aws

參考指南

AWS 帳戶管理

AWS 帳戶管理: 參考指南

Table of Contents

歡迎使用AWS帳戶管理參考指南

AWS 帳戶是訪問AWS服務的基本組成部分。

一個AWS 帳戶提供兩個基本功能：

- 容器-A AWS 帳戶 是您作為AWS客戶創建的所有AWS資源的基本容器。例如，亞馬遜 Simple Storage Service (Amazon S3) 儲存貯體、Amazon Relational Database Service 服務 (Amazon RDS) 資料庫和亞馬遜 Elastic Compute Cloud (Amazon EC2) 執行個體都是資源。每個資源都由 Amazon 資源名稱 (ARN) 唯一識別，該名稱包含或擁有該資源的帳戶的帳戶 ID。
- 安全邊界 — A 也AWS 帳戶是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認證的使用者使用。

  您可以在帳戶中建立的關鍵資源包括身分識別，例如使用者和角色。身分擁有某人可用來登入 (驗證) 的認證AWS。身分識別也有權限原則，指定使用者可以對帳戶中的資源執行的動作 (授權)。

  安全性最佳做法是要求使用者在存取時使用臨時登入資料AWS。若要提供臨時登入資料，您可以使用同盟和身分識別提供者，例如 AWS IAM Identity Center(IAM 身分中心)。如果您的公司已經使用身分識別提供者，請將其與聯盟搭配使用，以簡化您提供對AWS 帳戶.

  如需有關安全最佳實務的資訊，請參閱 IAM 使用者指南中的 IAM 中的安全最佳實務。

主題

我是否需要多個AWS 帳戶?

AWS 帳戶作為基本的安全邊界AWS。它們充當資源容器，可提供有用的隔離級別。隔離資源和用户的能力是建立安全、管理良好的環境的關鍵要求。

將您的資源分離為單獨的AWS 帳戶可幫助您在雲環境中支持以下原則：

- 安全控制— 不同的應用程序可以有不同的安全配置文件，需要圍繞它們不同的控制策略和機制。例如，與審計員交談要容易得多，並且能夠指向單個AWS 帳戶，託管工作負載中受支付卡產業 (PCI) 安全標準。

- 隔離— 一個AWS 帳戶是一個安全保護單位。潛在風險和安全威脅應包含在AWS 帳戶而不影響他人. 由於不同的團隊或不同的安全配置文件，可能存在不同的安全需求。
- 許多隊伍— 不同的團隊有不同的職責和資源需求。您可以防止團隊互相幹擾，方法是將它們移動到分離AWS 帳戶。
- 數據隔離— 除了隔離團隊之外，還必須將數據存儲隔離到帳户。這有助於限制可以訪問和管理該數據存儲的人數。這有助於控制高度私有數據的暴露，因此有助於遵守歐盟《一般資料保護條例》(GDPR)。
- B. 業務流程— 不同的業務部門或產品可能具有完全不同的目的和流程。使用多個AWS 帳戶，您可以支持業務部門的特定需求。
- 計費— 賬户是在賬單級別分隔項目的唯一真正方法。多個帳户有助於跨業務部門、職能團隊或個人用户在賬單級別分隔項目。您仍然可以將所有賬單合併到一個付款人（使用AWS Organizations和整合賬單），同時將行項目由AWS 帳戶。
- 配額分配–AWS服務配額分別為每個AWS 帳戶。將工作負載分離到不同的AWS 帳戶防止它們相互消耗配額。

本文檔中描述的所有建議和程序均符合AWSWell-Architected 框架。此框架旨在幫助您設計靈活、具有彈性和可擴展性的雲基礎架構。即使您從小開始，我們也建議您按照框架中的本指南繼續操作。這樣做可以幫助您安全地擴展環境，而不會隨着增長而影響您的日常運營。

管理多個AWS 帳戶

在開始添加多個帳户之前，您需要制定一個管理它們的計劃。為此，我們建議您使用AWS Organizations，這是一個免費的AWS服務來管理所有AWS 帳戶在您的組織中。

AWS還提供AWS Control Tower，它添加了AWS託管自動化到 Organizations，並自動將其與其他AWSLIKEAWS CloudTrail、AWS Config、Amazon CloudWatch、AWS Service Catalog和其他。這些服務會產生額外成本。如需詳細資訊，請參閱 AWS Control Tower 定價。

開始使用：您是第一次AWS使用嗎？

如果您是的第一次使用者AWS，您的第一步是註冊AWS 帳戶. 當您註冊時，使用您提供AWS 帳戶的詳細信息AWS創建一個並將該帳戶分配給您。建立之後AWS 帳戶，請以 root 使用者身分登入、為 root 使用者啟用多因素驗證 (MFA)，然後將管理存取權指派給使用者。

步驟

- 先決條件

- 步驟 1：建立您的 AWS 帳戶
- 步驟 2：為您的根使用者啟用 MFA
- 步驟 3：建立管理員使用者
- 相關主題

先決條件

要註冊AWS 帳戶，您需要以下信息：

- 帳戶名稱 — 帳戶名稱會顯示在數個位置 (例如發票上) 以及主控台 (例如 [Billing and Cost Management] 儀表板和AWS Organizations主控台) 中。

  我們建議您使用標準方式為帳戶命名，以便為您提供易於識別的帳戶名稱。對於公司帳戶，請考慮使用命名標準，例如組織-目的-環境（例如，AnyCompany-審計-prod）。對於個人帳戶，請考慮使用命名標準，例如名字-姓氏-目的（例如 paulo-santos-testaccount）。

  如需變更帳戶名稱的相關資訊，請參閱如何變更帳戶名稱AWS 帳戶？ 。
- 地址 — 如果您的聯絡地址位於印度，則您帳戶的使用者合約為印度當地AWS賣家 Amazon Internet Services Private Limited (AISPL)。在驗證過程中您必須提供您的 CVV。視乎您的銀行而定，您可能還必須輸入一次性密碼。AISPL 會在驗證過程中向您收取 2 INR 的付款方式收取費用。驗證完成後，AISPL 會退回這 2 盧比。
- 電子郵件地址 — 電子郵件地址用作 root 使用者的登入名稱，而且是復原帳戶所必需的。您必須能夠接收傳送至此地址的電子郵件訊息。在執行特定工作之前，您必須確認您有權存取傳送至此地址的電子郵件。

  > **Important**
  >
  > 如果此帳戶適用於企業，請使用安全的公司通訊群組清單 (例如，`it.admins@example.com`)，以便AWS 帳戶即使員工變更職位或離開公司，您的公司仍可保留對的存取權。因為電子郵件地址可用來重設帳戶的根使用者認證，因此請保護對此通訊群組清單或地址的存取。
- 電話號碼 — 此號碼可用於確認您帳戶的所有權。您必須能夠透過此電話號碼接聽電話。

> **Important**
>
> 如果此帳戶適用於企業，請使用公司電話號碼，以便AWS 帳戶即使員工變更職位或離開公司，您的公司仍可保留對該帳戶的存取權。

步驟 1：建立您的 AWS 帳戶

1. 在瀏覽器中，開啟AWS首頁。
2. 選擇 [建立] AWS 帳戶。

   > **Note**
   >
   > 如果您AWS最近登入，請選擇 [登入]。如果看AWS 帳戶不到 [建立新帳戶] 選項，請先選擇 [登入其他帳戶]，然後選擇 [建立新帳戶] AWS 帳戶。

3. 輸入您的帳戶資訊，然後選擇 [驗證電子郵件地址]。驗證碼將發送到您指定的電子郵件地址。
4. 輸入您的驗證碼，然後選擇「驗證」。
5. 輸入 root 使用者的強式密碼，確認密碼，然後選擇 [繼續]。 AWS您的密碼必須符合下列條件：
   - 它必須至少包含 8 個字元，最多 128 個字元。
   - 它必須至少包含下列三種字元類型混合：大寫、小寫、數字和! @ # $% ^ & * () <> [] {} | _ +-= 符號。
   - 它不得與您的AWS 帳戶姓名或電子郵件地址相同。
6. 選擇「商業」或「個人」 這些選項之間的區別在於我們要求您提供的信息。兩種帳戶類型具有相同的特性和功能。
7. 輸入您的公司或個人信息。請參閱 [必要條件] 區段中有關電子郵件地址和電話號碼的建議。
8. 閱讀並接受AWS客戶協議。請確保您已閱讀並理解AWS客戶協議的條款。
9. 選擇 Continue (繼續)。此時，您將收到一封電子郵件，以確認您AWS 帳戶已準備好使用。您可以使用註冊過程中提供的電子郵件地址和密碼登錄新帳戶。但是，在完成激活帳戶之前，您無法使用任何AWS服務。
10. 輸入有關付款方式的資訊。如果您想要使用其他地址作為帳單用途，請選擇 [使用新地址]。
11. 選擇驗證並繼續。

12. 從清單中輸入您的國家或地區代碼，然後輸入電話號碼，在接下來的幾分鐘內就可以聯絡到您。輸入驗證碼，然後提交。
13. 當自動系統與您聯繫時，請輸入您收到的 PIN 碼，然後提交。
14. 選擇您的AWS Support計劃。如需可用計劃的說明，請參閱比較AWS Support方案。
15. 選擇 [完成註冊]。會出現確認頁面，指出您的帳戶正在啟用。
16. 檢查您的電子郵件和垃圾郵件文件夾是否有確認您的帳戶已激活的電子郵件。激活通常需要幾分鐘，但有時可能需要長達 24 小時。

    收到啟用訊息後，您就可以完整存取所有AWS服務。

> **Note**
>
> 如果您在啟用帳戶時遇到問題，請參閱the section called “帳號建立問題”。

步驟 2：為您的根使用者啟用 MFA

強烈建議您為根使用者啟用 MFA。MFA 可大幅降低他人未經您授權存取您帳戶的風險。

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

   AWS Management Console如需使用 root 使用者登入的說明，請參閱登入使用者指南中的「以 root 使用者身分AWS登入」。
2. 為您的根使用者開啟 MFA。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

步驟 3：建立管理員使用者

因為您無法限制 root 使用者可以執行的動作，因此強烈建議您不要將 root 使用者用於任何不明確需要 root 使用者的工作。而是在 IAM Identity Center 中將管理存取權指派給管理使用者，然後以該管理使用者身分登入以執行您的日常管理工作。

如需指示，請參閱 IAM 身分中心使用者指南中的設定 IAM 身分中心管理使用者的AWS 帳戶存取權限。

相關主題

- 如需保護根使用者登入資料的相關資訊，請參閱《IAM 使用者指南》中的保護根使用者登入資料的安全。
- 如需需要 root 使用者的工作清單，請參閱 IAM 使用者指南中的需要 root 使用者登入資料的工作。

使用 AWS 帳戶根使用者

> **Important**
>
> 擁有您 AWS 帳戶 之根使用者憑證的所有使用者，都能無限制地存取該帳戶中的所有資源 (包含帳單資訊)。

如果是建立 AWS 帳戶，您會先有一個登入身分，可以完整存取帳戶中所有 AWS 服務 與資源。此身分稱為 AWS 帳戶 根使用者，使用建立帳戶時所使用的電子郵件地址和密碼即可登入並存取。強烈建議您不要以根使用者處理日常作業。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 root 使用者用於日常工作，請瞭解如何在中設定系統管理使用者AWS IAM Identity Center。如需其他 root 使用者安全性建議，請參閱您的 AWS 帳戶.

您可以變更或重設 root 使用者密碼，以及建立或刪除 root 使用者的存取金鑰 (存取金鑰 ID 和秘密存取金鑰)。AWS Management Console如需使用 root 使用者登入的說明，請參閱登入使用者指南中的「以 root 使用者身分AWS登入」。

管理您的AWS 帳戶

本節包含說明如何管理您的AWS 帳戶。

> **Note**
>
> 如果您的AWS 帳戶在印度通過使用創建Amazon Internet Services Private Limited（AISPL），還有其他考慮因素。如需詳細資訊，請參閱 管理印度帳戶。

主題

創建一個獨立的 AWS 帳戶

本主題說明如何建立不AWS 帳戶受管理的獨立版AWS Organizations。如果您想要建立屬於組織所管理的帳戶AWS Organizations，請參閱《使用指南》中的〈在組織中建立成員帳AWS Organizations戶〉。

這些說明是為了創建印度AWS 帳戶以外的地方。若要在印度建立帳戶，請參閱創建一個AWS 帳戶與艾斯普。

AWS Management Console

建立 AWS 帳戶

1. 打開 Amazon Web Services 主頁。
2. 選擇 [建立] AWS 帳戶。

> **Note**
>
> 如果您AWS最近登入，則該選項可能不存在。請改為選擇 [登入主控台]。然後，如果沒有顯示 [建立新AWS 帳戶的帳戶]，請先選擇 [登入其他帳戶]，然後選擇 [建立新帳戶] AWS 帳戶。

3. 輸入您的帳戶資訊，然後選擇 [驗證電子郵件地址]。驗證碼將發送到您指定的電子郵件地址。

> **Important**
>
> 由於帳戶 root 使用者的嚴重性質，我們強烈建議您使用可供群組存取的電子郵件地址，而不是僅使用個人存取。這樣，如果註冊的人AWS 帳戶離開了公司，則仍然可以使用該電子郵件地址，因為仍然AWS 帳戶可以訪問該電子郵件地址。
> 如果您無法存取與相關聯的電子郵件地址AWS 帳戶，則在您遺失密碼時將無法復原對該帳戶的存取權。

4. 輸入您的驗證碼，然後選擇「驗證」。
5. 輸入 root 使用者的強式密碼，確認密碼，然後選擇 [繼續]。 AWS您的密碼必須符合下列條件：
   - 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。
   - 它不能與您的 AWS 帳戶 名稱或電子郵件地址相同。
6. 選擇「商業」或「個人」 個人帳戶和企業帳戶具有相同的特點和功能。
7. 輸入您的公司或個人信息。

> **Important**
>
> 對於企業而言AWS 帳戶，最佳做法是輸入：
>
> - 公司電話號碼，而不是個人電話號碼。

- 具有網域名稱的電子郵件地址，該地址屬於將使用該帳戶的公司或組織。

使用個別電子郵件地址或個人電話號碼設定帳戶的 root 使用者可能會導致帳戶不安全。

8. 閱讀並接受AWS客戶協議。請確保您已閱讀並理解AWS客戶協議的條款。
9. 選擇 Continue (繼續)。此時，您將收到一封電子郵件，以確認您AWS 帳戶已準備好使用。您可以使用註冊過程中提供的電子郵件地址和密碼登錄新帳戶。但是，在完成激活帳戶之前，您將無法使用任何AWS服務。
10. 輸入付款方式的相關資訊，然後選擇 [驗證並繼續]。如果您想要使用其他帳單地址作為AWS帳單資訊，請選擇 [使用新地址]。

    您必須新增有效的付款方式，才能繼續進行註冊程序。
11. 從清單中輸入您的國家或地區代碼，然後輸入電話號碼，在接下來的幾分鐘內就可以聯絡到您。
12. 輸入驗證碼中顯示的代碼，然後提交。
13. 當自動系統與您聯繫時，請輸入您收到的 PIN 碼，然後提交。
14. 選取其中一個可用的AWS Support計劃。如需可用 Support 方案及其權益的說明，請參閱比較AWS Support方案。
15. 選擇 [完成註冊]。此時會出現確認頁面，指出您的帳戶正在啟用。
16. 檢查您的電子郵件和垃圾郵件文件夾是否有確認您的帳戶已激活的電子郵件。激活通常需要幾分鐘，但有時可能需要長達 24 小時。

    收到啟用訊息後，您就可以完整存取所有AWS服務。

AWS CLI & SDKs

您可以在登入組織的管理帳戶時執AWS Organizations行CreateAccount作業來管理的組織中建立成員帳戶。

您無法使用 AWS Command Line Interface (AWS CLI) 或 AWS API 作業在組織AWS 帳戶外部建立獨立作業。

檢視 AWS 帳戶 識別碼

AWS 將下列唯一識別碼指派給每個識別碼 AWS 帳戶：

AWS 帳戶 ID

一個十二位數的數字，例如 012345678901，可唯一識別一個. AWS 帳戶許多 AWS 資源在其 Amazon 資源名稱 (ARN) 中包含帳戶 ID。帳號 ID 部分會區分一個帳號中的資源與另一個帳號中的資源。如果您是 AWS Identity and Access Management (IAM) 使用者，則可以 AWS Management Console 使用帳戶 ID 或帳戶別名登入。雖然帳號 ID 與任何識別資訊一樣，都應小心使用和分享，但這些 ID 並不被視為秘密、敏感或機密資訊。

規範使用者 ID

字母數字標識符，例如79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be，它是 ID 的模糊形式。 AWS 帳戶 使用 Amazon 簡單儲存服務 (Amazon S3) 授予儲存貯體和物件的跨帳戶存取權 AWS 帳戶 時，您可以使用此 ID 識別。您可以根使用者或 IAM 使用者身分擷取您 AWS 帳戶 的標準使用者 ID。

您必須經過驗證 AWS 才能檢視這些識別碼。

> **Warning**
>
> 請勿將您的 AWS 憑據（包括密碼和訪問密鑰）提供給需要您的 AWS 帳戶 識別碼才能與您共享 AWS 資源的第三方。這樣做會給他們相同 AWS 帳戶 的訪問權限。

找到您的 AWS 帳戶 身份證

您可以使用 AWS Management Console 或 AWS Command Line Interface (AWS CLI) 來尋找 AWS 帳戶 識別碼。在主控台中，帳戶 ID 的位置取決於您是以根使用者或 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。

以 root 使用者身分尋找您的帳號 ID

AWS Management Console

若要在以 root 使用者 AWS 帳戶 身分登入時尋找您的 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，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 [安全認證]。

   > **Tip**
   >
   > 如果您沒有看到「安全登入資料」選項，您可能是以具有 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。在這種情況下，查找條目帳戶和其旁邊的帳戶 ID 號。

2. 在「帳戶詳細資料」區段下，帳號會顯示在 AWS 帳戶 ID 旁邊。

AWS CLI & SDKs

若要尋找您的 AWS 帳戶 ID，請使用 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 root 使用者身分執行命令時，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
```

以 IAM 使用者身分尋找您的帳戶 ID

AWS Management Console

以 IAM 使用者 AWS 帳戶 身分登入時尋找您的 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 [安全認證]。

   > **Tip**
   >
   > 如果您沒有看到「安全登入資料」選項，您可能是以具有 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。在這種情況下，查找條目帳戶和其旁邊的帳戶 ID 號。

2. 在頁面頂端的 [帳戶詳細資料] 底下，帳號會顯示在 AWS 帳戶 ID 旁邊。

AWS CLI & SDKs

若要尋找您的 AWS 帳戶 ID，請使用 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，您必須具備：
>   - `sts:GetCallerIdentity`

使用 get-caller-identity 命令，如下所示。

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

```
123456789012
```

找到您的標準用戶 ID AWS 帳戶

您可以使用或來尋找您的標準 AWS 帳戶 使用 AWS Management Console 者 ID。 AWS CLI的標準使用者 ID 專屬 AWS 帳戶 於該帳戶。您可以擷取身為根使用者、聯合 AWS 帳戶 身分使用者或 IAM 使用者的標準使用者 ID。

以根使用者或 IAM 使用者身分尋找標準 ID

AWS Management Console

以 root 使用者或 IAM 使用者身分登入主控台時，尋找帳戶的標準使用者 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 root 使用者身分執行命令時，不需要任何 IAM 許可。
> - 當您以 IAM 使用者身分登入時，您必須擁有：
>   - `account:GetAccountInformation`

1. 以根使用者或 IAM 使用者身分登入。 AWS Management Console
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 [安全認證]。

   > **Tip**
   >
   > 如果您沒有看到「安全登入資料」選項，您可能是以具有 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。在這種情況下，查找條目帳戶和其旁邊的帳戶 ID 號。

3. 在「帳戶詳細資料」區段下，標準使用者 ID 會顯示在「標準使用者 ID」旁邊。您可以使用規範使用者 ID 來設定 Amazon S3 存取控制清單 (ACL)。

AWS CLI & SDKs

若要使用 AWS CLI

相同 AWS CLI 的 API 命令也適用 AWS 帳戶根使用者於 IAM 使用者或 IAM 角色。

使用列表桶命令，如下所示。

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

以具有 IAM 角色的聯合身分使用者身分尋找標準 ID

AWS Management Console

在以具有 IAM 角色的聯合身分使用者身分登入主控台時，尋找帳戶的標準 ID

> **最低許可**
>
> - 您必須擁有列出和查看 Amazon S3 儲存貯體的權限。

1. 以具有 IAM 角色 AWS Management Console 的聯合身分使用者身分登入。
2. 在 Amazon S3 主控台中，選擇儲存貯體名稱以檢視有關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 [值區擁有者] 底下，會顯示您 AWS 帳戶 的標準 ID。

AWS CLI & SDKs

若要使用 AWS CLI

相同 AWS CLI 的 API 命令也適用 AWS 帳戶根使用者於 IAM 使用者或 IAM 角色。

使用列表桶命令，如下所示。

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

更新 root 使用者的 AWS 帳戶 名稱、電子郵件地址或密碼

若要編輯您 AWS 帳戶的名稱，或變更 root 使用者的密碼或電子郵件地址，請執行下列程序中的步驟。此電子郵件地址和密碼是您用來登入的認證 AWS 帳戶根使用者。

> **Note**
>
> 對 a 的變更最多 AWS 帳戶 可能需要四個小時才能在任何地方傳播。

AWS Management Console

編輯您的 AWS 帳戶 名稱、root 使用者密碼或 root 使用者電子郵件地址

> **最低許可**
>
> 若要執行下列步驟，您至少必須擁有下列 IAM 許可：
>
> - 您必須以不需要其他 IAM 許可的身分登入。 AWS 帳戶根使用者您無法以 IAM 使用者或角色的身分執行這些步驟。

1. 使用您 AWS 帳戶的電子郵件地址和密碼登入 AWS 帳戶根使用者。AWS Management Console
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] 頁面上，選擇 [帳戶設定] 旁邊的 [編輯]。出於安全目的，系統會提示您再次進行身分驗證。

   > **Note**
   >
   > 如果您看不到編輯選項，則可能是您未以帳戶根使用者的身分登入。在以 IAM 使用者或角色的身分登入時，您無法修改帳戶設定。

4. 在 [更新帳戶設定] 頁面上，選擇您要更新之欄位旁的 [編輯]。

   a. [名稱] — 在 [更新您的帳戶名稱] 頁面上的 [新帳戶名稱] 中，輸入新的帳戶名稱，然後選擇 [儲存變更]。

> **Note**
>
> 如果您無法修改 AWS 帳戶 名稱，請檢查服務控制策略（SCP）是否存在 AWS Organizations 限制訪問`account`或設置為拒絕該`iam:UpdateAccountName`操作。

b. 電子郵件 — 在 [更新您的電子郵件地址] 頁面上，填寫 [新電子郵件地址]、[確認新電子郵件地址] 和 [確認您目前的密碼] 欄位。然後，選擇 Save changes (儲存變更)。系統會將驗證碼傳送到您的新電子郵件地址`no-reply@verify.signin.aws`。在 [驗證您的新電子郵件地址] 頁面的 [驗證碼] 底下，輸入您從電子郵件收到的驗證碼，然後選擇 [儲存變更]。

> **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該電子郵件，請檢查垃圾郵件和垃圾郵件資料夾。

c. 密碼 — 在 [更新您的密碼] 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 Save changes (儲存變更)。如需其他指引，包括設定 root 使用者密碼的最佳做法，請參閱《IAM 使用者指南》 AWS 帳戶根使用者中的《變更密碼》。

5. 完成所有變更後，選擇完成。

AWS CLI & SDKs

其中一個 AWS SDK 的 AWS CLI 或 API 作業不支援此工作。您只能使用來執行此工作 AWS Management Console。

了解 API 操作模式

與一起使用的 API 操作AWS 帳戶的屬性始終在兩種操作模式之一下工作：

- 獨立內容— 當帳號中的使用者或角色存取或變更中的帳號屬性時，會使用此模式相同帳戶。獨立前後關聯模式會在您時自動使用Don't (不)包括`AccountId`當您調用其中一個帳戶管理時的參數AWS CLI或者AWS開發套件作業。
- Organizations 內容— 當組織中某個帳號的使用者或角色存取或變更同一組織中不同成員帳戶中的帳號屬性時，會使用此模式。當您時，會自動使用組織前後關聯模式做包括`AccountId`當您調用其中

一個帳戶管理時的參數AWS CLI或者AWS開發套件作業。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下的作業。

所以此AWS CLI和AWSSDK 操作可以在獨立或組織內容中工作。

- 如果您Don't (不)包括`AccountId`參數，則作業會在獨立內容中執行，並自動將要求套用至您用來提出要求的帳戶。無論帳戶是否為組織的成員，都是如此。
- 如果您確實包含`AccountId`參數，則作業會在 Organizations 前後關聯中執行，而作業會在指定的「組織」帳戶上運作。
  - 如果呼叫作業的帳戶是帳戶管理服務的管理帳戶或委派管理員帳戶，則您可以在`AccountId`參數以更新指定帳戶。
  - 組織中唯一可呼叫其中一個替代聯絡人作業，並在`AccountId`參數是指定為委派管理員帳戶用於帳戶管理服務。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作業，則必須允許您使用包含`Resource`任一元素`"*"`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作業，則必須允許您使用包含`Resource`任一元素`"*"`允許所有資源，或ARN，使用組織的成員帳戶的語法。

授與更新帳號屬性的權限

與大多數人一樣AWS作業時，您授與新增、更新或刪除帳號屬性的權限AWS 帳戶通過使用IAM 許可政策。將 IAM 許可政策附加到 IAM 主體 (使用者或角色) 時，您可以指定主體在何種條件下對哪些資源執行哪些動作。

以下是建立權限原則時的一些帳戶管理特定考量事項。

的 Amazon Resource ource ource ource ource ource ource ource ourceAWS 帳戶

- 所以此Amazon Resource Name (ARN)對於一個AWS 帳戶您可以包含在`resource`根據您要參考的科目是獨立科目還是組織中的科目，建構政策陳述式的要素會有所不同。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
    ```

在獨立模式下執行帳號屬性作業時，必須使用此格式，但不包括AccountID參數。

- 組織的成員帳戶的帳戶 ARN：

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

當您以組織模式執行帳號屬性作業時，必須使用此格式，方法是包含AccountID參數。

IAM 政策的上下文金鑰

帳戶管理服務還提供了幾種帳戶管理服務特定的條件金鑰提供對您授予權限的精細控制。

account:AccountResourceOrgPaths

上下文鍵account:AccountResourceOrgPaths可讓您指定通過組織階層到特定組織單位 (OU) 的路徑。只有該 OU 所包含的成員帳戶符合條件。下列範例程式碼片段限制策略僅套用至位於兩個指定 OU 中任何一個的帳戶。

由於account:AccountResourceOrgPaths是多值字串類型，您必須使用ForAnyValue或者ForAllValues多值字串運算子。另外，請注意，條件鍵上的前綴是account，即使您正在參考組織中 OU 的路徑。

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

account:AccountResourceOrgTags

上下文鍵account:AccountResourceOrgTags可讓您參考可附加至組織中帳號的標籤。標籤是索引鍵/值字串配對，可用來對帳戶中的資源進行分類和標記。如需標記的詳細資訊，請參閱Tag Editor中的AWS Resource Groups使用者指南。如需有關使用標籤作為屬性型存取控制策略的一部分的資訊，請參閱的 ABAC 是什麼AWS中的IAM User Guide。下列範例程式碼片段限制策略僅套用至組織中具有金鑰標籤的帳號project和任何一個blue或者red。

由於account:AccountResourceOrgTags是多值字串類型，您必須使用ForAnyValue或者ForAllValues多值字串運算子。另外，請注意，條件鍵上的前綴是account，即使您在組織的成員帳戶上引用了標籤。

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

> **Note**
>
> 您只能將標籤附加至組織中的帳戶。您無法將標籤附加到獨立AWS 帳戶。

更新您的AWS 帳戶聯絡資訊

您可以存儲有關的聯繫信息主要帳戶聯絡人為您的AWS 帳戶。您也可以新增或編輯下列項目的聯絡資訊替代帳戶聯絡人:

- 帳單— 替代帳單聯絡人會收到帳單相關通知，例如發票可用性通知。
- 操作— 替代營運聯絡人將收到與營運相關的通知。
- 安全性— 替代安全聯絡人將收到與安全性相關的通知，包括來自AWS虐待團隊。

主題

- 更新您的替代聯絡人 AWS 帳戶
- 更新您的主要聯絡人 AWS 帳戶

更新您的替代聯絡人 AWS 帳戶

備用聯絡人最多可 AWS 聯絡三位與該帳戶相關聯的備用聯絡人。替代聯絡人不一定是特定人員。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 root 使用者相關聯的電子郵件地址之外的附加資訊。主要帳戶連絡人會繼續收到傳送至 root 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種與帳戶相關聯的聯絡人類型。

- 帳單聯絡人
- 營運聯絡
- 安全聯絡

您可以根據帳戶是獨立帳戶還是組織的一部分，以不同方式新增或編輯替代聯絡人：

- 獨立 AWS 帳戶 — 如果 AWS 帳戶 不與組織產生關聯，您可以使用 AWS 管理主控台或透過 AWS CLI 和 SDK 更新自己的替代連絡人。若要瞭解如何執行此操作，請參閱更新獨立的 AWS 帳戶 替代連絡人。
- AWS 帳戶 組織內 — 對於屬於組 AWS 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 AWS CLI 和 SDK 以程式設計方式更新組織中的任何成員帳戶。若要瞭解如何執行此操作，請參閱更新組織中的 AWS 帳戶 替代連絡人。

主題

- 電話號碼和電子郵件地址要求
- 更新獨立聯絡人的替代聯絡人 AWS 帳戶
- 更新組織 AWS 帳戶 中任何人的替代連絡人
- 帳戶:AlternateContactTypes上下文鍵

電話號碼和電子郵件地址要求

在繼續更新帳戶的備用聯絡人資訊之前，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需求。

- 電話號碼只能包含數字，空格和以下字符：」+-()」。
- 電子郵件地址最多可包含 254 個字元，除了標準英數字元之外，電子郵件地址的本機部分還可以包含下列特殊字元："+=.#|!&-_」。

更新獨立聯絡人的替代聯絡人 AWS 帳戶

若要新增或編輯獨立連絡人的替代連絡人 AWS 帳戶，請執行下列程序中的步驟。下面的 AWS Management Console 程序始終僅適用於獨立上下文。您可以使用僅存 AWS Management Console 取或變更您用來呼叫作業之帳戶中的備用連絡人。

AWS Management Console

若要新增或編輯獨立連絡人的替代連絡人 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`（查看替代聯繫方式）
> - `account:PutAlternateContact`(以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 使用者或角色身分登入。AWS Management Console
2. 在視窗右上方選擇您的帳戶名稱，然後選擇「帳戶」。
3. 在 [帳戶] 頁面上，向下捲動至 [備用聯絡人]，然後選擇標題右側的 [編輯]。

   > **Note**
   >
   > 如果您沒有看到 [編輯] 選項，表示您可能未以帳戶的 root 使用者身分登入，或是以具有上述指定最低權限的使用者身分登入。

4. 變更任何可用欄位中的值。

   > **Important**
   >
   > 對於企業而言 AWS 帳戶，最佳做法是輸入公司電話號碼和電子郵件地址，而不是一個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 等效作業來擷取、更新或刪除替代連絡人資訊：

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **備註**
>
> - 若要從管理帳戶或組織中委派的管理員帳戶對成員帳戶執行這些作業，您必須啟用 Account 服務的受信任存取權。

> **最低許可**
>
> 對於每項作業，您必須擁有對應至該作業的權限：
>
> - `GetAlternateContact`（查看替代聯繫方式）
> - `PutAlternateContact`(以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權限，您可以授予某些使用者僅讀取連絡人資訊的能力，並授予其他使用者讀取和寫入的能力。

Example

下列範例會擷取來電者帳戶目前的 [帳單] 替代連絡人。

```
$ 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

下列範例會為來電者帳戶設定新的 Operations 替代連絡人。

```
$ 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**
>
> 如果您對相同接觸類型 AWS 帳戶 和相同的接觸類型執行多項PutAlternateContact作業，則第一個接觸會加入新接點，並且所有連續呼叫至相同的接觸類型 AWS 帳戶 並更新既有接觸類型。

Example

下列範例會刪除來電者帳戶的安全性替代連絡人。

```
$ 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連絡人，則第一個連絡人會以無訊息的方式成功。所有以後的嘗試都會產生`ResourceNotFound`異常。

更新組織 AWS 帳戶 中任何人的替代連絡人

若要新增或編輯組織 AWS 帳戶 中任何人的替代連絡人詳細資訊，請執行下列程序中的步驟。

要求

若要透過 AWS Organizations 主機更新其他聯絡人，您需要進行一些初步設定：

- 您的組織必須啟用所有功能，才能管理成員帳戶的設定。這允許管理員控制成員帳戶。這是在您建立組織時預設設定的。如果您的組織設定為僅合併帳單，而您想要啟用所有功能，請參閱啟用組織中的所有功能。
- 您必須為 AWS 帳戶管理服務啟用受信任的存取權。若要進行設定，請參閱啟用 AWS 帳戶管理的受信任存取權。

> **Note**
>
> AWS Organizations 受管理的政策`AWSOrganizationsReadOnlyAccess`或`AWSOrganizationsFullAccess`已更新，以提供存取 AWS 帳戶管理 API 的權限，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理策略，請參閱 Organ izations AWS 受管理策略的更新。

AWS Management Console

若要新增或編輯組織 AWS 帳戶 中任何人的替代連絡人

1. 使用組織的管理帳戶認證登入AWS Organizations 主控台。
2. 從中 AWS 帳戶，選取您要更新的帳戶。
3. 選擇 [連絡人資訊]，然後在 [替代聯絡人] 底下，找出連絡人類型：[帳單聯絡人]、[安全性連絡人] 或 [作業
4. 若要新增聯絡人，請選取 [新增]，或選取 [編輯] 來更新現有聯絡人。

5. 變更任何可用欄位中的值。

> **Important**
>
> 對於企業而言 AWS 帳戶，最佳做法是輸入公司電話號碼和電子郵件地址，而不是一個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 等效作業來擷取、更新或刪除替代連絡人資訊：

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **備註**
>
> - 若要從管理帳戶或組織中委派的管理員帳戶對成員帳戶執行這些作業，您必須啟用 Account 服務的受信任存取權。
> - 您無法存取其他組織中的帳戶，而不是您用來呼叫作業的帳戶。

> **最低許可**
>
> 對於每項作業，您必須擁有對應至該作業的權限：
>
> - `GetAlternateContact`（查看替代聯繫方式）
> - `PutAlternateContact`(以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權限，您可以授予某些使用者僅讀取連絡人資訊的能力，並授予其他使用者讀取和寫入的能力。

Example

下列範例會擷取組織中來電者帳戶的目前 [帳單] 替代連絡人。使用的認證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

下列範例會設定組織中指定成員帳戶的「作業」替代聯絡人。使用的認證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**
>
> 如果您對相同接觸類型 AWS 帳戶 和相同的接觸類型執行多項PutAlternateContact作業，則第一個接觸會加入新接點，並且所有連續呼叫至相同的接觸類型 AWS 帳戶 並更新既有接觸類型。

Example

下列範例會刪除組織中指定成員帳戶的安全性替代連絡人。使用的認證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連絡人，則第一個連絡人會以無訊息的方式成功。所有以後的嘗試都會產生ResourceNotFound異常。

帳戶:AlternateContactTypes上下文鍵

您可以使用內容金鑰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 權限政策使用此條件金鑰，允許附加的主體僅擷取組織中特定帳戶的BILLING替代聯絡人，但不能修改。

由account:AlternateContactTypes於是多值字串類型，因此您必須使用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"
                    ]
                }
            }
        }
    ]
}
```

更新您的主要聯絡人 AWS 帳戶

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

您可以根據帳戶是獨立帳戶還是組織的一部份，以不同方式編輯主要帳戶聯絡人：

- 獨立 AWS 帳戶 — 如果與組織AWS 帳戶沒有關聯，您可以使用AWS管理主控台或透過 AWS CLI 和 SDK 更新自己的主要帳戶連絡人。若要瞭解如何執行此操作，請參閱更新獨立的AWS 帳戶主要連絡人。
- AWS 帳戶組織內 — 對於屬於組AWS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 AWS CLI 和 SDK 以程式設計方式更新組織中的任何成員帳戶。若要瞭解如何執行此操作，請參閱更新組織中的AWS 帳戶主要連絡人。

主題

- 電話號碼和電子郵件地址要求
- 更新獨立連絡人的主要連絡人 AWS 帳戶
- 更新組織AWS 帳戶中任何人的主要連絡人

電話號碼和電子郵件地址要求

在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需求。

- 電話號碼只能包含數字，空格和以下字符：」+-()」。
- 電話號碼必須以+和國碼開頭，且國碼後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)。
- 電話號碼應包含區碼、交換代碼和本地代碼之間的連字號 - ""。例如，1 202-555-0179。

> **Note**
>
> 在為 root 使用者重設 MFA 裝置時，輸入不含連字號的電話號碼可能會導致在電話號碼驗證程序期間無法接聽電話。如需詳細資訊，請參閱如何重設 AWS root 使用者帳戶 MFA 裝置？ 。

- 基於安全理由，電話號碼必須能夠接收來自的 SMS AWS。免費電話號碼將不被接受，因為大多數不支持短信。
- 對於企業而言AWS 帳戶，最佳做法是輸入公司電話號碼和電子郵件地址，而不是一個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號 root 使用者可能會讓您的帳戶在離開公司時難以復原。

更新獨立連絡人的主要連絡人 AWS 帳戶

若要編輯獨立版的主要連絡人詳細資料AWS 帳戶，請執行下列程序中的步驟。下面的AWS Management Console程序始終僅適用於獨立上下文。您可以使用AWS Management Console來存取或變更您用來呼叫作業之帳戶的主要聯絡人資訊。

AWS Management Console

若要編輯獨立連絡人的主要連絡人 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`（以查看主要聯繫方式）
> - `account:PutContactInformation`(以更新主要聯絡人詳細資料)

1. 以具有最低許可的 IAM 使用者或角色身分登入。AWS Management Console

2. 在視窗右上方選擇您的帳戶名稱，然後選擇「帳戶」。
3. 向下滾動到部分聯繫信息，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 等效作業來擷取、更新或刪除主要連絡人資訊：

- GetContactInformation
- PutContactInformation

> **備註**
>
> - 若要從管理帳戶或組織中委派的管理員帳戶對成員帳戶執行這些作業，您必須啟用 Account 服務的受信任存取權。

> **最低許可**
>
> 對於每項作業，您必須擁有對應至該作業的權限：
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> 如果您使用這些個別權限，您可以授予某些使用者僅讀取連絡人資訊的能力，並授予其他使用者讀取和寫入的能力。

Example

下列範例會擷取來電者帳戶的目前主要連絡人資訊。

```
$ 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

下列範例會為來電者帳戶設定新的主要連絡人資訊。

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

此命令如果成功就不會產生輸出。

更新組織AWS 帳戶中任何人的主要連絡人

若要編輯組織中任何AWS 帳戶一個的主要連絡人詳細資訊，請執行下列程序中的步驟。

其他要求

若要透過主AWS Organizations機更新主要聯絡人，您需要進行一些初步設定：

- 您的組織必須啟用所有功能，才能管理成員帳戶的設定。這允許管理員控制成員帳戶。這是在您建立組織時預設設定的。如果您的組織設定為僅合併帳單，而您想要啟用所有功能，請參閱啟用組織中的所有功能。
- 您必須為AWS帳戶管理服務啟用受信任的存取權。若要進行設定，請參閱啟用AWS帳戶管理的受信任存取權。

AWS Management Console

若要編輯組織AWS 帳戶中任何一位的主要連絡人

1. 使用組織的管理帳戶認證登入AWS Organizations主控台。
2. 從中 AWS 帳戶，選取您要更新的帳戶。
3. 選擇聯繫信息，然後找到主要聯繫人，
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 等效作業來擷取、更新或刪除主要連絡人資訊：

- GetContactInformation
- PutContactInformation

> **備註**
>
> - 若要從管理帳戶或組織中委派的管理員帳戶對成員帳戶執行這些作業，您必須啟用 Account 服務的受信任存取權。
> - 您無法存取其他組織中的帳戶，而不是您用來呼叫作業的帳戶。

> **最低許可**
>
> 對於每項作業，您必須擁有對應至該作業的權限：
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> 如果您使用這些個別權限，您可以授予某些使用者僅讀取連絡人資訊的能力，並授予其他使用者讀取和寫入的能力。

Example

下列範例會擷取組織中指定成員帳戶的目前主要連絡人資訊。使用的認證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人資訊。使用的認證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。

更新安全性挑戰問題

安全性挑戰問題是先前在帳戶復原案例中用來驗證身分的驗證方法。它們比更現代的驗證形式（例如多因素身份驗證（MFA）更安全。如果您目前有啟用的安全性挑戰問題 AWS 帳戶， AWS Support 可以使用這些問題來協助驗證您是帳戶的擁有者。

> **Important**
>
> 自 2024 年 1 月 5 日起，對於尚未啟用和使用這些問題的帳戶， AWS 將不再支援安全性挑戰問題。這將移除從中的 [帳戶] 頁面新增安全性挑戰問題的選項 AWS Management Console。如果您已經設定安全性挑戰問題，或已在 AWS 組織中的管理帳戶中設定問題，您可以繼續使用這些問題。2025 年 1 月 6 日之後， AWS 將不再支援所有剩餘客戶的安全性挑戰問題。我們鼓勵您MFA改為新增。如需詳細資訊，請參閱AWS 帳戶 停止使用安全性挑戰問題。

若要編輯現有的安全性挑戰問題並提供答案，請執行下列程序中的步驟。

AWS Management Console

若要編輯您的安全性挑戰問題 AWS 帳戶

> **最低許可**
>
> 若要執行下列步驟，您必須至少具備下列IAM權限：
>
> - `account:GetChallengeQuestions`（查看安全挑戰問題）
> - `account:PutChallangeQuestions`（設置或更新安全性挑戰問題）

1. 以具有最低權限的 AWS 帳戶根使用者 IAM使用者或角色身分登入。AWS Management Console
2. 在視窗右上方選擇您的帳戶名稱，然後選擇「帳戶」。
3. 向下滾動到部分安全挑戰問題，然後選擇編輯。

   > **Note**
   >
   > 如果您沒有看到 [編輯] 選項，表示您可能未以帳戶的 root 使用者身分登入，或是以具有上述指定最低權限的使用者身分登入。

4. 變更任何可用欄位中的值。您可以選擇任何提供的問題，然後輸入適當的答案。
5. 完成變更後，請選擇 [更新]。

AWS CLI & SDKs

在 AWS CLI 或其中一個API作業中不支援此工作 AWS SDKs。您只能使用來執行此工作 AWS Management Console。

指定 AWS 區域 您的帳戶可以使用

A AWS 區域是世界上我們有多個可用區域的實體位置。可用區域由一或多個獨立 AWS 資料中心組成，每個資料中心都有備援電源、網路和連線能力，並安裝在不同的設施中。這意味著每個區域都 AWS 區域 是物理上隔離的，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。如需可用區域和即將推出區域的地圖，請參閱區域和可用區域。

除非您明確使用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 AWS 中。例如，Amazon S3 和 Amazon EC2 支援跨區域複寫。某些服務 (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，因此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，以便更接近歐洲客戶或符合法律要求。
- AWS GovCloud (美國西部) 帳戶提供 (美國西部) 區域和 AWS GovCloud (美國東部) 區域的 AWS GovCloud 存取權。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地區的存取權。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 (無端點) 支援的 AWS 服務清單，請參閱區AWS 域服務清單。

> **Important**
>
> AWS 建議您使用地區 AWS Security Token Service (AWS STS) 端點而非全域端點，以減少延遲。來自 AWS 地區 AWS STS 端點的會話令牌在所有區域中都有效。如果您使用區域 AWS STS 端點，則不需要進行任何變更。但是，來自全域 AWS STS 端點 (https://sts.amazonaws.com) 的工作階段權杖僅 AWS 區域 在您啟用時有效，或預設為啟用。如果您打算為您的帳戶啟用新的區域，則可以使用區域 AWS STS 端點的會話令牌，也可以激活全局 AWS STS 端點以發出完全有效的會話令牌 AWS 區域。在所有區域中都有效的會話令牌較

大。如果您存儲會話令牌，則這些較大的令牌可能會影響您的系統。如需 AWS STS 端點如何與區 AWS 域搭配使用的詳細資訊，請參閱AWS STS 在 AWS 區域中管理。

主題

啟用和停用區域前的注意事項

在您啟用或停用「地區」之前，請務必考慮下列事項：

- 2019 年 3 月 20 日之前推出的區域預設為啟用狀態， AWS 最初預設會啟用所有新 AWS 區域 的區域，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為啟用的 [地區]。今天，當新 AWS 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，則必須先啟用該區域。依預設，會停用下列「區域」。

名稱	代碼
非洲 (開普敦)	af-south-1
亞太區域 (香港)	ap-east-1
亞太區域 (海德拉巴)	ap-south-2
亞太區域 (雅加達)	ap-southeast-3
亞太區域 (墨爾本)	ap-southeast-4
加拿大 (卡加利)	ca-west-1
歐洲 (米蘭)	eu-south-1
歐洲 (西班牙)	eu-south-2
歐洲 (蘇黎世)	eu-central-2

名稱	代碼
以色列 (特拉維夫)	`il-central-1`
Middle East (Bahrain)	`me-south-1`
中東 (阿拉伯聯合大公國)	`me-central-1`

- 您可以使用 IAM 許可來控制對區域的存取 — AWS Identity and Access Management (IAM) 包括四個許可，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 AWS 區域中的 AWS：允許啟用和停用。您也可以使用`aws:RequestedRegion`條件鍵來 AWS 服務 控制對 AWS 區域.
- 啟用區域是免費的 — 啟用區域無需任何費用。您只需為在新區域中建立的資源付費。
- 停用某個區域會停用對該區域中資源的 IAM 存取權限 — 如果停用仍包含 AWS 資源的區域 (例如 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，則您將無法存取該區域中資源的 IAM 存取權。例如，您無法使用檢視或變更已停用區域中任何 EC2 執行個體的組態。 AWS Management Console
- 如果您停用「區域」，則有效資源的費用會繼續收費 — 如果停用仍包含 AWS 資源的「區域」，則這些資源的費用 (若有的話) 會繼續以標準費率計算。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 — 停用某個區域後，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數小時才會生效。
- 在某些情況下，啟用區域需要花費幾分鐘到幾個小時 — 啟用區域時， AWS 會執行動作準備該區域中的帳戶，例如將 IAM 資源分配到該區域。對於大多數帳戶來說，此過程需要幾分鐘的時間，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 Organ@@ izations 在指定時間內可以在 AWS 組織中開啟 50 個區域選擇請求 — 管理帳戶可以在任何時間點有 50 個未結請求，等待其組織完成。一個請求等於對一個帳戶啟用或停用一個特定區域。
- 在任何給定時間，單一帳戶可以有 6 個區域選擇請求正在進行-一個請求等於啟用或停用一個帳戶的一個特定區域。
- Amazon EventBridge 整合 — 客戶可以在中訂閱區域選擇狀態更新通知。 EventBridge系統會針對每個狀態變更建立 EventBridge通知，讓客戶自動化工作流程。
- 表現性區域選擇狀態 — 由於啟用/停用選擇加入區域的非同步性質，因此區域選擇請求有四種可能的狀態：
  - `ENABLING`

- DISABLING
- ENABLED
- DISABLED

當選擇加入或選擇退出處於或DISABLING狀態時，您無法取消該選擇加入ENABLING或退出。否則，ConflictException將拋出一個。完成 (啟用/停用) 區域選擇要求取決於主要基礎服務的佈建。 AWS 儘管狀態為，但可能有些 AWS 服務無法立即使用ENABLED。

- 完全整合 AWS Organizations — 管理帳戶可以修改或讀取該 AWS 組織的任何成員帳戶的區域選擇。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

若要更新您 AWS 帳戶 有權存取的區域，請執行下列程序中的步驟。下面的 AWS Management Console 程序始終僅適用於獨立上下文。您可以使 AWS Management Console 用僅檢視或更新您用來呼叫作業之帳戶中的可用區域。

AWS Management Console

若要啟用或停用獨立版的區域 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權限：
>
> - account:ListRegions(需要檢視的清單，以 AWS 區域 及它們目前是否已啟用或停用)。
> - account:EnableRegion
> - account:DisableRegion

1. 以具有最低權限的 IAM 使用者或角色身分登入。AWS Management Console AWS 帳戶根使用者
2. 在視窗右上方選擇您的帳戶名稱，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對此資訊的存取權限。 AWS 傳送要求至與帳戶相關聯的電子郵件地址，以及主要聯絡人電話號碼。選擇要求中的連結，在瀏覽器中開啟該連結，然後核准存取權。

4. 在「動作」欄中 AWS 區域 具有選項的每個項目旁邊，根據您是否希望帳戶中的使用者能夠在該區域中建立和存取資源，選擇「啟用」或「停用」。
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 等效作業來啟用、停用、讀取和列出區域選擇狀態：

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

> **最低許可**
>
> 若要執行下列步驟，您必須擁有對應至該作業的權限：
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

如果您使用這些個別權限，則可以授予某些使用者僅讀取區域選擇資訊的能力，並授予其他使用者讀取和寫入的能力。

下列範例會為組織中指定的成員帳戶啟用區域。使用的認證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指令停用區域，然後enable-region用取代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。

該操作是異步的。以下命令將允許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

若要更新您的成員帳戶的已啟用區域 AWS Organizations，請執行下列程序中的步驟。

> **Note**
>
> AWS Organizations 受管理的政策AWSOrganizationsReadOnlyAccess或AWSOrganizationsFullAccess已更新，以提供存取 AWS 帳戶管理 API 的權限，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理策略，請參閱 Organ izations AWS 受管理策略的更新。

> **Note**
>
> 您必須先從組織中的管理帳戶或委派管理員帳戶執行這些作業，才能執行這些作業，以便搭配成員帳戶使用：
>
> - 啟用組織中的所有功能，以管理成員帳戶的設定。這允許管理員控制成員帳戶。這是在您建立組織時預設設定的。如果您的組織設定為僅合併帳單，而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 帳戶管理」服務的受信任存取權。若要進行設定，請參閱為AWS帳戶管理啟用受信任的存取。

AWS Management Console

若要在組織中啟用或停用區域

1. 使用您組織的管理帳戶認證登入 AWS Organizations 主控台。
2. 在AWS 帳戶頁面上，選取您要更新的帳戶。
3. 選擇 [帳戶設定] 索引標籤。
4. 在地區下，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] 以確認，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 等效作業來啟用、停用、讀取和列出組織成員帳戶的區域選擇狀態：

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

最低許可

若要執行下列步驟，您必須擁有對應至該作業的權限：

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

如果您使用這些個別權限，則可以授予某些使用者僅讀取區域選擇資訊的能力，並授予其他使用者讀取和寫入的能力。

下列範例會為組織中指定的成員帳戶啟用區域。使用的認證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指令停用區域，然後`enable-region`用取代`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**
>
> 一個組織在指定時間最多只能有 20 個區域請求。否則，您將收到一個`TooManyRequestsException`.

該操作是異步的。以下命令將允許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"
  }
```

建立或更新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 識別碼)，而不是 AWS 帳戶 ID，您可以建立帳戶別名。

若要瞭解如何建立或更新帳戶別名，請參閱 IAM 使用指南中的建立、刪除和列出AWS 帳戶別名。

您的帳單AWS 帳戶

對於與計費相關的過程和任務與AWS 帳戶，請參中的下列主題。AWS Billing and Cost Management 使用者指南：

- 變更您用於支付帳單的貨幣

- 更新與刪除稅務登記號碼
- 啟用稅金設定繼承

管理印度帳戶

如果您註冊一個新的AWS 帳戶並選擇印度作為您的聯繫地址，您的用戶協議Amazon Internet Services Private Limited(艾斯普爾), 當地AWS印度的賣家。Aispl 會管理您的帳單，您的發票總金額會以印度盧比 (INR) 列出，而非美元 (USD)。在您與 AISPL 建立帳戶後，就無法變更聯絡資訊中的國家/地區。

如果您有現有的AWS 帳戶使用印度地址，您的帳戶是AWS或 AISPL，具體取決於您打開帳戶的時間。瞭解您的帳戶是否在AWS或艾斯普爾，請參閱Determining which company your account is with。如果您是現有 AWS 客戶，您可以繼續使用 AWS 帳戶。您也可以選擇同時擁有AWS 帳戶和一個 AISPL 帳戶，儘管它們不能合併到同一個帳戶中AWS組織。如需有關管理AWS 帳戶，請參閱管理您的AWS 帳戶。

如果您的帳戶使用 AISPL，請依照本主題中的程序來管理您的帳戶。本主題說明如何註冊 AISPL 帳戶、編輯 AISPL 帳戶的相關資訊，以及新增或編輯永久帳戶號碼 (PAN)。

在註冊期間的信用卡驗證程序中，AISPL 會向您的信用卡收取 2 盧比的費用。驗證完成後，AISPL 會退回這 2 盧比。在驗證過程中您可能會跳轉至您的銀行。

主題

- 確定您的帳戶所在的公司
- 創建一個AWS 帳戶與艾斯普
- 管理您的 AISPL 帳戶

確定您的帳戶所在的公司

AWS 和 AISPL 會一起提供 AWS 服務。請使用此程序來判斷您的帳戶是向哪個銷售商建立的。

AWS Management Console

若要判斷您的帳戶是向哪個公司建立

> **最低許可**
>
> 若要執行下列步驟，您必須至少具備下列 IAM 許可：

- 此程序不需要特殊權限。

1. 打開AWS Management Console在AWS Management Console。
2. 在頁面底部的頁尾中，查看版權聲明。如果著作權屬於 Amazon Web Services，則您的帳戶是向 AWS 建立。如果著作權屬於 Amazon Internet Services Private Ltd.，則您的帳戶是向 AISPL 建立。

AWS CLI & SDKs

中不支援此工作AWS CLI或者通過其中一個 API 操作AWS軟體開發套件。您只能使用AWS Management Console。

創建一個AWS 帳戶與艾斯普

AISPL 是當地的賣家AWS在印度。如果您的聯絡地址位在印度，請使用下列程序註冊 AISPL 帳戶。

AWS Management Console

註冊 AISPL 帳戶

最低許可

若要執行下列步驟，您必須至少具備下列 IAM 許可：

- 因為這個操作發生在你有一個AWS 帳戶，此操作不需要AWS權限。

1. 打開AWS Management Console，然後選擇登入主控台。
2. 在「」登入頁面上，輸入您要使用的電子郵件地址。
3. 在電子郵件地址下方，選取 I am a new user (我是新使用者)，然後選擇 Sign in using our secure server (使用我們的安全伺服器登入)。
4. 在每個登入認證欄位中，輸入您的資訊，然後選擇建立帳戶。
5. 在每個聯絡資訊欄位中，輸入您的資訊。
6. 閱讀過客戶協議後，選取條款和條件核取方塊，然後選擇 Create Account and Continue (建立帳戶並繼續)。

7. 在 Payment Information (付款資訊) 頁面上，輸入您要使用的付款方式。
8. 下泛信息，選擇沒有如果您沒有永久帳戶號碼（PAN）或想稍後添加。如果您有 PAN 且想要立即新增，請選擇是，並在鍋字段輸入你的 PAN。
9. 選擇 Verify Card and Continue (驗證卡片並繼續)。在驗證過程中您必須提供您的 CVV。AISPL 在驗證程序中會向您的卡片收取 2 盧比的費用。驗證完成後，AISPL 會退回這 2 盧比。
10. 對於提供電話號碼，輸入您的電話號碼。如果您有電話分機，對於分機」下方，輸入您的電話分機。
11. 選擇 Call Me Now (立刻打電話給我)。幾分鐘後，四位數 PIN 碼就會顯示在您的螢幕上。
12. 接受 AISPL 的自動語音來電。在電話鍵盤上，輸入螢幕上顯示的四位數 PIN 碼。
13. 自動語音來電驗證您的聯絡號碼後，請選擇 Continue to Select Your Support Plan (繼續選取您的支援方案)。
14. 在 Support Plan (支援方案) 頁面，選擇您的支援方案，然後選擇 Continue (繼續)。在您的付款方式通過驗證並啟用帳戶後，您會收到一封確認帳戶啟用的電子郵件訊息。

AWS CLI & SDKs

中不支援此工作AWS CLI或者通過其中一個 API 操作AWS軟體開發套件。您只能使用AWS Management Console。

管理您的 AISPL 帳戶

除了下列工作外，管理帳戶的程序與在印度境外建立的帳戶相同。請參閱 管理您的AWS 帳戶。

使用AWS Management Console以執行下列工作：

- 新增或編輯永久帳號 (PAN)
- 編輯多個永久帳戶號碼 (PAN)
- 編輯多個商品和服務稅號（GST）
- 檢視稅務發票

關閉 AWS 帳戶

如果您不再需要 AWS 帳戶，可以按照本節中的說明隨時將其關閉。關閉帳戶後，您可以在關閉帳戶當天起 90 天內重新開啟該帳戶。關閉帳戶當天到 AWS 永久關閉帳戶之間的時間範圍稱為關閉後期間。

關閉帳戶前需要了解的內容

在關閉之前 AWS 帳戶，您應該考慮以下幾點：

- 關閉您的帳戶將作為您終止此帳 AWS 戶的客戶協議的通知。
- 在關閉資源 AWS 帳戶 之前，您不需要刪除其中的資源。不過，我們建議您備份要保留的任何資源或資料。如需有關如何備份特定資源的指示，請參閱該服務的適當AWS 文件。
- 您可以在關閉後的期間重新開啟您的帳戶。如果您重新開啟帳戶中剩餘服務的費用將會重新啟動。您也必須對任何未付款的發票、未完成的預留執行個體和 S avings Plan s 負責。
- 您仍然負責關閉帳戶前所使用的服務的所有未付費用和收費。您將在關閉帳戶後的下一個月收到賬 AWS 單。例如，如果您在 1 月 15 日關閉帳戶，您將在 2 月初收到 1 月 1 日至 1 月 15 日期間產生的帳單。關閉帳戶後，您將繼續收到預留執行個體和 S avings Plan s 的發票，直到帳戶過期為止。
- 您將不再能夠訪問以前在您的帳戶中可用的 AWS 服務。但是，您只能 AWS 帳戶 在關閉後期間登錄並訪問已關閉的帳單信息，訪問帳戶設置或聯繫AWS Support人。
- 您不能使用在關閉時註冊的相同電子郵件地址作為其他電子郵件的主要電子郵件地址 AWS 帳戶。AWS 帳戶 如果您想使用相同的電子郵件地址作為不同的電子郵件地址 AWS 帳戶，我們建議您在關閉之前更新它。更新 root 使用者的 AWS 帳戶 名稱、電子郵件地址或密碼如需更新電子郵件地址的指示，請參閱。
- 如果您在 AWS 帳戶 root 使用者上啟用了多重要素驗證 (MFA)，或在使用者上設定了MFA裝置，則在您關閉帳戶時MFA不會自動移除。IAM如果您選擇在關閉後 90 天內保持開MFA啟狀態，請保持MFA裝置啟用狀態，直到關閉後期間過期，以防您在該期間需要存取帳戶。請注意，在永久關閉您的帳戶後，硬件TOTP令牌設備將無法與其他用戶關聯。如果您想稍後與其他用戶一起使用硬件TOTP令牌，則可以選擇在關閉帳戶之前停用硬件MFA設備。MFA帳戶管理員必須刪除使IAM用者的裝置。

成員帳戶的其他注意事項

- 當您關閉成員帳戶時，該帳戶在關閉後期間之後才會從組織中移除。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，請參閱在關閉成員帳戶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。最低帳戶關閉為 10，即使帳戶的 10% 超過 1000，最大帳戶關閉也是 1000。如需 Organizations 配額的詳細資訊，請參閱 AWS Organizations.

- 如果您使用 AWS Control Tower，則需要先取消管理會員帳戶，然後再嘗試關閉帳戶。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，訂閱不會自動取消。如果您有任何訂閱，請先終止訂閱中軟體的所有執行個體。然後，前往 AWS Marketplace 主控台的 [管理訂閱] 頁面，取消您的訂閱。
- 帳戶關閉後，我們 AWS 將在我們暫停域之前最多五天發送每日電子郵件。網域暫停後，視網域註冊商而定，我們會在 30 天內刪除網域，或將網域釋放給其註冊商。如需詳細資訊，請參閱我的 AWS 帳戶 已關閉或永久關閉，以及我的網域已透過 Route 53 註冊。
- AWS CloudTrail 是一項基礎安全服務。這意味著用戶創建的跟踪可以繼續存在，即使在關閉之後傳遞事件，除非用戶在關閉 AWS 帳戶 之前明確刪除其中的跟踪。 AWS 帳戶 在您關閉之前 AWS 帳戶，請考慮下列事項：
  - 即使在封閉後期已過後，小徑仍然存在。關閉後的期限是指從您關閉帳戶到 AWS 永久關閉帳戶之間的 AWS 帳戶 90 天。
  - 此行為也適用於管理帳戶或委派管理員所建立的組織追蹤，以及在組織成員帳戶中建立的多區域組織追蹤。
  - 對於將事件傳遞至相同帳戶中 S3 儲存貯體的追蹤，即使帳戶關閉後，追蹤仍會繼續存在。不過，由於 S3 儲存貯體會在帳戶關閉時刪除，因此追蹤不會繼續傳遞事件。
  - 對於將事件傳遞至不同帳戶中 S3 儲存貯體的追蹤，即使帳戶關閉後，追蹤仍會繼續存在。如果事件可以交付，追蹤也會繼續將事件傳遞至 S3 儲存貯體。例如，如果您關閉組織中的成員帳戶，但未關閉管理帳戶，組織追蹤會繼續將事件傳遞至 S3 儲存貯體。
  - 對於使用加密的跟踪 AWS KMS keys，除了密KMS鑰之外，在帳戶關閉後，跟踪仍然存在。

  如需關閉後如何要求追蹤刪除的詳細資訊和資訊，請參閱CloudTrail 使用者指南中的AWS 帳戶 封閉與追蹤。 AWS 帳戶

如何關閉您的帳戶

您可以 AWS 帳戶 使用以下步驟關閉您的。請注意，每個選項卡中提供了不同的指導，具體取決於您要關閉的帳戶類型 [獨立，成員，管理和 AWS GovCloud (US)]。

如果您在關閉帳戶的過程中遇到任何問題，請參閱AWS 帳戶 關閉問題疑難排解。

Standalone account

獨立帳戶是個別管理的帳戶，不屬於 AWS Organizations。

若要從「帳戶」頁面關閉獨立帳戶

1. 以您要關閉的 AWS Management Console root 使用者身分登入。 AWS 帳戶 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（顯示在關閉對話框的頂部），以確認您已閱讀並了解帳戶關閉過程。
5. 選擇「關閉帳戶」按鈕以啟動科目關閉處理。
6. 在幾分鐘之內，您應該會收到一封電子郵件，確認您的帳戶已被關閉。

> **Note**
>
> 在 AWS CLI 或其中一個API作業中不支援此工作 AWS SDKs。您只能使用來執行此工作 AWS Management Console。

Member account

成員帳戶是屬於 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)。處於合併帳單模式的 Organizations 無法在主控台中看到 [關閉] 按鈕。要以合併帳單模式關閉帳戶，您需要按照獨立帳戶標籤中的步驟進行操作。
4. 閱讀並確保您了解帳戶關閉指南。
5. 輸入會員帳號 ID，然後選擇「關閉帳戶」以啟動帳戶關閉程序。

從「帳戶」頁面關閉成員帳戶

或者，您可以直接從中的「帳戶」頁面關閉 AWS 成員帳戶 AWS Management Console。如需 step-by-step 指引，請依照獨立帳戶標籤中的指示進行。

若要使用和關閉成員帳 AWS CLI 戶 SDKs

如需有關如何使用和關閉成員帳戶的指示 AWS CLI SDKs，請參閱使用AWS Organizations 者指南中的關閉組織中的成員帳戶。

Management account

管理帳號是 AWS 帳戶 做為的父帳號或根帳號 AWS Organizations。

> **Note**
>
> 您無法直接從 AWS Organizations 主控台關閉管理帳戶。

若要從 [帳戶] 頁面關閉管理帳戶

1. 以您要關閉之 AWS Management Console 管理帳戶的根使用者身分登入。以IAM使用者或角色身分登入時，您無法關閉帳戶。
2. 確認您的組織中沒有任何作用中的成員帳戶。為此，請轉到AWS Organizations 控制台，並確保所有成員帳戶都顯示在其帳戶名稱Suspended旁邊。如果您的會員帳戶仍處於活動狀態，則需要遵循「會員帳戶」標籤中提供的帳戶關閉指引，然後才能進入下一步。
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（顯示在關閉對話框的頂部），以確認您已閱讀並了解帳戶關閉過程。
6. 選擇「關閉帳戶」按鈕以啟動科目關閉處理。
7. 在幾分鐘之內，您應該會收到一封電子郵件，確認您的帳戶已被關閉。

> **Note**
>
> 在 AWS CLI 或其中一個API作業中不支援此工作 AWS SDKs。您只能使用來執行此工作 AWS Management Console。

AWS GovCloud (US) account

基於 AWS GovCloud (US) 帳單和付款目的，帳戶永遠會與單一標準 AWS 帳戶 連結。

關閉帳 AWS GovCloud (US) 戶

如果您有 AWS 帳戶 已連結至 AWS GovCloud (US) 帳戶的帳戶，則必須先關閉標準帳戶，才能關閉 AWS GovCloud (US) 帳戶。有關更多詳細信息，包括如何備份數據並避免意外 AWS GovCloud (US) 費 AWS GovCloud (US) 用，請參閱用戶指南中的關閉 AWS GovCloud (US) 帳戶。

關閉帳戶後會有什麼期望

在您關閉帳戶後，將立即發生以下情況：

- 您將收到一封電子郵件，確認帳戶關閉到 root 用戶的電子郵件地址。如果您在幾個小時內沒有收到此電子郵件，請參閱AWS 帳戶 關閉問題疑難排解。
- 您關閉的任何成員帳戶都會在 AWS Organizations 主控台的帳戶名稱旁邊顯示一個SUSPENDED標籤。
- 如果您已授予存取其他帳戶中服務的 AWS 帳戶 權限，從這些帳戶發出的任何存取要求都應該會在帳戶關閉後失敗。如果您重新開啟您的帳戶 AWS 帳戶，其他人 AWS 帳戶 可以再次存取您帳戶的 AWS 服務和資源 (如果您授予他們必要的權限)。

關閉後期

關閉後的期限是指您關閉帳戶之間的時間長度，以及 AWS 永久關閉帳戶之間的 AWS 帳戶時間長度。關閉後的期限為 90 天。在關閉後期間，您只能通過重新開設帳戶來訪問您的內容和 AWS 服務。在關閉後期間之後， AWS 永久關閉您的 AWS 帳戶，您將無法再重新打開它。 AWS 同時也會刪除您帳戶中的任何內容和資源。永久關閉帳戶後，其 AWS 帳戶 ID 將永遠不能重複使用。

重新開放您的 AWS 帳戶

您的帳戶將在 90 天後永久關閉，之後您將無法重新開啟帳戶，並且 AWS 會刪除帳戶中剩餘的內容。若要在帳戶永久關閉之前重新開啟您的帳戶，(1) 您必須AWS Support儘快聯絡，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全額付款，包括提供發票上指定的必要資訊。

> **Note**
>
> 如果您重新開啟帳戶中剩餘服務的費用將會重新啟動。

在組織中使用AWS帳戶管理

AWS Organizations是您可以用來管理您的群組AWS 帳戶的AWS服務。這提供了諸如合併帳單之類的功能，其中所有帳戶的帳單都會分組在一起，並由單一付款人處理。您也可以使用以原則為基礎的控制項，集中管理組織的安全性。如需有關 AWS Organizations 的詳細資訊，請參閱《使用者指南》AWS Organizations。

受信任的存取權

當您使用群組AWS Organizations來管理帳戶時，組織的大多數系統管理工作只能由組織的管理帳戶執行。依預設，這只包括與管理組織本身相關的作業。您可以啟用組織與該AWS服務之間的信任存取，將此額外功能延伸至其他服務。受信任的存取權會授與指定AWS服務的權限，以存取有關組織及其所包含帳戶的資訊。當您啟用「帳戶管理」的受信任存取權時，帳戶管理服務會授與組織及其管理帳戶存取組織所有成員帳戶中繼資料的權限，例如主要或替代聯絡人資訊。

如需詳細資訊，請參閱為AWS帳戶管理啟用受信任的存取。

委派管理員

啟用信任存取後，您也可以選擇將其中一個成員帳戶指定為帳戶管理的委派管理員AWS帳戶。這可讓委派的管理員帳戶對組織中的成員帳戶執行相同的帳戶管理中繼資料管理工作，而這些工作之前只有管理帳戶可以執行。委派的管理員帳戶只能存取帳戶管理服務的管理工作。委派的管理員帳戶沒有管理帳戶擁有之組織的所有系統管理存取權。

如需詳細資訊，請參閱啟用委派管理員帳户AWS帳戶管理。

服務控制政策

當您屬AWS 帳戶於由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原則 (SCP)，以限制成員帳戶中的主參與者可執行的動作。SCP 永遠不會授予權限；相反，它是一個過濾器，用於限制成員帳戶可以使用的權限。成員帳戶中的使用者或角色 (主體) 只能執行那些作業，這些作業與 SCP 適用於該帳戶和附加至主體的 IAM 權限政策所允許的項目相交。例如，您可以使用 SCP 來防止帳戶中的任何主體修改其帳戶的替代聯絡人。

例如，適用於的 SCPAWS 帳戶，請參閱限制存取AWS Organizations服務控制政策。

為AWS帳戶管理啟用受信任的存取

啟用「AWS帳戶管理」的受信任存取權，可讓管理帳戶的管理員修改中每個成員帳戶特定的資訊和中繼資料 (例如，主要或替代聯絡人詳細資料) AWS Organizations。如需詳細資訊，請參閱AWS帳戶管

理和AWS Organizations使用指南AWS Organizations中的。如需受信任存取如何運作的一般資訊，請參閱AWS Organizations搭配其他AWS服務使用。

啟用受信任存取權之後，您可以在支援該accountID參數的帳戶管理 API 作業中使用該參數。只有在使用管理帳戶的認證呼叫作業時，才能成功使用此參數，或從組織的委派管理員帳戶 (如果啟用) 呼叫作業。如需詳細資訊，請參閱啟用委派管理員帳户AWS帳戶管理。

請使用下列程序來啟用組織中「帳戶管理」的受信任存取權。

> **最低許可**
>
> 若要執行這些工作，您必須符合下列需求：
>
> - 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帳戶管理的受信任存取

1. 登入 AWS Organizations 主控台。您必須以 IAM 使用者登入、擔任 IAM 角色，或是以組織管理帳戶中的根使用者 (不建議) 身分登入。
2. 在導覽窗格中選擇 [服務]。
3. 在服務列表中選擇「AWS帳戶管理」。
4. 選擇 Enable trusted access (啟用信任存取)。
5. 在 [啟用AWS帳戶管理的受信任存取權限] 對話方塊中，輸入 enable 加以確認，然後選擇 [啟用信任的存取]。

AWS CLI & SDKs

啟用AWS帳戶管理的受信任存取

執行下列命令後，您可以使用組織管理帳戶中的認證呼叫帳戶管理 API 作業，這些作業使用--accountId參數來參照組織中的成員帳戶。

- AWS CLI: enable-aws-service-access

  下列範例會在通話帳戶的組織中啟用「AWS帳戶管理」的受信任存取權。

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

此命令如果成功就不會產生輸出。

啟用委派管理員帳戶AWS帳戶管理

委派管理員帳戶可以調用AWS組織中其他成員帳戶的賬戶管理 API 操作。要將組織中的成員帳戶指定為委派管理員帳戶，請按以下步驟操作。

最低許可

若要執行這些任務，您必須符合下列要求：

- 您可以從組織的管理帳戶來執行這項作業。
- 您的組織必須啟用所有功能。
- 您必須有為您的組織中的賬戶管理啟用了可信訪問。

為組織指定委派管理員帳戶後，該帳戶中的用户和角色可以調用AWS CLI和AWS軟件開發工具包操作`account`命名空間，可以在 Organizations 模式下工作，方法是支持可選`AccountId`參數。

AWS Management Console

此任務在AWS帳戶管理主控台。您可以使用AWS CLI或者來自其中一個AWS開發套件。

AWS CLI & SDKs

為賬戶管理服務註冊委派管理員帳戶

您可以使用下列命令來啟用帳戶管理服務的委派管理員。

您必須指定下列服務委託人：

```
account.amazonaws.com
```

- AWS CLI：註冊-委託管理員

  以下示例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。

運行此命令後，您可以使用來自帳戶 123456789012 的憑據來調用賬戶管理AWS CLI和 SDK API 操作，這些操作使用`--account-id`參數來引用組織中的成員帳戶。

限制存取AWS Organizations服務控制政策

本主題提供的範例說明如何使用服務控制政策 (SCP) 來限制組織帳戶中的使用者和角色可以執行的動作。如需有關服務控制政策的詳細資訊，請參閱中的下列主題AWS Organizations使用者指南：

- 建立 SCP
- 將 SCP 附加至作業單位和帳戶
- SCP 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

下面的例子拒絕`PutAlternateContact`和`DeleteAlternateContact`API 操作由中的任何成員帳戶調用獨立帳戶模式。這樣可以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

下面的例子概括Resource元素為「*」，這意味著它適用於兩者獨立模式請求與組織模式請求。這表示即使是帳戶管理的委派管理員帳戶 (如果套用 SCP)，也會遭到封鎖，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 中的成員帳戶修改其本身的替代連絡人

下列範例 SCP 包含一個條件，可將帳戶的組織路徑與兩個 OU 清單進行比較。這會導致封鎖指定 OU 中任何帳戶中的主體，使其無法修改其本身的替代連絡人。

```
{
    "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/"
                    ]
                }
```

```
            }
    ]
}
```

中的安全AWS帳戶管理

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同肩負的責任。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：

- 雲端本身的安全 – AWS 負責保護執行 AWS 雲端 內 AWS 服務的基礎設施。AWS 提供的服務，也可讓您安全使用。第三方稽核人員會定期測試和驗證我們安全性的有效性，作為 AWS 合規計劃的一部分。若要了解適用於帳號管理的合規計劃，請參AWS 服務在範圍內按合規性計劃。
- 雲端內部的安全 – 您的責任取決於所使用的 AWS 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

本文件有助於您了解如何在使用AWS帳號管理。它會示範如何設定帳號管理以符合您的安全性和合規目標。您也會了解如何使用其他AWS服務，協助您監控並保護帳號管理資源。

主題

- 帳戶管理中的AWS資料保護
- AWS PrivateLink為了AWS帳戶管理
- AWS 帳戶管理的 Identity and Access Management
- AWS受管理的政策AWS帳戶管理
- AWS帳戶管理的合規性驗證
- 中的恢復能力AWS帳戶管理
- AWS Account Management 中的基礎設施安全

帳戶管理中的AWS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 AWS 雲端 的全球基礎設施。您必須負責維護在此基礎設施上託管之內容的控制權。您也必須負責您所使用的 AWS 服務 安全性設定和管理工作。如需有關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，建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 憑證，並設定個別使用者。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 AWS CloudTrail 設定 API 和使用者活動記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務 內的所有預設安全控制項。
- 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。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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 Name (名稱) 欄位。這包括當您使用主控台、API 或 AWS SDK AWS 服務 使用帳戶管理或其他工作時。AWS CLI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為了AWS帳戶管理

如果您使用 Amazon Virtual Private Cloud (Amazon VPC) 來託管您的AWS資源時，您可以使用AWS從 VPC 內部的賬户管理服務，而無需跨公共互聯網。

使用亞馬遜 VPC，您可以啟動AWS資源在自訂虛擬網路中。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 VPC 的詳細資訊，請參Amazon VPC User Guide。

要將您的亞馬遜 VPC 連接到賬户管理，您必須首先定義界面 VPC 端點，使您可以使 VPC 與其他AWS服務。端點可提供可靠、可擴展的連線能力，且不需要網際網路閘道、網路地址轉譯 (NAT) 執行個體或 VPN 連接。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的界面 VPC 端點 (AWS PrivateLink)。

建立端點

您可以建立AWS賬户管理終端節點使用AWS Management Console，AWS Command Line Interface(AWS CLI），一個AWS軟體開發套件，AWS賬户管理 API，或AWS CloudFormation。

如需使用 Amazon VPC 主控台或 AWS CLI，請參閱 Amazon VPC 使用者指南中的建立界面端點。

> **Note**
>
> 建立端點時，請使用以下格式指定帳戶管理作為您希望 VPC 連線的目標服務：
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> 您必須完全按照所示使用字符串，指定us-east-1區域。作為一項全球性服務，賬戶管理僅託管在AWS區域。

如需使用 AWS CloudFormation 建立和設定端點的詳細資訊，請參閱 AWS CloudFormation 使用者指南中的 AWS::EC2::VPCEndpoint 資源。

Amazon VPC 端點政策

您可以通過在創建 Amazon VPC 終端節點時附加終端節點策略來控制可通過此服務終端節點執行的操作。您可以通過附加多個端點政策來建立複雜的 IAM 規則。如需更多詳細資訊，請參閱：

- Amazon Virtual Private Cloud 端點政策
- 使用 VPC 端點控制對服務的存取中的AWS PrivateLink指南。

Amazon Virtual Private Cloud 端點政策

您可以為賬戶管理建立 Amazon VPC 端點政策，在其中您可以指定以下內容：

- 可執行動作的委託人。
- 委託人可以執行的動作。
- 可供執行動作的資源。

以下示例顯示了一個 Amazon VPC 終端節點策略，該策略允許賬戶 123456789012 中名為 Alice 的一個 IAM 用户檢索和更改任何AWS 帳戶，但拒絕所有 IAM 用户刪除任何賬户上的任何備用聯繫人信息的權限。

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

```
                "account:GetAlternateContact",
                "account:PutAlternateContact"
            ],
            "Resource": "arn:aws::iam:*:account,
            "Effect": "Allow",
            "Principal": {
              "AWS": "arn:aws::iam:123456789012:user/Alice"
            }
        },
        {
            "Action": "account:DeleteAlternateContact",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "arn:aws::iam:*:root"
        }
    ]
}
```

如果您要授予對屬於AWS組織轉換為位於組織成員帳戶中的委託人，然後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，請參使用 VPC 端點控制對服務的存取中的AWS PrivateLink指南。

AWS 帳戶管理的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM系統管理員控制誰可以驗證 (登入) 和授權 (具有權限) 使用帳戶管理資源。IAM是您 AWS 服務 可以免費使用的。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- AWS 帳戶管理如何使用 IAM
- 帳戶管理的基於身份的政策示例 AWS
- 使用基於身份的策略（IAM策略）進行帳戶 AWS 管理
- 疑難排解 AWS 帳戶管理身分和存取

物件

根據您在帳戶管理中執行的工作， AWS Identity and Access Management (IAM) 的使用方式會有所不同。

服務使用者 — 如果您使用帳戶管理服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多帳戶管理功能來完成工作時，您可能需要額外的權限。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。如果您無法在帳戶管理中使用某項功能，請參閱疑難排解 AWS 帳戶管理身分和存取。

服務管理員 — 如果您負責公司的帳戶管理資源，您可能擁有帳戶管理的完整存取權。決定您的服務使用者應該存取哪些帳戶管理功能和資源是您的工作。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要深入瞭解貴公司如何IAM搭配帳戶管理使用，請參閱AWS 帳戶管理如何使用 IAM。

IAM系統管理員 — 如果您是IAM系統管理員，您可能想要瞭解如何撰寫原則以管理帳戶管理存取權限的詳細資訊。若要檢視您可以在中使用的帳戶管理基於身分的策略範例IAM，請參閱。帳戶管理的基於身份的政策示例 AWS

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以IAM使用者身分或假設IAM角色來驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您使 AWS 用同盟存取時，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。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以密碼編譯方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署要求的詳細資訊，請參閱使用IAM者指南中的簽署 AWS API要求。

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 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。若要深入瞭解，請參閱使用AWS IAM Identity Center 者指南中的多重要素驗證和使用多重要素驗證 (MFA) AWS的使用IAM者指南。

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，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 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。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

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，也可以連線並同步處理至您自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需IAM身分識別中心的相關資訊，請參閱IAM識別中心是什麼？ 在《AWS IAM Identity Center 使用者指南》中。

IAM 使用者和群組

IAM使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。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的群組，IAMAdmins並授與該群組管理IAM資源的權限。

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，但角色僅提供暫時憑證。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM 角色

IAM角色是您 AWS 帳戶 中具有特定權限的身份。它類似於用IAM戶，但不與特定人員相關聯。您可以切換角色來暫時擔任中 AWS Management Console 的角色。IAM您可以呼叫 AWS CLI 或 AWS

API作業或使用自訂來擔任角色URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 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。如需聯合角色的相關資訊，請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。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使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用者指南》IAM中的〈跨帳號資源存取〉。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 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。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。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會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。
  - 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。
- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行的應用程式以及發出 AWS CLI 或 AWS API請求的臨時登入資料。這比在EC2實例中存儲訪問密鑰更好。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以JSON文件的形式儲存在中。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或取得角色資訊 AWS API。

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。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。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

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。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的策略IAM中使用 AWS 受管政策。

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3 和 Amazon VPC 是支持服務的示例ACLs。 AWS WAF若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務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原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。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。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的JSON策略 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個帳戶 AWS 帳戶根使用者。若要取得有關 Organizations 的更多資訊SCPs，請參閱《AWS Organizations 使用指南》中的〈SCPs運作方式〉
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。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使用指南中的工作階段原則。

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。若要瞭解如何在涉及多個原則類型時 AWS 決定是否允許要求，請參閱IAM使用指南中的原則評估邏輯。

AWS 帳戶管理如何使用 IAM

在您用IAM來管理帳戶管理的存取權限之前，請先了解哪些IAM功能可與帳戶管理搭配使用。

IAM可與 AWS 帳戶管理搭配使用的功能

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
ACLs	否
ABAC(策略中的標籤)	是
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	否

若要深入瞭解帳戶管理和其他 AWS 服務如何搭配大部分IAM功能運作，請參閱IAM使用者指南IAM中的適用AWS 服務。

帳戶管理的基於身份的策略

支援以身分識別為基礎的原則：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。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。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。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。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

帳戶管理的基於身份的政策示例

若要檢視帳戶管理以身分識別為基礎的策略範例，請參閱。帳戶管理的基於身份的政策示例 AWS

帳戶管理中的資源型政策

支援以資源為基礎的政策：否

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (使用者或角色) 權限，才能存取資源。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使用指南》IAM中的〈跨帳號資源存取〉。

帳號管理的政策動作

支援原則動作：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON策略`Action`元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯的 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。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清單，請參閱服務授權參考中的AWS 帳戶管理定義的動作。

帳號管理中的策略動作會在動作之前使用下列前置詞。

```
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，若要指定與替代連絡人配合使用 AWS 帳戶的所有動作，請包含下列動作。

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

若要檢視帳戶管理以身分識別為基礎的策略範例，請參閱。帳戶管理的基於身份的政策示例 AWS

用於帳戶管理的政策資源

支援原則資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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。

ResourceJSON原則元素會指定要套用動作的一或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 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": "*"
```

帳號管理服務在IAM策略的Resources元素中支援下列特定資源類型，可協助您篩選策略並區分這些類型 AWS 帳戶：

- account

  此resource類型僅符合不 AWS 帳戶 是服務所管理之組織中成員帳戶的獨立帳 AWS Organizations 戶。

- accountInOrganization

  此resource類型僅 AWS 帳戶 符合服務所管理之組織中的成員帳 AWS Organizations 戶。

若要查看帳號管理資源類型及其清單ARNs，請參閱服務授權參考中的AWS 帳號管理定義的資源。若要瞭解您可以針對每個資源指定哪些動作，請參閱 AWS 帳號管理定義ARN的動作。

若要檢視帳戶管理以身分識別為基礎的策略範例，請參閱。帳戶管理的基於身份的政策示例 AWS

帳戶管理的政策條件金鑰

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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，請使用邏輯OR運算來 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，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》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條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

帳戶管理服務支援下列條件金鑰，您可以使用這些金鑰為您的IAM政策提供精細篩選：

- 帳戶：TargetRegion

  此條件鍵採用由AWS 區域代碼清單組成的引數。它可讓您篩選原則，使其僅影響套用至指定區域的動作。
- 帳戶：AlternateContactTypes

  此條件鍵會取得替代接觸類型的清單：

  - BILLING
  - OPERATIONS
  - SECURITY

  使用此鍵可讓您將要求篩選為僅針對指定替代連絡人類型的動作。

- 帳戶：AccountResourceOrgPaths

  此條件索引鍵採用一個引數，該引數包含代表組織中帳戶的萬ARNs用字元清單。它可讓您篩選策略，使其僅影響針對該相符帳號ARNs的動作。例如，下列ARN項目僅符合指定組織和指定組織單位 (OU) 中的帳戶。

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

- 帳戶：AccountResourceOrgTags

  此條件鍵採用由標籤鍵和值清單組成的引數。它可讓您篩選策略，使其僅影響屬於組織成員且使用指定標籤索引鍵和值標記的帳戶。

若要查看帳戶管理條件金鑰清單，請參閱服務授權參考資料中的AWS 帳戶管理的條件金鑰。若要瞭解可以使用條件金鑰的動作和資源，請參閱AWS 帳號管理定義的動作。

若要檢視帳戶管理以身分識別為基礎的策略範例，請參閱。帳戶管理的基於身份的政策示例 AWS

帳戶管理中的存取控制清單

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

以屬性為基礎的存取控制與帳號管理

支援 ABAC (策略中的標籤): 是

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

透過帳戶管理使用臨時憑證

支援臨時登入資料:是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。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認證。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。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。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，而非使用長期存取金鑰。如需詳細資訊，請參閱IAM。

帳戶管理的跨服務主體權限

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色在中執行動作時 AWS，您會被視為主參與者。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會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

帳戶管理的服務角色

支援服務角色：否

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色 IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給

帳戶管理服務連結角色

支援服務連結角色：否

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需有關建立或管理服務連結角色的詳細資訊，請參閱使用IAM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。

帳戶管理的基於身份的政策示例 AWS

根據預設，使用者和角色沒有建立或修改帳號管理資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或執行工作 AWS API。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

若要瞭解如何使用這些範例原則文件來建立以IAM身分識別為基礎的JSON策略，請參閱使用指南中的IAM建立IAM策略。

如需有關帳號管理所定義的動作和資源類型的詳細資訊，包括每種資源類型的格式，請參閱服務授權參考中的AWS 帳號管理的動作、資源和條件金鑰。ARNs

主題

- 政策最佳實務
- 使用中的 [帳戶] 頁面 AWS Management Console
- 提供對「帳戶」頁面的唯讀存取權 AWS Management Console
- 提供對「帳戶」頁面的完整存取權 AWS Management Console

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以在您的帳戶中建立、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 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，請參閱AWS 《IAM使用指南》中針對工作職能的AWS 受管理策略或受管理的策略。
- 套用最低權限權限 — 當您使用原則設定權限時，IAM只授與執行工作所需的權限。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。如需有關使用套用權限IAM的詳細資訊，請參閱《使用指南》IAM中的IAM《策略與權限》。
- 使用IAM策略中的條件進一步限制存取 — 您可以在策略中新增條件，以限制對動作和資源的存取。例如，您可以撰寫政策條件，以指定必須使用傳送所有要求SSL。您也可以使用條件來授與對服務動

作的存取權 (如透過特定 AWS 服務) 使用 AWS CloudFormation。如需詳細資訊，請參閱《IAM使用指南》中的IAMJSON策略元素：條件。

- 使用 IAM Access Analyzer 驗證您的原IAM則，以確保安全和功能性的權限 — IAM Access Analyzer會驗證新的和現有的原則，以便原則遵循IAM原則語言 (JSON) 和IAM最佳做法。IAMAccess Analyzer 提供超過 100 項原則檢查和可行的建議，協助您撰寫安全且功能正常的原則。如需詳細資訊，請參閱IAM使IAM用指南中的存取分析器原則驗證。
- 需要多因素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟以取得額外MFA的安全性。若要在呼叫API作業MFA時需要，請在原則中新增MFA條件。如需詳細資訊，請參閱《IAM使用指南》中的 < 設定MFA受保護的API存取 > 。

如需有關中最佳作法的詳細資訊IAM，請參閱《IAM使用指南》IAM中的「安全性最佳作法」。

使用中的 [帳戶] 頁面 AWS Management Console

若要存取中的「帳戶」頁面 AWS Management Console，您必須擁有最少一組權限。這些權限必須允許您列出並檢視您的 AWS 帳戶. 如果您建立的以身分識別為基礎的原則比所需的最低權限更嚴格，則控制台將無法如預期用於具有該原則的實體 (IAM使用者或角色) 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 受管理的策略附加到實體。如需詳細資訊，請參閱《使用指南》中的〈將權限新增至IAM使用者〉。

您不需要為只對 AWS CLI或撥打電話的使用者允許最低主控台權限 AWS API。相反地，在許多情況下，您可以選擇只允許存取與您嘗試執行之作API業相符的動作。

提供對「帳戶」頁面的唯讀存取權 AWS Management Console

在下列範例中，您想要授與IAM使用者對於中「帳戶」頁面的 AWS 帳戶 唯讀存取權 AWS Management Console。附加此原則的使用者無法進行任何變更。

此`account:GetAccountInformation`動作會授與檢視 [帳戶] 頁面上大部分設定的存取權。不過，若要檢視目前啟用的「 AWS 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": "*"
        }
    ]
}
```

提供對「帳戶」頁面的完整存取權 AWS Management Console

在下列範例中，您想要授與IAM使用者對於中「帳戶」頁面的 AWS 帳戶 完整存取權限 AWS Management Console。附加此策略的使用者可以變更帳號的設定。

此範例原則建立在上述範例原則之上，方法是新增每個可用的寫入權限 (除了 CloseAccount)，讓使用者變更帳戶的大部分設定，包括`account:EnableRegion`和`account:DisableRegion`權限。

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

使用基於身份的策略（IAM策略）進行帳戶 AWS 管理

有關 AWS 帳戶 和IAM用戶的完整討論，請參閱什麼是IAM？ 在《IAM使用者指南》中。

如需有關如何更新客戶受管政策的指示，請參閱IAM使用指南中的編輯客戶管理策略 (主控台)。

AWS 帳號管理動作政策

此表格總結列出授與帳戶設定存取權的權限。如需使用這些權限的策略範例，請參閱AWS 帳戶管理策略範例。

> **Note**
>
> 若要授與使用IAM者對「帳戶」頁面中特定帳戶設定的寫入GetAccountInformation權限 AWS Management Console，除了要用來修改該設定的權限 (或權限) 之外，您還必須允許該權限。

許可名稱	存取層級	描述
account:ListRegions	清單	授予列出可用區域的權限。
account:GetAccountInformation	讀取	授予擷取帳戶帳戶資訊的權限。
account:GetAlternateContact	讀取	授予擷取帳戶替代聯絡人的權限。
account:GetChallengeQuestions	讀取	授予擷取帳號提示問題的權限。
account:GetContactInformation	讀取	授予擷取帳戶主要聯絡人資訊的權限。
account:GetRegionOptStatus	讀取	授予取得區域選擇加入狀態的權限。
account:AcceptPrimaryEmailUpdate	寫入	授予接受 AWS 組織中成員帳戶主要電子郵件地址更新的權限。
account:CloseAccount	寫入	授予關閉帳戶的權限。

許可名稱	存取層級	描述
		Note 此許可僅適用於主控台。此權限沒有可用的API存取權。
account:DeleteAlternateContact	寫入	授予刪除帳戶替代聯絡人的權限。
account:DisableRegion	寫入	授予禁用區域使用的權限。
account:EnableRegion	寫入	授予允許使用區域的權限。
account:PutAlternateContact	寫入	授予修改帳戶替代聯絡人的權限。
account:PutChallengeQuestions	寫入	授予修改帳號提示問題的權限。 Note 此許可僅適用於主控台。此權限沒有可用的API存取權。
account:PutContactInformation	寫入	授予更新帳戶主要聯絡人資訊的權限。
account:StartPrimaryEmailUpdate	寫入	授予啟動 AWS 組織中成員帳戶主要電子郵件地址更新的權限。

疑難排解 AWS 帳戶管理身分和存取

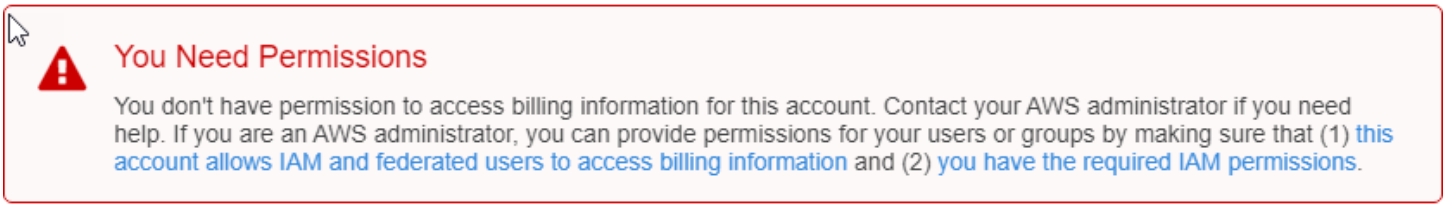
使用下列資訊可協助您診斷並修正使用帳戶管理和時可能會遇到的常見問題IAM。

主題

我沒有在「帳戶」頁面中執行動作的授權

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡您的管理員以尋求協助。您的管理員是提供您使用者名稱和密碼的人員。

當使用mateojacksonIAM者嘗試使用主控台 AWS 帳戶 在的 [帳戶] 頁面中檢視他的詳細資料， AWS Management Console 但沒有account:GetAccountInformation權限時，就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

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的政策，以允許您將角色傳遞給帳戶管理。

有些 AWS 服務 允許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。

當名為的使用IAM者marymajor嘗試使用主控台在帳戶管理中執行動作時，就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 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪問我 AWS 帳戶 的帳戶詳細信息

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。對於支援以資源為基礎的政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策授與人員存取您的資源。

如需進一步了解，請參閱以下內容：

- 若要瞭解帳戶管理是否支援這些功能，請參閱AWS 帳戶管理如何使用 IAM。
- 若要瞭解如何提供您所擁有資 AWS 帳戶 源的存取權，請參閱《IAM使用指南》中的〈提供存取權給您 AWS 帳戶 所擁有的其他IAM使用者〉。
- 若要瞭解如何將您的資源存取權提供給第三方 AWS 帳戶，請參閱《IAM使用指南》中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要瞭解如何透過身分聯盟提供存取權，請參閱《使用指南》中的提供對外部驗證使用IAM者的存取權 (身分聯合)。
- 若要瞭解針對跨帳號存取使用角色與以資源為基礎的政策之間的差異，請參閱《使用IAM者指南》IAM中的〈跨帳號資源存取〉。

AWS受管理的政策AWS帳戶管理

AWS帳戶管理目前提供兩種AWS可供您使用的受管理策略：

- AWS 受管政策：AWSAccountManagementReadOnlyAccess
- AWS 受管政策：AWSAccountManagementFullAccess
- 帳戶管理更新AWS受管理政策

AWS 受管政策是由 AWS 建立和管理的獨立政策。AWS 受管政策的設計在於為許多常見使用案例提供許可，如此您就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與您特定使用案例的最低權限許可，因為它們可供所有 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。

您無法更改 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，更新會影響政策連接的所有主體身分 (使用者、群組和角色)。在推出新的 AWS 服務 或有新的 API 操作可供現有服務使用時，AWS 很可能會更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html#aws-managed-policies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。

此原則提供只檢視下列項目的唯讀權限：

- 關於您的中繼資料AWS 帳戶
- 該AWS 區域已啟用或停用AWS 帳戶(您只能在帳戶中檢視區域狀態，只能使用AWS控制台)

它通過授予運行任何的權限來執行此操作Get*或者List*操作。它不提供任何修改帳戶元數據或啟用或禁用的功能AWS 區域對於該帳戶。

許可詳細資訊

此政策包含以下許可。

- account— 允許主參與者擷取有關的中繼資料資訊AWS 帳戶。它還允許主參與者列出AWS 區域已針對中的帳戶啟用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。

此原則提供檢視或修改下列項目的完整管理存取權限：

- 關於您的中繼資料AWS 帳戶
- 該AWS 區域已啟用或停用AWS 帳戶(您可以檢視狀態或啟用或停用帳戶的區域，只有使用AWS控制台)

它通過授予運行任何權限來做到這一點account操作。

許可詳細資訊

此政策包含以下許可。

- account— 允許主參與者檢視或修改有關的中繼資料資訊AWS 帳戶。它還允許主參與者列出AWS區域已針對帳戶啟用，並在AWS Management Console。

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

帳戶管理更新AWS受管理政策

檢視有關更新的詳細資訊AWS由於此服務開始追蹤這些變更，因此帳戶管理的受管理政策。如需有關此頁面變更的自動警示，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帳戶管理推出全新AWS受管理的政策並開始追蹤變更	帳戶管理最初啟動，具有以下內容AWS受管理的策略：	2021 年 9 月 30 日

變更	描述	日期
	• AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	

AWS帳戶管理的合規性驗證

協力廠商稽核人員會評估可在您的多個合規方案中執行的AWS服務AWS 帳戶的安全性與合AWS規性。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需特定法規遵循方案範圍內的AWS服務清單，請參閱AWS 服務合規性計劃範圍內的合規性計劃的服務。如需一般資訊，請參閱 AWS 合規計畫。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱《AWS Artifact使用指南》中的〈AWS Artifact的〈下載報告〉。

在您使用服務時，您的合規責任取決AWS 帳戶於您資料的敏感性、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遵循法規：

- 安全與合規快速入門指南 – 這些部署指南討論在 AWS 上部署以安全及合規為重心的基準環境的架構考量和步驟。
- Amazon Web Services 的 HIPAA 安全與合規架構：本白皮書說明公司可如何運用 AWS 來建立符合 HIPAA 規定的應用程式。

> **Note**
>
> 並非全部的 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：這組手冊和指南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 服務可評估資源組態對於內部實務、業界準則和法規的合規狀態。
- AWS Security Hub – 此 AWS 服務 可供您檢視 AWS 中的安全狀態，可助您檢查是否符合安全產業標準和最佳實務。
- AWS Audit Manager – 此 AWS 服務 可協助您持續稽核 AWS 使用情況，以簡化管理風險與法規與業界標準的法規遵循方式。

中的恢復能力AWS帳戶管理

所以此AWS全球基礎設施是以AWS 區域與可用區域。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、容錯能力和擴充能力，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 與可用區域的詳細資訊，請參閱AWS全球基礎架構。

AWS Account Management 中的基礎設施安全

作為託管服AWS務，運行在您的服務AWS 帳戶受到AWS全球網絡安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 AWS 雲端安全。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的基礎設施保護。

您可以使用AWS已發佈的 API 呼叫透過網路存取帳戶設定。用戶端必須支援下列項目：

- 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，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

監控AWS帳戶管理

監控是維持AWS帳戶管理和其他AWS解決方案的可靠性，可用性和性能的重要組成部分。 AWS提供以下監控工具來監視帳戶管理，報告出現錯誤，並在適當時自動採取措施：

- AWS CloudTrail擷取 (記錄) 由您或代表您發出的 API 呼叫和相關事件，AWS 帳戶並將日誌檔寫入您指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。這可讓您識別呼叫的使用者和帳戶AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。
- Amazon EventBridge 透過自動回應系統事件 (例如應用程式可用性問題或資源變更)，為您的AWS服務增加額外的自動化功能。來自AWS服務的事件會以近乎即時 EventBridge 的方式傳送到。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。

日誌AWS使用賬户管理 API 呼叫AWS CloudTrail

所以此AWS賬户管理 API 與AWS CloudTrail，該服務可提供由使用者、角色或AWS服務，調用賬户管理操作。CloudTrail 會將所有帳户管理 API 呼叫當作事件。捕獲的呼叫包括對賬户管理操作的所有調用。如果您建立追蹤，就可以將 CloudTrail 事件持續交付至 Amazon S3 儲存儲體，包括 Account Management 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 Event history (事件歷史記錄) 檢視最新事件。您可以使用由 CloudTrail 收集的資訊來判斷稱為帳户管理操作的請求、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 中的帳户管理資訊

CloudTrail 已在您的AWS 帳戶當您建立帳户時，系統會發出。此外，帳户管理操作發生活動時，CloudTrail 便會將該活動記錄至 CloudTrail 事件，並將其他AWS中的服務事件事件歷史記錄。您可以檢視、搜尋和下載 AWS 帳戶 的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

若要持續記錄至AWS 帳戶（包括帳户管理操作的事件），請建立線索。追蹤能讓 CloudTrail 將日誌檔交付至 Amazon S3 儲存貯體。默認情況下，當您建立線索時，系統會在AWS Management Console，則跟蹤應用於所有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。您可設定其他 AWS 服務，以進一步分析和處理 CloudTrail 記錄中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 從多個區域接收 CloudTrail 日誌檔案
- 從多個帳戶接收 CloudTrail 記錄檔案

AWS CloudTrail記錄所有賬户管理 API 操作，請參閱API 參考章節。例如，呼叫至`CreateAccount`、`DeleteAlternateContact`，以及`PutAlternateContact`操作會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或日誌項目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：

- 該請求是否使用根或AWS Identity and Access Management(IAM) 用户證書
- 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
- 該請求是否由另一項 AWS 服務提出

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

瞭解賬户管理日誌條目

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 日誌檔包含一或多個日誌項目。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：下列範例顯示了對`GetAlternateContact`操作來檢索當前`OPERATIONS`帳户的備用聯繫人。操作返回的值不包括在記錄的信息中。

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：下列範例顯示了對PutAlternateContact操作來添加新的BILLING替代聯繫人到一個帳戶。

```
{
  "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：下列範例顯示了對DeleteAlternateContact操作來刪除當前OPERATIONS備用聯絡。

```
{
  "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"
}
```

監控帳戶管理事件 EventBridge

Amazon EventBridge (以前稱為 E CloudWatch vents) 可協助您監控特定事件，並啟動使用其他目標動作的事件AWS 服務。來自的事件AWS 服務會以近乎即時 EventBridge 的方式傳送至。

您可以使用建立符合傳入事件的規則 EventBridge，並將其路由到目標進行處理。

如需詳細資訊，請參閱 Amazon EventBridge 使用者指南 EventBridge中的開始使用 Amazon。

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。

帳戶管理目前只能透過啟用和停用區域和 API CloudTrail 呼叫特定的事件。

Event types (事件類型)

- 啟用和停用區域的事件

啟用和停用區域的事件

當您從主控台或 API 啟用或停用帳戶中的區域時，就會啟動非同步工作。初始請求將記錄為目標帳戶中的 CloudTrail 事件。此外，當啟用或停用程序已啟動時， EventBridge 事件會傳送至呼叫帳戶，並在任一程序完成後再次傳送至呼叫帳戶。

下列範例事件顯示要求的傳送方式，表示 `2020-09-30` [`ap-east-1`區域] 上已列入`ENABLED`考量`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 API 傳回的狀態：

- ENABLED— 該地區已成功啟用指accountId示
- ENABLING— 該地區正在為accountId指示的啟用
- DISABLED— 該地區已成功禁用指accountId示
- DISABLING— 該地區正在被禁用的過程中指accountId示

下列範例事件模式會建立擷取所有 Region 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 Region 事件的規則。

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

API 參考

帳戶管理中的 API 操作 (account) 命名空間可讓您修改您的AWS 帳戶。

每AWS 帳戶支援包含帳戶相關資訊的中繼資料，包括最多三個與該帳戶相關聯的備用聯絡人的資訊。這些是與相關聯的電子郵件地址之外的根使用者該帳戶的。您只能指定下列其中一種與帳戶相關聯的聯絡人類型。

- 帳單聯絡人
- 營運聯絡人
- 安全聯絡人

根據預設，本指南中討論的 API 作業會直接套用至呼叫作業的帳戶。該身份呼叫作業的帳戶通常是 IAM 角色或 IAM 使用者，且必須具有 IAM 政策套用的權限才能呼叫 API 作業。或者，您可以從中的身份調用這些 API 操作AWS Organizations管理帳戶並指定任何帳戶 ID 號碼AWS 帳戶是組織的成員。

API 版本

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

> **Note**
>
> 作為直接使用 API 的替代方法，您可以使用其中一個AWS軟體開發套件，其中包含各種程式設計語言和平台 (Java、Ruby、.NET、iOS、安卓系統等) 的程式庫和範例程式碼。SDK 提供了一種方便的方式來創建程序化訪問AWS組織。例如，SDK 會處理密碼編譯簽署要求、管理錯誤，以及自動重試要求。如需 AWS SDK 的其他資訊 (包括如何下載並安裝開發套件)，請參閱 Amazon Web Services 工具。

我們建議您使用AWSSDK 可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。若要深入瞭解帳戶管理查詢 API，請參閱提出 HTTP 查詢請求以呼叫 API在帳戶管理用戶指南中。組織支援所有動作的 GET 和 POST 要求。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，對於需要較大尺寸的操作，請使用 POST 請求。

簽署請求

當您將 HTTP 請求發送到AWS，您必須簽署請求，以便AWS可以識別誰發送給他們。您使用AWS存取金鑰，其中包含存取金鑰 ID 和秘密存取金鑰。強烈建議您不要為根帳戶建立存取金鑰。擁有 root 帳戶存取金鑰的任何人都可以不受限制地存取您帳戶中的所有資源。而是為具有管理權限的 IAM 使用者建立存取金鑰。作為另一種選擇，使用AWS安全令牌服務生成臨時安全憑據，並使用這些憑據來簽署請求。

若要簽署請求，建議您使用簽名版本 4。如果您有使用「簽名版本 2」的現有應用程式，則不需要更新它即可使用「簽名版本 4」。但是，某些操作現在需要簽名版本 4。需要版本 4 的操作文檔說明了這一要求。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指令行介面 (AWSCLI) 或其中一個AWS向其發出請求的 SDKAWS，這些工具會使用您在設定工具時指定的存取金鑰自動為您簽署要求。

帳戶管理的支持和反饋

我們誠摯歡迎您提供意見回饋。將您的評論發送到feedback-awsaccounts@amazon.com或發表您的反饋和問題帳戶管理支援討論區。如需 AWS 支援論壇的詳細資訊，請參閱論壇說明。

範例如何呈現

帳戶管理員回應您的要求時傳回的 JSON 會以單一長字串的形式傳回，不會有換行符號或格式化空格。本指南的範例中會顯示換行符號和空白，以提高可讀性。當示例輸入參數也會導致長字符串超出屏幕時，我們插入換行符以增強可讀性。您應該始終將輸入提交為單個 JSON 文本字符串。

錄製 API 要求

帳戶管理支援CloudTrail，記錄的服務AWS適用於您的 API 呼叫AWS 帳戶並將日誌檔交付到 Amazon S3 儲存貯體。通過使用收集的信息CloudTrail，您可以決定哪些要求已成功向帳戶管理提出、提出要求的人員、提出要求的時間等等。了解更多有關帳戶管理及其支持CloudTrail，請參閱日誌AWS使用賬户管理 API 呼叫AWS CloudTrail。若要深入瞭解CloudTrail，包括如何開啟和尋找您的記錄檔，請參閱AWS CloudTrail使用者指南。

動作

支援以下動作：

- AcceptPrimaryEmailUpdate
- DeleteAlternateContact
- DisableRegion

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

AcceptPrimaryEmailUpdate

接受來源要求，StartPrimaryEmailUpdate以更新指定帳號的主要電子郵件地址 (也稱為 root 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

指定您要透過此作業存取或修改的 12 位數帳號 ID 號碼。 AWS 帳戶 若要使用此參數，來電者必須是組織管理帳戶中的身分識別，或是委派的系統管理員帳戶。指定的帳號 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，並選擇性地指派委派管理員帳戶。

此作業只能從成員帳戶的管理帳戶或組織的委派系統管理員帳戶呼叫。

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

類型：String

模式：^\d{12}$

必要：是

Otp

發送到 StartPrimaryEmailUpdate API 調用PrimaryEmail指定的 OTP 代碼。

類型：String

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PrimaryEmail來自 StartPrimaryEmailUpdate API 呼叫的。

類型：字串

長度約束：最小長度為 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要求的狀態。

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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

ConflictException

由於資源的當前狀態發生衝突，因此無法處理請求。例如，如果您嘗試啟用目前已停用的 [區域] (狀態為 [停用])，或嘗試將帳戶的 root 使用者電子郵件變更為已在使用中的電子郵件地址，就會發生這種情況。

HTTP 狀態碼：409

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再次嘗試操作。

HTTP 狀態碼：500

ResourceNotFoundException

作業失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁，而且超出了節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteAlternateContact

從刪除指定的替代連絡人 AWS 帳戶。

如需如何使用替代連絡人作業的完整詳細資訊，請參閱存取或更新替代連絡人。

> **Note**
>
> 您必須先啟用「 AWS 帳戶管理」與「Organ AWS 帳戶 izations」之間的整合 AWS Organizations，才能更新由管理的替代聯絡人資訊。如需詳細資訊，請參閱啟用 AWS 帳戶管理的受信任存取權。

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

指定您要透過此作業存取或修改的 AWS 帳戶的 12 位數帳號 ID 號碼。

如果您未指定此參數，它會預設為用來呼叫作業之識別的 AWS 帳戶。

若要使用此參數，來電者必須是組織管理帳戶中的身分識別或委派的系統管理員帳戶，而且指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，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帳戶AccountId；它必須在獨立內容中呼叫作業，方法是不包含AccountId參數。

若要在非組織成員的帳戶上呼叫此作業，請勿指定此參數，並使用屬於您要擷取或修改其連絡人之帳戶的識別碼呼叫作業。

類型：String

模式：^\d{12}$

必要：否

AlternateContactType

指定要刪除的替代連絡人。

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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再試一次。

HTTP 狀態碼：500

ResourceNotFoundException

作業失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

範例

範例 1

下列範例會刪除其認證用於呼叫作業之帳戶的安全性替代連絡人。

請求範例

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

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

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。您必須使用組織的管理帳戶或帳戶管理服務委派管理員帳戶的認證。

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

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DisableRegion

停用（選擇退出）帳戶的特定區域。

> **Note**
>
> 停用某個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

指定您要透過此作業存取或修改的 12 位數帳號 ID 號碼。 AWS 帳戶 如果您未指定此參數，它會預設為用來呼叫作業之身分的 Amazon Web Services 帳戶。若要使用此參數，來電者必須是組織管理帳戶中的身分識別，或是委派的系統管理員帳戶。指定的帳號 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，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帳戶`AccountId`。它必須通過不包括`AccountId`參數在獨立上下文中調用操作。

若要在非組織成員的帳戶上呼叫此作業，請勿指定此參數。請改為使用屬於您要擷取或修改其聯絡人之帳戶的身分來呼叫作業。

類型：String

模式：`^\d{12}$`

必要：否

RegionName

指定給定區域名稱的區域代碼 (例如，`af-south-1`)。停用區域時，請 AWS 執行動作以停用帳戶中的該區域，例如銷毀該區域中的 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「地區」。

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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

ConflictException

由於資源的當前狀態發生衝突，因此無法處理請求。例如，如果您嘗試啟用目前已停用的 [區域] (狀態為 [停用])，或嘗試將帳戶的 root 使用者電子郵件變更為已在使用中的電子郵件地址，就會發生這種情況。

HTTP 狀態碼：409

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再次嘗試操作。

HTTP 狀態碼：500

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁，而且超出了節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的开发
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 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

指定您要透過此作業存取或修改的 12 位數帳號 ID 號碼。 AWS 帳戶 如果您未指定此參數，它會預設為用來呼叫作業之身分的 Amazon Web Services 帳戶。若要使用此參數，來電者必須是組織管理帳戶中的身分識別，或是委派的系統管理員帳戶。指定的帳號 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，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帳戶`AccountId`。它必須通過不包括`AccountId`參數在獨立上下文中調用操作。

若要在非組織成員的帳戶上呼叫此作業，請勿指定此參數。請改為使用屬於您要擷取或修改其聯絡人之帳戶的身分來呼叫作業。

類型：String

模式：^\d{12}$

必要：否

RegionName

指定給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。對於大多數帳戶來說，此過程需要幾分鐘的時間，但可能需要幾個小時。直到此過程完成之前，您都無法使用區域。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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

ConflictException

由於資源的當前狀態發生衝突，因此無法處理請求。例如，如果您嘗試啟用目前已停用的 [區域] (狀態為 [停用])，或嘗試將帳戶的 root 使用者電子郵件變更為已在使用中的電子郵件地址，就會發生這種情況。

HTTP 狀態碼：409

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再次嘗試操作。

HTTP 狀態碼：500

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁，而且超出了節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetAlternateContact

擷取附加至的指定替代接點 AWS 帳戶。

如需如何使用替代連絡人作業的完整詳細資訊，請參閱存取或更新替代連絡人。

> **Note**
>
> 您必須先啟用「 AWS 帳戶管理」與「Organ AWS 帳戶 izations」之間的整合 AWS Organizations，才能更新由管理的替代聯絡人資訊。如需詳細資訊，請參閱啟用 AWS 帳戶管理的受信任存取權。

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

指定您要透過此作業存取或修改的 AWS 帳戶的 12 位數帳號 ID 號碼。

如果您未指定此參數，它會預設為用來呼叫作業之識別的 AWS 帳戶。

若要使用此參數，來電者必須是組織管理帳戶中的身分識別或委派的系統管理員帳戶，而且指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，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帳戶AccountId；它必須在獨立內容中呼叫作業，方法是不包含AccountId參數。

若要在非組織成員的帳戶上呼叫此作業，請勿指定此參數，並使用屬於您要擷取或修改其連絡人之帳戶的識別碼呼叫作業。

類型：String

模式：^\d{12}$

必要：否

AlternateContactType

指定您要擷取的替代連絡人。

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

包含指定替代連絡人之詳細資訊的結構。

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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再次嘗試操作。

HTTP 狀態碼：500

ResourceNotFoundException

作業失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁，而且超出了節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

範例

範例 1

下列範例會擷取其認證用於呼叫作業之帳戶的安全性替代連絡人。

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作業替代連絡人。您必須使用組織的管理帳戶或帳戶管理服務委派管理員帳戶的認證。

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

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetContactInformation

擷取的主要連絡人資訊 AWS 帳戶。

如需如何使用主要聯絡人作業的完整詳細資訊，請參閱更新主要與替代聯絡人資訊。

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

指定您要透過此作業存取或修改的 12 位數帳號 ID 號碼。 AWS 帳戶 如果您未指定此參數，它會預設為用來呼叫作業之身分的 Amazon Web Services 帳戶。若要使用此參數，來電者必須是組織管理帳戶中的身分識別，或是委派的系統管理員帳戶。指定的帳號 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，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帳戶AccountId。它必須通過不包括AccountId參數在獨立上下文中調用操作。

若要在非組織成員的帳戶上呼叫此作業，請勿指定此參數。請改為使用屬於您要擷取或修改其聯絡人之帳戶的身分來呼叫作業。

類型：String

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人資訊的詳細資料 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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再次嘗試操作。

HTTP 狀態碼：500

ResourceNotFoundException

作業失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁，而且超出了節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK

- AWS 適用於紅寶石 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

指定您要透過此作業存取或修改的 12 位數帳號 ID 號碼。 AWS 帳戶 若要使用此參數，來電者必須是組織管理帳戶中的身分識別或委派的系統管理員帳戶。指定的帳號 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，並選擇性地指派委派管理員帳戶。

此作業只能從成員帳戶的管理帳戶或組織的委派系統管理員帳戶呼叫。

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

類型：String

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

長度約束：最小長度為 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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再試一次。

HTTP 狀態碼：500

ResourceNotFoundException

作業失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetRegionOptStatus

檢索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

指定您要透過此作業存取或修改的 12 位數帳號 ID 號碼。 AWS 帳戶 如果您未指定此參數，它會預設為用來呼叫作業之身分的 Amazon Web Services 帳戶。若要使用此參數，來電者必須是組織管理帳戶中的身分識別，或是委派的系統管理員帳戶。指定的帳號 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，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帳戶`AccountId`。它必須通過不包括`AccountId`參數在獨立上下文中調用操作。

若要在非組織成員的帳戶上呼叫此作業，請勿指定此參數。請改為使用屬於您要擷取或修改其聯絡人之帳戶的身分來呼叫作業。

類型：String

模式：^\d{12}$

必要：否

RegionName

指定給定區域名稱的區域代碼 (例如，af-south-1)。該函數將返回您傳遞給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

傳入的區域代碼。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

RegionOptStatus

區域可以經歷的潛在狀態之一（啟用，啟用，禁用，禁用，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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再次嘗試操作。

HTTP 狀態碼：500

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁，而且超出了節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的开发
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP

- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListRegions

列出指定帳戶的所有區域及其各自的選擇加入狀態。或者，您可以使用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

指定您要透過此作業存取或修改的 12 位數帳號 ID 號碼。 AWS 帳戶 如果您未指定此參數，它會預設為用來呼叫作業之身分的 Amazon Web Services 帳戶。若要使用此參數，來電者必須是組織管理帳戶中的身分識別或委派的系統管理員帳戶。指定的帳號 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，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帳戶AccountId。它必須通過不包括AccountId參數在獨立上下文中調用操作。

若要在非組織成員的帳戶上呼叫此作業，請勿指定此參數。請改為使用屬於您要擷取或修改其聯絡人之帳戶的身分來呼叫作業。

類型：String

模式：^\d{12}$

必要：否

MaxResults

要在命令輸出中傳回的項目總數。如果可用的項目總數大於指定的值，則會NextToken在命令的輸出中提供 a。若要繼續分頁，請在後續命令的 starting-token 引數中提供 NextToken 值。請勿直接在 AWS CLI 之外使用NextToken回應元素。如需使用範例，請參閱《指 AWS 令行介面使用指南》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

用來指定從何處開始分頁的權杖。這是先前截斷的NextToken回應。如需使用範例，請參閱《指 AWS 令行介面使用指南》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」、「已啟用」、「停用」、「已停用」、「已啟用 _BY_DEFAULT」)，用於篩選指定帳戶的區域清單。例如，傳入 ENABLED 的值只會傳回「地區」狀態為「啟用」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

如果有更多的數據要返回，這將被填充。它應該被傳遞到的next-token請求參數list-regions。

類型：字串

Regions

這是指定帳戶的「區域」清單，或者如果使用篩選的參數，則會列出符合filter參數中設定之篩選準則的「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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再次嘗試操作。

HTTP 狀態碼：500

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁且超過節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的开发
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

PutAlternateContact

修改貼附至的指定替代接點 AWS 帳戶。

如需如何使用替代連絡人作業的完整詳細資訊，請參閱存取或更新替代連絡人。

> **Note**
>
> 您必須先啟用「 AWS 帳戶管理」與「Organ AWS 帳戶 izations」之間的整合 AWS Organizations，才能更新由管理的替代聯絡人資訊。如需詳細資訊，請參閱啟用 AWS 帳戶管理的受信任存取權。

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

指定您要透過此作業存取或修改的 AWS 帳戶的 12 位數帳號 ID 號碼。

如果您未指定此參數，它會預設為用來呼叫作業之識別的 AWS 帳戶。

若要使用此參數，來電者必須是組織管理帳戶中的身分識別或委派的系統管理員帳戶，而且指定的帳戶 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，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帳戶`AccountId`；它必須在獨立內容中呼叫作業，方法是不包含`AccountId`參數。

若要在非組織成員的帳戶上呼叫此作業，請勿指定此參數，並使用屬於您要擷取或修改其連絡人之帳戶的識別碼呼叫作業。

類型：String

模式：`^\d{12}$`

必要：否

AlternateContactType

指定您要建立或更新的替代連絡人。

類型：字串

有效值:`BILLING | OPERATIONS | SECURITY`

必要：是

EmailAddress

指定替代連絡人的電子郵件地址。

類型：字串

長度限制：長度下限為 1。最大長度為 254。

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

必要：是

Name

指定替代連絡人的名稱。

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。最大長度為 25。

模式：^[\s0-9()+-]+$

必要：是

Title

指定替代連絡人的標題。

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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再次嘗試操作。

HTTP 狀態碼：500

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁，而且超出了節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

範例

範例 1

下列範例會針對其認證用於呼叫作業的帳戶，設定帳單替代聯絡人。

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。您必須使用組織的管理帳戶或帳戶管理服務委派管理員帳戶的認證。

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

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

PutContactInformation

更新的主要聯絡人資訊 AWS 帳戶。

如需如何使用主要聯絡人作業的完整詳細資訊，請參閱更新主要與替代聯絡人資訊。

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

指定您要透過此作業存取或修改的 12 位數帳號 ID 號碼。 AWS 帳戶 如果您未指定此參數，它會預設為用來呼叫作業之身分的 Amazon Web Services 帳戶。若要使用此參數，來電者必須是組織管理帳戶中的身分識別，或是委派的系統管理員帳戶。指定的帳號 ID 必須是相同組織中的成員帳

戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，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帳戶AccountId。它必須通過不包括AccountId參數在獨立上下文中調用操作。

若要在非組織成員的帳戶上呼叫此作業，請勿指定此參數。請改為使用屬於您要擷取或修改其聯絡人之帳戶的身分來呼叫作業。

類型：String

模式：^\d{12}$

必要：否

ContactInformation

包含與相關聯的主要聯絡人資訊的詳細資料 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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再次嘗試操作。

HTTP 狀態碼：500

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁，而且超出了節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

StartPrimaryEmailUpdate

啟動更新指定帳戶的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

指定您要透過此作業存取或修改的 12 位數帳號 ID 號碼。 AWS 帳戶 若要使用此參數，來電者必須是組織管理帳戶中的身分識別，或是委派的系統管理員帳戶。指定的帳號 ID 必須是相同組織中的成員帳戶。組織必須啟用所有功能，且組織必須啟用帳戶管理服務的受信任存取權，並選擇性地指派委派管理員帳戶。

此作業只能從成員帳戶的管理帳戶或組織的委派系統管理員帳戶呼叫。

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

類型：String

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 root 使用者電子郵件地址)。

類型：字串

長度約束：最小長度為 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

主要電子郵件更新要求的狀態。

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

作業失敗，因為呼叫識別沒有必要的最低權限。

HTTP 狀態碼：403

ConflictException

由於資源的當前狀態發生衝突，因此無法處理請求。例如，如果您嘗試啟用目前已停用的 [區域] (狀態為 [停用])，或嘗試將帳戶的 root 使用者電子郵件變更為已在使用中的電子郵件地址，就會發生這種情況。

HTTP 狀態碼：409

InternalServerException

作業失敗，因為內部的錯誤 AWS。請稍後再次嘗試操作。

HTTP 狀態碼：500

ResourceNotFoundException

作業失敗，因為它指定了找不到的資源。

HTTP 狀態碼：404

TooManyRequestsException

作業失敗，因為呼叫頻率太頻繁，而且超出了節流限制。

HTTP 狀態碼：429

ValidationException

作業失敗，因為其中一個輸入參數無效。

HTTP 狀態碼：400

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS 適用於轉到 V2 的 SDK
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK

- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

其他中的相關操作AWS服務

下列操作與有關AWS Account Management，但屬於AWS Organizations命名空間：

- CreateAccount
- 創建政府雲賬户
- DescribeAccount

CreateAccount

所以此`CreateAccount`API 操作僅可用於由AWS Organizations服務。API 操作在該服務的命名空間中定義。

如需詳細資訊，請參閱「」CreateAccount中的AWS OrganizationsAPI 參考。

創建政府雲賬户

所以此`CreateGovCloudAccount`API 操作僅可用於由AWS Organizations服務。API 操作在該服務的命名空間中定義。

如需詳細資訊，請參閱「」創建政府雲賬户中的AWS OrganizationsAPI 參考。

DescribeAccount

所以此`DescribeAccount`API 操作僅可用於由AWS Organizations服務。API 操作在該服務的命名空間中定義。

如需詳細資訊，請參閱「」DescribeAccount中的AWS OrganizationsAPI 參考。

資料類型

目前支援下列資料類型：

- AlternateContact

- ContactInformation
- Region
- ValidationExceptionField

AlternateContact

包含與 AWS 帳戶相關聯之替代聯絡人詳細資訊的結構

目錄

AlternateContactType

替代接觸的類型。

類型：字串

有效值:BILLING | OPERATIONS | SECURITY

必要：否

EmailAddress

與此替代連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。最大長度為 254。

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

必要：否

Name

與此替代連絡人相關聯的名稱。

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。最大長度為 25。

模式：^[\s0-9()+-]+$

必要：否

Title

與此替代連絡人相關聯的標題。

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

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

ContactInformation

包含與相關聯的主要聯絡人資訊的詳細資料 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。最大長度為 60。

必要：是

City

主要聯絡人地址的城市。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

必要：是

CountryCode

主要聯絡人地址的 ISO-3166 兩個字母的國家/地區代碼。

類型：字串

長度約束：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

主要聯絡人資訊的電話號碼。該號碼將被驗證，並在某些國家/地區檢查是否激活。

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

主要聯絡人地址的郵遞區號。

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。最大長度為 60。

必要：否

AddressLine3

主要聯絡人地址的第三行 (如果有的話)。

類型：字串

長度限制：長度下限為 1。最大長度為 60。

必要：否

CompanyName

與主要聯絡人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

主要聯絡人地址的地區或縣 (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

主要聯絡人地址的州或地區。如果郵寄地址位於美國 (US) 境內，則此欄位中的值可以是兩個字元的州碼 (例如，NJ) 或完整的州名 (例如，New Jersey)。此欄位在下列國家/地區為必填欄位：USCAGBDE、JP、IN、、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

與主要聯絡人資訊相關聯的網站 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

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的開發
- AWS 適用於紅寶石 V3 的 SDK

Region

這是表示給定帳戶的「區域」的結構，包含名稱和選擇加入狀態。

目錄

RegionName

給定區域的區域代碼（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 (已啟用、啟用、停用、停用、已啟用 _By_Default)。

類型：字串

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

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的开发
- AWS 適用於紅寶石 V3 的 SDK

ValidationExceptionField

輸入無法符合指定欄位中 AWS 服務所指定的條件約束。

目錄

message

關於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

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Java V2 的开发
- AWS 適用於紅寶石 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。如需簽名版本 4 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已簽署的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 AWSAPI 請求簽名元素。

類型：字串

必要：有條件

X-Amz-Security-Token

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

條件：如果您使用安全憑證AWS STS，則必須納入安全字符。

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。如需有關指定已簽署標頭的詳細資訊，請參閱 IAM 使用者指南中的建立已簽署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

本部分列出所有 AWS 服務 API 動作的常見錯誤。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

請求簽署不符合 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

輸入不符合 AWS 服務規定的限制。

HTTP 狀態碼：400

提出 HTTP 查詢請求以呼叫 API

本節包含以下項目使用查詢 API 的一般資訊AWS帳戶管理。如需 API 操作和錯誤的詳細資訊，請參閱 API 參考。

> **Note**
>
> 而不是直接呼叫AWS帳戶管理查詢 API，您可以使用其中一個AWS軟體開發套件。AWS 開發套件以程式庫以及適用於多種程式設計語言及平台 (Java、Ruby、.NET、iOS、Android 等) 的範本程式碼所組成。SDK 提供了一種方便的方式來創建程序化訪問AWS帳戶管理及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 開發套件的其他資訊 (包括如何下載並安裝開發套件)，請參閱 Amazon Web Services 工具。

使用下列項目的查詢 APIAWS帳戶管理，您可以調用服務操作。查詢 API 請求是 HTTPS 請求，其中必須包含`Action`參數，以指示要執行的操作。AWS帳戶管理支援`GET`和`POST`對所有操作的請求。也就是說，API 不需要您使用`GET`對於一些行動和`POST`對於其他人。然而，`GET`請求受 URL 的限制大小限制。雖然此限制取決於瀏覽器，但典型的限制是 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 要求

端點

AWS帳戶管理具有託管於美國東部 (維吉尼亞北部) 的單一全域 API 端點AWS 區域。

如需更多相關資訊AWS所有服務的端點和區域，請參閱區域和端點在AWS 一般參考。

必要的 HTTPS

由於查詢 API 可以傳回機密資訊 (例如安全性認證)，因此您必須使用 HTTPS 來加密所有 API 要求。

簽署AWS帳戶管理 API 要求

請求必須使用存取金鑰 ID 和私密存取金鑰簽署。我們強烈建議您不要使用AWS用於日常工作的 root 帳戶憑據AWS帳戶管理。您可以將憑據用於AWS Identity and Access Management(IAM) 使用者或臨時登入資料，例如搭配 IAM 角色使用。

若要簽署 API 請求，您必須使用 AWS 簽章第 4 版。如需有關使用 Signature 第 4 版的資訊，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 中的安全最佳做法— 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。
- 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 Account Management

您的每項 AWS 服務都 AWS 帳戶 有預設配額 (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。

每個人都 AWS 帳戶 有以下與帳戶管理相關的配額。

資源	配額
每個目標帳戶的StartPrimaryEmailUpdate 要求數目上限	每 30 秒 3 次
在一個替代聯繫人的數量 AWS 帳戶	3-每個一個 BILLINGSECURITY，和 OPERATIONS
每個帳戶的並行區域選擇要求數	6
每個組織的並行區域選擇要求數目	20
每個來電者帳戶的AcceptPrimaryEmailUpdate 請求率	每秒 1 次，突發至每秒 1 次
每個帳戶的DeleteAlternateContact 請求率	每秒 1 次，突發至每秒 6 次
每個帳戶的DisableRegion 請求率	每秒 1 次，突發至每秒 1 次
每個帳戶的EnableRegion 請求率	每秒 1 次，突發至每秒 1 次
每個帳戶的GetAlternateContact 請求率	每秒 10 次，突發至每秒 15 次
每個帳戶的GetContactInformation 請求率	每秒 10 次，突發至每秒 15 次
每個來電者帳戶的GetPrimaryEmail 請求率	每秒 3 次，突發至每秒 3 次
每個帳戶的GetRegionOptStatus 請求率	每秒 5 次，突發至每秒 5 次
每個帳戶的ListRegions 請求率	每秒 5 次，突發至每秒 5 次

資源	配額
每個帳戶的PutAlternateContact 請求率	每秒 5 次，突發至每秒 8 次
每個帳戶的PutContactInformation 請求率	每秒 5 次，突發至每秒 8 次
每個來電者帳戶的StartPrimaryEmailUpdate 請求率	每秒 1 次，突發至每秒 1 次

疑難排解 AWS 帳戶

使用下列主題中的資訊來協助您診斷和修正AWS 帳戶. 如需 root 使用者的說明，請參閱《IAM 使用者指南》中的針對 root 使用者的疑難排解問題。如需登入程序的說明，請參閱AWS 帳戶登入使用手冊中的疑難排解AWS登入問題。

故障診斷主題

- 疑難排解 AWS 帳戶 建立問題
- AWS 帳戶 關閉問題疑難排解
- 其他問題的故障診斷AWS 帳戶

疑難排解 AWS 帳戶 建立問題

使用下表中的參考連結來協助您診斷並修正建立新的問題 AWS 帳戶。

問題	參考連結	來源
我不知道如何註冊或創建帳戶	創建一個獨立的 AWS 帳戶	本指南
如果我沒有收到來電 AWS 以驗證我的新帳戶，或者輸入的 PIN 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 通過電話驗證時，如何解決「嘗試失敗的次數上限」錯誤？	https://repost.aws/knowledge-center/ maximum-failed-attempts	AWS re:Post
已經超過 24 小時，我的帳戶尚未激活	https://repost.aws/knowledge-center/ 帳create-and-activate-aws戶	AWS re:Post
建立新帳戶後，我無法登入	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，我們建議您搜AWS re:Post尋與特定問題相關的內容。如果您仍需要協助，請聯絡AWS Support。

AWS 帳戶 關閉問題疑難排解

使用以下資訊協助您診斷和修正帳戶關閉程序期間發現的常見問題。如需關閉帳戶程序的一般資訊，請參閱關閉 AWS 帳戶。

主題

我不知道如何刪除或取消帳戶

要關閉您的帳戶，請按照中的說明進行操作關閉 AWS 帳戶。

我在「帳戶」頁面上看不到「關閉帳戶」按鈕

如果您未以 root 使用者身分登入，則不會在 [帳戶] 頁面上看到 [關閉帳戶] 按鈕。您必須以 root 使用者身分登入，才能關閉您的帳戶。 AWS Management Console 如果您無法登入，請參閱疑難排解 root 使用者的問題。

我關閉了帳戶，但仍未收到確認電子郵件

此確認電子郵件只會傳送至的 root 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，則可以以 root 用戶 AWS Management Console 身份登錄以檢查您的帳戶是否已關閉。如果您的帳戶已成功關閉，您將看到一條消息，指示您的帳戶已關閉。如果您關閉的帳戶是會員帳戶，則可以通過檢查關閉的帳戶是否在 AWS Organizations 控制台SUSPENDED中標記為來驗證是否已關閉。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，但沒有收到關於帳戶關閉的電子郵件確認，則您的組織很可能擁有有效的成員帳戶。如果您的組織沒有任何作用中的成員帳戶，您才能關閉管理帳戶。若要確認您的組織中沒有

任何作用中的成員帳戶，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。之後，您可以關閉管理帳戶。

我在嘗試關閉帳戶時收到 ConstraintViolationException「」錯誤訊息

您嘗試使用 AWS Organizations 控制台關閉管理帳戶，這是不可能的。若要關閉管理帳戶，您必須以管理帳戶的 root 使用者身分登入，然後從 [帳戶] 頁面關閉該帳戶。 AWS Management Console 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「關閉帳戶」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。最低帳戶關閉為 10，即使帳戶的 10% 超過 1000，最大帳戶關閉也是 1000。如需有關 Organizations 配額的詳細資訊，請參閱AWS Organizations 使用指南 AWS Organizations中的配額。

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 AWS 組織。不過，如果您的組織沒有任何作用中的成員帳戶，您才能關閉管理帳戶。若要確認您的組織中沒有任何作用中的成員帳戶，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。之後，您可以關閉管理帳戶。

其他問題的故障診斷AWS 帳戶

使用此處的資訊來協助您針對與AWS 帳戶。

問題

- 我需要變更我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AWS 帳戶

如要變更您AWS 帳戶，您必須要能夠登入。AWS具備保護措施，會請求您證明您是帳號的擁有者。如需說明，請參閱「」管理您的信用卡付款方式中的AWS Billing使用者指南。

我需要報告詐騙AWS 帳戶活動

如果您懷疑使用AWS 帳戶並想要做一份報告，請參閱如何報告濫用AWS資源。

如果您在 Amazon.com 上進行購買時遇到問題，請參亞馬遜客服。

我需要關閉我的AWS 帳戶

有關關閉AWS 帳戶，請參關閉 AWS 帳戶。

帳戶管理用戶指南的文檔歷史記錄

下表說明「 AWS 帳戶管理」的文件版本。

變更	描述	日期
新的主要電子郵件 API	Support 新的GetPrimaryEmail 、和 AcceptPrimaryEmailUpdate APIStartPrimaryEmailUpdate ，以集中更新中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《使用指南》中的更新成員帳戶的 root AWS Organizations 使用者電子郵件地址。	2024年6月6日
重寫關閉帳戶主題	徹底改變了整個關閉帳戶主題，包括新增關閉成員和管理帳戶的步驟。	2024年2月1日
終止新增安全性挑戰問題的支援	已新增新內容，指出新增挑戰問題的選項已從「帳號」頁面移除。	2024年1月5日
對aws-portal 命名空間的支持結束	AWS Identity and Access Management (IAM) 先前用來管理您帳戶的動作 (例如，aws-portal:ModifyAccount 和aws-portal:ViewAccount) 已經到達標準支援的結束。	2024年1月1日
重寫「區域」主題	徹底更新了整個「區域」主題，包括新增展開和收合控制項。	2023年10月8日

將根使用者主題重新定位至 IAM 使用者指南	將有關 root 使用者的討論整合為一個主題，並新增移至 IAM 使用者指南的根使用者主題的交叉參考連結。	2023 年 9 月 18 日
新增至主要帳戶連絡人主題的新區段	添加了新的電話號碼和電子郵件地址要求部分。	2023 年 9 月 12 日
新的聯絡人資訊 API	Support 新的`GetContactInformation` 和 `PutContactInformation` API。	2022 年 7 月 22 日
AWS 帳號管理現在支援透過 AWS Organizations 主控台更新其他聯絡人。	您現在可以使用由更新的 AWS Organizations 受管理政策提供的帳戶 API 權限，透過 AWS Organizations 主控台更新組織的備用聯絡人。	2022 年 2 月 8 日
初始版本	《AWS 帳戶管理參考指南》的初次發行	2021 年 9 月 30 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

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。