改其聯絡人之帳戶的身分來呼叫操作。

類型：字串

模式：`\d{12}`

必要：否

AlternateContactType

指定您要建立或更新的替代聯絡人。

類型：字串

有效值:`BILLING | OPERATIONS | SECURITY`

必要：是

EmailAddress

指定替代聯絡人的電子郵件地址。

類型：字串

長度限制：長度下限為 1。長度上限為 254。

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

必要：是

Name

指定替代聯絡人的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

必要：是

PhoneNumber

指定替代聯絡人的電話號碼。

類型：字串

長度限制：長度下限為 1。長度上限為 25。

模式：`[\s0-9()+-]+`

必要：是

Title

指定替代聯絡人的標題。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：是

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

範例

範例 1

下列範例會為登入資料用於呼叫 操作的帳戶設定帳單備用聯絡人。

請求範例

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

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

回應範例

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

範例 2

下列範例會設定或覆寫組織中指定成員帳戶的帳單替代聯絡人。您必須使用來自組織管理帳戶的登入資料，或來自帳戶管理服務的委派管理員帳戶。

請求範例

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

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

回應範例

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

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

PutContactInformation

更新 的主要聯絡資訊 AWS 帳戶。

如需如何使用主要聯絡人操作的完整詳細資訊，請參閱更新主要聯絡人 AWS 帳戶。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要透過此操作存取或修改之 AWS 帳戶 的 12 位數帳戶 ID 號碼。如果您未指定此參數，它會預設為用於呼叫 操作之身分的 Amazon Web Services 帳戶。若要使用此參數，發起人必須是組織

管理帳戶或委派管理員帳戶中的身分。指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用信任存取，並選擇性地指派委派管理員帳戶。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`。它必須藉由不包含 `AccountId` 參數，在獨立內容中呼叫 操作。

若要在非組織成員的帳戶上呼叫此操作，請勿指定此參數。反之，使用屬於您想要擷取或修改其聯絡人之帳戶的身分來呼叫 操作。

類型：字串

模式：`\d{12}`

必要：否

ContactInformation

包含與 相關聯的主要聯絡資訊的詳細資訊 AWS 帳戶。

類型：ContactInformation 物件

必要：是

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

StartPrimaryEmailUpdate

開始更新指定帳戶主要電子郵件地址的程序。

請求語法

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

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

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

AccountId

指定您要透過此操作存取或修改之 AWS 帳戶 的 12 位數帳戶 ID 號碼。若要使用此參數，發起人必須是組織管理帳戶或委派管理員帳戶中的身分。指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須針對帳戶管理服務啟用受信任存取，並選擇性地指派委派的管理員帳戶。

此操作只能從成員帳戶的管理帳戶或組織的委派管理員帳戶呼叫。

> **Note**
>
> 管理帳戶無法指定自己的 `AccountId`。

類型：字串

模式：`\d{12}`

必要：是

PrimaryEmail

要在指定帳戶中使用的新主要電子郵件地址（也稱為根使用者電子郵件地址）。

類型：字串

長度限制：長度下限為 5。長度上限為 64。

必要：是

回應語法

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

{
   "Status": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

Status

主要電子郵件更新請求的狀態。

類型：字串

有效值:`PENDING | ACCEPTED`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

操作失敗，因為呼叫身分沒有所需的最低許可。

HTTP 狀態碼：403

ConflictException

由於資源目前狀態發生衝突，無法處理請求。例如，如果您嘗試啟用目前正在停用的區域（處於 DISABLING 狀態），或嘗試將帳戶的根使用者電子郵件變更為已在使用的電子郵件地址，就會發生這種情況。

HTTP 狀態碼：409

InternalServerException

由於 內部發生錯誤，操作失敗 AWS。請稍後重試您的操作。

HTTP 狀態碼：500

ResourceNotFoundException

操作失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

操作失敗，因為呼叫次數太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

操作失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS 適用於 .NET 的 SDK
- AWS 適用於 C++ 的 SDK
- AWS 適用於 Go 的 SDK v2
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK

- AWS 適用於 Kotlin 的 SDK
- AWS 適用於 PHP V3 的 SDK
- AWS 適用於 Python 的 SDK
- AWS 適用於 Ruby V3 的 SDK

其他服務中的相關動作 AWS

下列操作與 相關， AWS 帳戶管理 但屬於 命名空間的一部分 AWS Organizations ：

- CreateAccount
- CreateGovCloudAccount
- DescribeAccount

CreateAccount

`CreateAccount` API 操作僅適用於由 AWS Organizations 服務管理的組織內容。API 操作是在該服務的命名空間中定義。

如需詳細資訊，請參閱 AWS Organizations API 參考中的 CreateAccount。

CreateGovCloudAccount

`CreateGovCloudAccount` API 操作僅適用於由 AWS Organizations 服務管理的組織內容。API 操作是在該服務的命名空間中定義。

如需詳細資訊，請參閱 AWS Organizations API 參考中的 CreateGovCloudAccount。

DescribeAccount

`DescribeAccount` API 操作僅適用於由 AWS Organizations 服務管理的組織內容。API 操作是在該服務的命名空間中定義。

如需詳細資訊，請參閱 AWS Organizations API 參考中的 DescribeAccount。

資料類型

目前支援下列資料類型：

- AlternateContact
- ContactInformation
- Region
- ValidationExceptionField

AlternateContact

包含與帳戶相關聯之替代聯絡人詳細資訊的 AWS 結構

目錄

AlternateContactType

替代聯絡人的類型。

類型：字串

有效值:`BILLING | OPERATIONS | SECURITY`

必要：否

EmailAddress

與此替代聯絡人相關聯的電子郵件地址。

類型：字串

長度限制：長度下限為 1。長度上限為 254。

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

必要：否

Name

與此替代聯絡人相關聯的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 64。

必要：否

PhoneNumber

與此替代聯絡人相關聯的電話號碼。

類型：字串

長度限制：長度下限為 1。長度上限為 25。

模式：`[\s0-9()+-]+`

必要：否

Title

與此替代聯絡人相關聯的標題。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ContactInformation

包含與 相關聯的主要聯絡資訊的詳細資訊 AWS 帳戶。

目錄

AddressLine1

主要聯絡人地址的第一行。

類型：字串

長度限制：長度下限為 1。長度上限為 60。

必要：是

City

主要聯絡地址的城市。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：是

CountryCode

主要聯絡地址的 ISO-3166 雙字母國家/地區代碼。

類型：字串

長度限制：固定長度為 2。

必要：是

FullName

主要聯絡人地址的完整名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：是

PhoneNumber

主要聯絡資訊的電話號碼。號碼將會經過驗證，而且在某些國家/地區會檢查是否啟用。

類型：字串

長度限制：長度下限為 1。長度上限為 20。

模式：`[+][\s0-9()-]+`

必要：是

PostalCode

主要聯絡地址的郵遞區號。

類型：字串

長度限制：長度下限為 1。長度上限為 20。

必要：是

AddressLine2

主要聯絡人地址的第二行，如果有的話。

類型：字串

長度限制：長度下限為 1。長度上限為 60。

必要：否

AddressLine3

主要聯絡地址的第三行，如果有的話。

類型：字串

長度限制：長度下限為 1。長度上限為 60。

必要：否

CompanyName

與主要聯絡資訊相關聯的公司名稱，如果有的話。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：否

DistrictOrCounty

主要聯絡地址的區或郡，如果有的話。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：否

StateOrRegion

主要聯絡人地址的狀態或區域。如果郵寄地址位於美國 (US) 內，此欄位的值可以是兩個字元的狀態碼（例如 NJ) 或完整狀態名稱（例如 New Jersey)。下列國家/地區需要此欄位：US、CA、GB、DE、IN、 JP和 BR。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：否

WebsiteUrl

與主要聯絡資訊相關聯的網站 URL，如果有的話。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的開發套件
- AWS 適用於 Ruby V3 的 SDK

Region

這是表示指定帳戶區域結構，包含名稱和選擇加入狀態。

目錄

RegionName

指定區域的區域代碼（例如 `us-east-1`)。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：否

RegionOptStatus

區域可以經歷的潛在狀態之一（啟用、啟用、停用、停用、啟用_By_Default)。

類型：字串

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

必要：否

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱以下內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

ValidationExceptionField

輸入不符合指定欄位中 AWS 服務指定的限制條件。

目錄

message

有關驗證例外狀況的訊息。

類型：字串

必要：是

name

偵測到無效項目的欄位名稱。

類型：字串

必要：是

另請參閱

如需在其中一種語言特定 AWS SDKs中使用此 API 的詳細資訊，請參閱以下內容：

- AWS 適用於 C++ 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 Ruby V3 的 SDK

常見參數

以下清單內含所有動作用來簽署 Signature 第 4 版請求的參數以及查詢字串。任何專屬於特定動作的參數則列於該動作的主題中。如需 Signature 第 4 版的詳細資訊，請參閱《IAM 使用者指南》中的簽署 AWS API 請求。

Action

要執行的動作。

類型：字串

必要：是

Version

編寫請求所憑藉的 API 版本，以 YYYY-MM-DD 格式表示。

類型：字串

必要：是

X-Amz-Algorithm

建立請求簽章時所使用的雜湊演算法。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

有效值:`AWS4-HMAC-SHA256`

必要：有條件

X-Amz-Credential

憑證範圍值，此為一個字串，其中包含您的存取金鑰、日期、您的目標區域、您請求的服務，以及終止字串 (“aws4_request”)。值以下列格式表示：access_key/YYYYMMDD/region/service/aws4_request。

如需詳細資訊，請參閱《IAM 使用者指南》中的建立簽署的 AWS API 請求。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

X-Amz-Date

用來建立簽署的日期。格式必須是 ISO 8601 基本格式 (YYYYMMDD'T'HHMMSS'Z')。例如，以下日期時間是有效的 X-Amz-Date 值：`20120325T120000Z`

條件： 對所有請求而言，X-Amz-Date 皆為選用，可用來覆寫用於簽署請求的日期。如果規定日期標頭採用 ISO 8601 基本格式，則不需要 X-Amz-Date。當使用 X-Amz-Date 時，其一律會覆寫日期標頭的值。如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS API 請求簽章元素。

類型：字串

必要：有條件

X-Amz-Security-Token

透過呼叫 AWS Security Token Service () 取得的臨時安全字符AWS STS。如需支援 AWS STS的臨時安全憑證的服務清單，請參閱《IAM 使用者指南》中的可搭配 IAM 運作的AWS 服務。

條件：如果您使用來自 的臨時安全登入資料 AWS STS，則必須包含安全字符。

類型：字串

必要：有條件

X-Amz-Signature

指定從要簽署的字串和衍生的簽署金鑰中計算出的十六進位編碼簽章。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

X-Amz-SignedHeaders

指定納入作為標準請求一部分的所有 HTTP 標頭。如需指定簽章標頭的詳細資訊，請參閱《IAM 使用者指南》中的建立簽章 AWS API 請求。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

常見錯誤

本節列出所有 AWS 服務的 API 動作常見的錯誤。如需此服務之 API 動作的特定錯誤，請參閱該 API 動作的主題。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：400

IncompleteSignature

請求簽章不符合 AWS 標準。

HTTP 狀態碼：400

InternalFailure

由於不明的錯誤、例外狀況或故障，處理請求失敗。

HTTP 狀態碼：500

InvalidAction

請求的動作或操作無效。確認已正確輸入動作。

HTTP 狀態碼：400

InvalidClientTokenId

提供的 X.509 憑證或 AWS 存取金鑰 ID 不存在於我們的記錄中。

HTTP 狀態碼：403

NotAuthorized

您沒有執行此動作的許可。

HTTP 狀態碼：400

OptInRequired

AWS 存取金鑰 ID 需要訂閱 服務。

HTTP 狀態碼：403

RequestExpired

請求送達服務已超過戳印日期於請求上之後的 15 分鐘，或者已超過請求過期日期之後的 15 分鐘 (例如預先簽章的 URL)，或者請求上的日期戳印在未來將超過 15 分鐘。

HTTP 狀態碼：400

ServiceUnavailable

由於伺服器暫時故障，請求失敗。

HTTP 狀態碼：503

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

ValidationError

輸入無法滿足 AWS 服務指定的限制條件。

HTTP 狀態碼：400

提出 HTTP 查詢請求以呼叫 API

本節包含有關使用 查詢 API for AWS Account Management 的一般資訊。如需 API 操作和錯誤的詳細資訊，請參閱 API 參考。

> **Note**
>
> 您可以使用其中一個 AWS SDKs，而不是直接呼叫 AWS 帳戶管理查詢 API。 AWS SDKs包含各種程式設計語言和平台 (Java、Ruby、.NET、iOS、Android 等） 的程式庫和範例程式碼。SDKs提供便捷的方式，以建立對 AWS Account Management 和 的程式設計存取 AWS。例如，開發套件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 的相關資訊，包括如何下載和安裝，請參閱適用於 Amazon Web Services 的工具。

使用適用於 AWS 帳戶管理的查詢 API，您可以呼叫 服務動作。查詢 API 請求是 HTTPS 請求，其中必須包含 `Action` 參數，以指出要執行的操作。 AWS 帳戶管理支援所有操作的 `GET`和 `POST`請求。也就是說，API 不需要您`GET`針對某些動作和其他動作使用 `POST` 。不過，`GET`請求會受到 URL 大小的限制。雖然此限制取決於瀏覽器，但一般限制為 2，048 個位元組。因此，對於需要較大大小的查詢 API 請求，您必須使用`POST`請求。

回應為 XML 文件。如需回應的詳細資訊，請參閱 API 參考中個別動作的頁面。

主題

- 端點
- 必要的 HTTPS
- 簽署 AWS 帳戶管理 API 請求

端點

AWS Account Management 有一個託管在美國東部（維吉尼亞北部）的單一全域 API 端點。 AWS 區域

如需所有 服務的 AWS 端點和區域的詳細資訊，請參閱 中的區域和端點AWS 一般參考。

必要的 HTTPS

由於查詢 API 可以傳回敏感資訊，例如安全登入資料，因此您必須使用 HTTPS 來加密所有 API 請求。

簽署 AWS 帳戶管理 API 請求

請求必須使用存取金鑰 ID 和私密存取金鑰簽署。強烈建議您不要將 AWS 根帳戶登入資料用於 AWS 帳戶管理的日常工作。您可以使用 AWS Identity and Access Management (IAM) 使用者的登入資料或臨時登入資料，例如搭配 IAM 角色使用的登入資料。

若要簽署 API 請求，您必須使用 AWS Signature 第 4 版。如需使用 Signature 第 4 版的相關資訊，請參閱《IAM 使用者指南》中的簽署 AWS API 請求。

如需詳細資訊，請參閱下列內容：

- AWS 安全憑證 – 提供關於可用來存取 AWS之憑證類型的一般資訊。
- IAM 中的安全最佳實務 – 提供使用 IAM 服務的建議，以協助保護您的 AWS 資源，包括 AWS 帳戶管理中的資源。
- IAM 暫時性安全憑證 – 描述如何建立和使用暫時性安全憑證。

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。除非另有說明，否則每個配額都是 AWS 區域特定的。

每個 AWS 帳戶 都有下列與帳戶管理相關的配額。

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 - 針對 `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
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

資源	配額
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

管理印度的帳戶

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，而您的發票總計會以印度盧比 (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 AWS 印度帳戶的相關資訊、管理客戶驗證，以及新增或編輯您的永久帳戶號碼 (PAN)。

在註冊期間進行信用卡驗證時， 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。請改為選擇登入 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. 選擇商業或個人。個人帳戶和企業帳戶具有相同的特徵和功能。
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 或在註冊後想要新增，請選擇否。
9. 選擇驗證並繼續。 AWS 在驗證程序中，印度會向您的卡片收取 2 盧比的費用。在驗證完成後，AWS 印度會退還 2 盧比。
10. 在確認您的身分頁面上，選取帳戶註冊的主要目的。
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邦核發的駕照，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取。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. 提供您的同意以提交資訊進行驗證，然後選擇繼續。

    完成帳戶註冊後，您會透過電子郵件收到客戶驗證結果的通知。您也可以在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. 選擇是否要透過簡訊 (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，您會在手機上的 SMS 或自動通話中收到四位數的 PIN 碼。
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，並編輯先前用來驗證身分的名稱、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應變團隊 (CERT-In) 法規， AWS 在授予您新的或持續存取 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 將檢查文件編號是否有效，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，例如帳單中的名稱或印度地址或聯絡資訊，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。

建立您的客戶驗證資訊

若要完成客戶驗證，您需要從接受的印度文件提供資訊。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 Management Console。
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。如果您上傳影像檔案，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目的、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. 登入 AWS Management Console。
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，您將需要上傳文件正面和背面（如適用）的副本。文件上傳中的所有資訊應該可見且清晰。
   - 如果您有個人帳戶，並打算使用不是由印度聯邦核發的駕照，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，永久帳戶號碼 (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。若要使用本文件進行驗證，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。
- 護照 - 護照可做為印度公民身分的證明，並可做為國際旅行的身分證明。在護照 Seva Kendra (PSK) 發行的護照中，護照檔案號碼是與個人護照相關聯的唯一英數字元識別符。護照檔案號碼包含 15 個字元，包括字母和數字。與護照號碼不同，護照檔案號碼可以在印度護照的最後一頁中找到。若要使用此文件進行驗證，您必須提供您的出生日期，並上傳護照的第一頁和最後一頁（包含護照檔案號碼）。您可以前往外務部的 Passport Seva Kendra 網站，檢查護照檔案號碼的有效性。

  > **Note**
  >
  > 為了進行客戶驗證，只接受來自印度核發之印度護照的護照檔案號碼。如果您的印度護照是在其他國家核發，您必須使用不同的印度文件進行客戶驗證。

- 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。每個憑證都包含公司識別號碼 (CIN)，這是唯一的英數字元識別符，由 21 個字元組成，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、駕照和護照。

- 對於企業帳戶 - 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 設定您的帳戶。

使用 AWS Management Console 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

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 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。	2024 年 6 月 6 日
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
結束對`aws-portal` 命名空間的支援	AWS Identity and Access Management 先前用來管理帳戶的 (IAM) 動作（例如，`aws-portal:ModifyA`	2024 年 1 月 1 日

	ccount 和 aws-portal:ViewAccount) 已結束標準支援。	
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 帳戶管理現在支援透過 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。