aws

使用者指南

AWS设置

AWS设置: 使用者指南

Table of Contents

概要

本指南提供了創建新的說明AWS 帳戶並設置您的第一個管理用戶AWS IAM Identity Center遵循最新的安全性最佳做法。

一個AWS 帳戶需要訪問AWS 服務並作為兩個基本功能：

- 容器— 一個AWS 帳戶是所有的容器AWS您可以建立的資源AWS客戶。當您建立 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體或 Amazon 關聯式資料庫服務 (Amazon RDS) 資料庫來存放資料時，或建立 Amazon 彈性運算雲端 (Amazon EC2) 執行個體來處理您的資料時，您正在建立一個資源在您的帳戶中。每個資源均由 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— 一個AWS 帳戶是您的基本安全界限AWS資源。您在帳戶中建立的資源僅供具有相同帳戶認證的使用者使用。

  您可以在帳戶中創建的關鍵資源包括身份，例如 IAM 使用者和角色，以及聯合身分，例如來自您企業使用者目錄的使用者、Web 身分識別提供者、IAM Identity Center 目錄或任何其他存取的使用者AWS 服務使用透過身分識別來源提供的認證。這些身分具有某人可用來登入的認證，或認證至AWS。身分識別也具有權限原則，可指定登入的人員獲授權處理帳戶中的資源。

術語

Amazon Web Services (AWS) 使用常用術語來描述登錄過程。我們建議您閱讀並理解這些條款。

管理員

也稱為AWS 帳戶管理員或 IAM 管理員。管理員 (通常是資訊技術 (IT) 人員，是負責監督. AWS 帳戶管理員對其組織的其他成員擁有更高層級的權限。AWS 帳戶系統管理員會建立並實作的設定AWS 帳戶。他們也會建立 IAM 或 IAM 身分中心使用者。系統管理員會為這些使用者提供他們的存取認證和登入 URL 來登入AWS。

帳戶

標準AWS 帳戶包含您的AWS資源和可存取這些資源的身分識別。帳戶與帳戶擁有者的電子郵件地址和密碼相關聯。

憑證

也稱為存取認證或安全認證。認證是使用者提供AWS給登入和取得資源存取權的AWS資訊。認證可以包括電子郵件地址、使用者名稱、使用者定義的密碼、帳戶 ID 或別名、驗證碼，以及單一使用多重要素驗證 (MFA) 程式碼。進行身分驗證和授權時，系統會使用登入資料來識別呼叫發起人，以及是否允許請求的存取。在中AWS，這些認證通常是存取金鑰 ID 和秘密存取金鑰。

如需認證的詳細資訊，請參閱瞭解並取得AWS認證。

> **Note**
>
> 使用者必須提交的認證類型取決於他們的使用者類型。

企業憑證

使用者在存取其公司網路和資源時提供的認證。您的公司管理員可AWS 帳戶以將您設定為使用與存取公司網路和資源相同的認證來存取。這些認證是由您的管理員或服務台員工提供給您。

設定檔

當您註冊AWS產生器 ID 時，您會建立設定檔。您的設定檔包括您提供的聯絡資訊，以及管理多重要素驗證 (MFA) 裝置和作用中工作階段的能力。您還可以在您的個人資料中進一步了解隱私以及我們如何處理您的數據。如需有關您的設定檔及其與設定檔如何關聯的詳細資訊AWS 帳戶，請參閱AWSBuilder ID 和其他AWS認證。

使用者

使用者是帳戶下的個人或應用程式，可對AWS產品進行 API 呼叫。每個使用者在中都有一個唯一的名稱，以AWS 帳戶及一組不與他人共用的安全認證。這些認證與. 的安全登入資料不同AWS 帳戶。每個用戶都與一個只有一個關聯AWS 帳戶。

根使用者憑證

根使用者身份證明與用於以 root 使用者身分登入AWS Management Console的認證相同。如需 root 使用者的詳細資訊，請參閱根使用者。

驗證碼

在登入過程中，驗證碼會使用多重要素驗證 (MFA) 來驗證您的身分。驗證碼的交付方式各不相同。他們可以通過短信或電子郵件發送。如需詳細資訊，請洽詢您的管理員。

AWS使用者和認證

與之互動時AWS，您可以指定AWS安全登入資料以驗證您的身分，以及您是否有權存取要求的資源。AWS使用安全認證來驗證和授權請求。

例如，如果要從 Amazon Simple Storage Service (Amazon S3) 儲存貯體下載受保護的檔案，您的憑證必須允許此存取動作。如果您的認證顯示您沒有下載檔案的授權，請AWS拒絕您的要求。不過，在公開共用的 Amazon S3 儲存貯體中下載檔案時，不需要安全登入資料。

根使用者

也稱為帳戶擁有者或帳號根使用者。身為 root 使用者，您可以AWS完整存取AWS 帳戶. 如果是首次建立 AWS 帳戶，您會先有單一的登入身分，可以完整存取帳戶中所有 AWS 服務與資源。此身份是AWS帳號根使用者。您可以使用您用來AWS Management Console建立帳戶的電子郵件地址和密碼，以 root 使用者身分登入。如需有關如何登入的逐步指示，請參閱以 root 使用者身分登入。AWS Management Console

> **Important**
>
> 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。

如需 IAM 身分 (包括根使用者) 的詳細資訊，請參閱 IAM 身分 (使用者、使用者群組和角色)。

IAM 身分中心使用者

IAM 身分中心使用者透過AWS存取入口網站登入。AWS存取入口網站或特定登入 URL 是由您的系統管理員或服務台員工所提供。如果您為您建立了 IAM 身分中心使用者AWS 帳戶，則會將加入 IAM 身分中心使用者的邀請傳送到的電子郵件地址AWS 帳戶。電子郵件邀請中包含特定的登入 URL。IAM 身分中心使用者無法透過AWS Management Console. 如需如何登入的逐步指示，請參閱登入AWS存取入口網站。

> **Note**
>
> 建議您將AWS存取入口網站的特定登入 URL 加入書籤，以便稍後可以快速存取。

如需 IAM 身分中心的詳細資訊，請參閱什麼是 IAM 身分中心？

聯合身分

聯合身份是可以使用知名的外部身份提供商（IdP）登錄的用戶，例如使用亞馬遜，Facebook，谷歌或任何其他 OpenID Connect（OIDC）兼容的 IdP 登錄。使用 Web 身份聯合，您可以接收身份驗證令牌，然後將該令牌交換為AWS該映射中的臨時安全登入資料，以使用AWS 帳戶. 您不要使用AWS Management Console或AWS存取入口網站登入。相反地，使用中的外部身分會決定您登入的方式。

如需詳細資訊，請參閱以同盟身分登入。

IAM 使用者

IAM 使用者是您在中建立的實體AWS。此使用者是授與特定自訂權限的AWS 帳戶身分。您的 IAM 使用者登入資料包含用於登入的名稱和密碼AWS Management Console。如需如何登入的逐步指示，請參閱以 IAM 使用者身分登入。AWS Management Console

如需 IAM 身分 (包括 IAM 使用者) 的詳細資訊，請參閱 IAM 身分 (使用者、使用者群組和角色)。

AWS生成器 ID 用戶

身為 AWS Builder ID 使用者，您會特別登入您要存取的AWS服務或工具。AWS生成器 ID 用戶可以補充AWS 帳戶您已經擁有或想要創建的任何內容。AWS生成器 ID 代表您作為一個人，您可以使用它來訪問AWS服務和工具，而無需AWS 帳戶. 您還擁有一個配置文件，您可以在其中查看和更新您的信息。如需詳細資訊，請參閱使用AWS產生器 ID 登入。

先決條件和考量

在開始設定程序之前，請先檢閱帳戶需求，並考慮您是否需要多個帳戶需求AWS 帳戶，並瞭解在 IAM 身分中心設定帳戶以進行管理存取的要求。

AWS 帳戶 要求

若要註冊成為AWS 帳戶，您需要提供以下信息：

- 帳戶名稱— 帳戶名稱出現在多個地方，例如在您的發票上，以及在諸如「計費和成本管理」儀表板和控制台中AWS Organizations控制台。

  我們建議您使用帳戶命名標準，以便可以輕鬆識別帳戶名稱並與您可能擁有的其他帳戶進行區分。如果是公司帳戶，請考慮使用命名標準，例如組織-目的-環境（例如，AnyCompany-審計-刺). 如果是個人帳戶，請考慮使用命名標準，例如名字-姓氏-目的（例如，paulo-santos-testaccount).
- 電子郵件地址— 此電子郵件地址用作帳戶 root 用戶的登錄名，並且是帳戶恢復所必需的，例如忘記密碼。您必須能夠接收傳送至此電子郵件地址的訊息。在執行特定工作之前，您必須確認您是否擁有電子郵件帳戶的存取權。

  > **Important**
  >
  > 如果此帳戶適用於企業，我們建議您使用公司通訊群組清單 (例如，`it.admins@example.com`). 避免使用個人的公司電子郵件地址（例如，`paulo.santos@example.com`). 這有助於確保您的公司可以訪問AWS 帳戶如果員工變更職位或離開公司。電子郵件地址可用於重設帳戶的 root 使用者認證。請務必保護對此通訊群組清單或位址的存取權。
- 一個電話號碼— 需要確認帳戶所有權時，可使用此號碼。您必須能夠透過此電話號碼接聽電話。

  > **Important**
  >
  > 如果此帳戶適用於公司，我們建議您使用公司電話號碼而不是個人電話號碼。這有助於確保您的公司可以訪問AWS 帳戶如果員工變更職位或離開公司。
- 多重驗證裝置— 為了保護您的AWS資源，在根使用者帳號上啟用多因素驗證 (MFA)。除了一般登入認證之外，啟用 MFA 時還需要次要驗證，以提供額外的安全性。如需 MFA 的更多資訊，請參閱什麼是 MFA？在IAM 使用者指南。

- AWS Support計劃— 在帳戶創建過程中，系統將要求您選擇其中一個可用計劃。如需可用計劃的說明，請參閱比較AWS Support計劃。

IAM 身分識別中心考量

下列主題提供針對特定環境設定 IAM 身分中心的指引。在繼續執行之前，請先瞭解適用於您環境的指引第 2 部分：在 IAM 身分中心建立管理使用者。

主題

- 作用中目錄或外部 IdP
- AWS Organizations
- IAM 角色
- 新世代防火牆和安全的 Web 閘道

作用中目錄或外部 IdP

如果您已經在 Active Directory 或外部 IdP 中管理使用者和群組，建議您在啟用 IAM 身分中心並選擇身分識別來源時考慮連線此身分識別來源。在預設 Identity Center 目錄中建立任何使用者和群組之前執行此動作，可協助您避免稍後變更身分識別來源時所需的其他組態。

如果您想要使用 Active Directory 做為身分識別來源，您的組態必須符合下列先決條件：

- 如果您正在使用AWS Managed Microsoft AD，您必須在同一個中啟用 IAM 身分中心AWS 區域你在哪裡AWS Managed Microsoft AD目錄已設置。IAM 身分識別中心會將指派資料儲存在與目錄相同的區域中。若要管理 IAM 身分中心，您可能需要切換至設定 IAM 身分中心的區域。另外，請注意AWS訪問門戶使用與您的目錄相同的訪問 URL。
- 使用存放在您的管理帳戶中的活動目錄：

  您必須擁有現有的 AD 連接器，或AWS Managed Microsoft AD目錄設定於AWS Directory Service，並且它必須駐留在您的AWS Organizations管理帳戶。您只能連接一個 AD 連接器或一個AWS Managed Microsoft AD在一個時間。如果您需要支援多個網域或樹系，請使用AWS Managed Microsoft AD。如需詳細資訊，請參閱：

  - 連接目錄AWS Managed Microsoft AD前往 IAM 身分識別中心在AWS IAM Identity Center使用者指南。
  - 將作用中目錄中的自我管理目錄連線至 IAM 身分識別中心在AWS IAM Identity Center使用者指南。

- 使用駐留在委託管理員帳戶中的活動目錄：

  如果您打算啟用 IAM 身分中心委派管理員，並使用 Active Directory 做為您的 IAM 身分識別來源，您可以使用現有的 AD 連接器或AWS Managed Microsoft AD目錄設定於AWS位於委派管理員帳戶中的目錄。

  如果您決定將 IAM 身分中心來源從任何其他來源變更為 Active Directory，或將其從 Active Directory 變更為任何其他來源，則該目錄必須位於 (由) IAM 身分中心委派管理員成員帳戶 (如果存在)；否則，該目錄必須位於管理帳戶中。

AWS Organizations

您的AWS 帳戶必須由以下人員管理AWS Organizations。如果您尚未設定組織，則不必這麼做。啟用 IAM 身分中心時，您將選擇是否要AWS為您創建一個組織。

如果您已設定AWS Organizations」，請確定已啟用所有功能。如需詳細資訊，請參閱 AWS Organizations 使用者指南中的啟用組織中的所有功能。

若要啟用 IAM 身分中心，您必須登入AWS Management Console通過使用您的憑據AWS Organizations管理帳戶。使用來自的登入資料登入時，無法啟用 IAM 身分中心AWS Organizations會員帳戶。如需詳細資訊，請參閱建立和管理AWS組織在AWS Organizations使用者指南。

IAM 角色

如果您已在AWS 帳戶，我們建議您檢查您的帳戶是否接近 IAM 角色的配額。如需詳細資訊，請參閱IAM 物件配額。

如果您接近配額，請考慮要求增加配額。否則，當您佈建權限集到超過 IAM 角色配額的帳戶時，您可能會遇到 IAM 身分中心的問題。如需如何要求提高配額的相關資訊，請參閱要求增加配額在服務配額使用指南。

新世代防火牆和安全的 Web 閘道

如果您篩選特定的存取權AWS網域或 URL 端點使用網頁內容過濾解決方案 (例如 NGFW 或 SWG)，您必須將下列網域或 URL 端點新增至您的網頁內容過濾解決方案允許清單。

特定的 DNS 網域

- *.aws.com (http://awsapps.com/)
- * 登入

特定網址端點

- HTTPS://[####].awsapp.com /開始
- HTTPS://[####]. aws.com /登錄
- HTTPS://[#####]. 登錄.aw/平台/登錄

使用多個 AWS 帳戶

AWS 帳戶作為基本的安全邊界AWS。它們作為提供有用的隔離級別的資源容器。隔離資源和使用者的能力是建立安全且受到妥善管理的環境的關鍵要求。

將您的資源分離為單獨AWS 帳戶協助您在雲端環境中支援下列原則：

- 安全控制— 不同的應用程式可以有不同的安全性設定檔，需要不同的控制原則和機制 例如，與稽核員交談更容易，並且能夠指向單一AWS 帳戶託管工作負載的所有元素支付卡產業 (PCI) 安全標準。
- 隔離— 一個AWS 帳戶是安全保護的一個單位。潛在風險和安全威脅應包含在AWS 帳戶而不影響他人。由於不同的團隊或安全配置文件不同，可能會有不同的安全需求。
- 許多團隊— 不同的團隊有不同的職責和資源需求。您可以通過將團隊移動到分開來防止團隊相互干擾AWS 帳戶。
- 資料隔離— 除了隔離團隊之外，將數據存儲區隔離到帳戶非常重要。這有助於限制可以存取和管理該資料存放區的人數。這有助於控制高度私密數據的暴露，因此可以幫助遵守歐盟的一般資料保護條例 (GDPR)。
- 事務, 過程— 不同的業務單位或產品可能有完全不同的目的和流程。有多個AWS 帳戶，您可以支援業務單位的特定需求。
- 帳單— 帳戶是在帳單級別分隔項目的唯一真正方法。多個帳戶有助於跨業務單位、功能團隊或個別使用者在帳單層級分隔項目。您仍然可以將所有賬單合併到單個付款人（使用AWS Organizations和合併帳單），同時將明細項目分隔AWS 帳戶。
- 配額分配—AWS每個服務配額都會分別強制執行AWS 帳戶。將工作負載區分為不AWS 帳戶防止它們彼此消耗配額。

本指南中描述的所有建議和程序均符合AWS架構良好的框架。此架構旨在協助您設計彈性、彈性且可擴充的雲端基礎架構。即使您從小規模開始，我們也建議您遵循框架中的指導進行操作。這樣做可以幫助您安全地擴展環境，而不會隨著您的成長而影響正在進行的操作。

在開始新增多個帳戶之前，您需要制定管理帳戶的計劃。為此，我們建議您使用AWS Organizations，這是一個免費的AWS服務，管理所有AWS 帳戶在您的組織中。

AWS還提供AWS Control Tower，這增加了圖層AWS管理自動化到組織，並自動與其他組織整合AWS服務喜歡AWS CloudTrail,AWS Config, 亞馬遜CloudWatch,AWS Service Catalog，和其他人。這些服務可能會產生額外費用。如需詳細資訊，請參閱 AWS Control Tower 定價。

第 1 部分：設置一個新的AWS 帳戶

這些說明將幫助您創建AWS 帳戶並保護根用戶憑據。完成所有步驟，然後再繼續第 2 部分：在 IAM 身分中心建立管理使用者。

主題

- 步驟 1：註冊 AWS 帳戶
- 步驟 2：以 root 使用者身分登入
- 步驟 3：為您的AWS 帳戶根使用者

步驟 1：註冊 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 選擇創建一個AWS 帳戶。

   > **Note**
   >
   > 如果您登入AWS最近，選擇登入主控台。如果選項創建一個新的AWS 帳戶不可見，先選擇登入其他帳戶，然後選擇創建一個新的AWS 帳戶。

3. 輸入您的帳戶資訊，然後選擇繼續。

   請務必正確輸入您的帳戶資訊，尤其是您的電子郵件地址。如果您輸入的電子郵件地址不正確，就無法存取您的帳戶。

4. 選擇個人或者專業。

   這些選項之間的區別僅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。

5. 根據中提供的指導輸入您的公司或個人信息AWS 帳戶 要求。
6. 閱讀並接受AWS客戶協議。
7. 選擇創建帳戶並繼續。

   此時，您將收到一封電子郵件，以確認您的AWS 帳戶準備使用。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，您不能使用任何AWS服務直到您完成啟用帳戶為止。

8. 在「」付款資訊頁面中，輸入有關您的付款方式的信息。如果您想要使用的地址與建立帳戶所用的地址不同，請選擇使用新地址並輸入您要用於帳單目的的地址。

9. 選擇驗證並新增。

> **Note**
>
> 如果您的聯絡地址位於印度，您的帳戶使用者合約為當地 AISPLAWS在印度的賣家。在驗證過程中您必須提供您的 CVV。您可能還需要輸入一次性密碼，具體取決於您的銀行。AISPL 會在驗證過程中向您收取 2 INR 的付款方式收取費用。AISPL 在完成驗證後退還 2 印度盧比。

10. 要驗證您的電話號碼，請從列表中選擇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可以撥打您的電話號碼。輸入驗證碼，然後提交。
11. 該AWS自動驗證系統會致電給您並提供 PIN 碼。使用手機輸入 PIN 碼，然後選擇繼續。
12. 選擇一個AWS Support計劃。

    如需可用計劃的說明，請參閱比較AWS Support計劃。

    此時會出現確認頁面，指出您的帳戶正在啟用。這通常只需要幾分鐘，但有時可能需要長達 24 小時。啟用期間，您可以登入新的AWS 帳戶。在啟用完成之前，您可能會看到完成註冊按鈕。您可以忽略。

    AWS帳號啟用完成後，會傳送確認電子郵件訊息。檢查您的電子郵件和垃圾郵件文件夾中的確認電子郵件。收到此消息後，您可以完全訪問所有信息AWS服務。

步驟 2：以 root 使用者身分登入

當您初次建立 AWS 帳戶 時，您會先有一個登入身分，可以完整存取帳戶中的所有 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。

> **Important**
>
> 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。

若要以 root 使用者身分登入

1. 開啟位於 https://console.aws.amazon.com/ 的 AWS Management Console。

   > **Note**
   >
   > 如果您先前曾在此瀏覽器中以 root 使用者身分登入，您的瀏覽器可能會記住的電子郵件地址AWS 帳戶。
   > 如果您先前已使用此瀏覽器以 IAM 使用者身分登入，您的瀏覽器可能會改為顯示 IAM 使用者登入頁面。若要返回主要登入頁面，請選擇 Sign in using root user email (使用根使用者電子郵件登入)。

2. 如果您先前從未使用過此瀏覽器登入，便會出現主要登入頁面。如果您是帳戶擁有者，請選擇 Root 使用者。輸入與帳戶相關聯的AWS 帳戶電子郵件地址，然後選擇「下一步」
3. 系統可能會提示您完成安全性檢查。完成此操作即可進入下一步。如果您無法完成安全性檢查，請嘗試聆聽音訊或重新整理安全性檢查是否有新的字元集。
4. 輸入您的密碼，然後選擇 Sign in (登入)。

步驟 3：為您的AWS 帳戶根使用者

若要加強 root 使用者認證的安全性，我們建議您遵循安全性最佳作法，為您的AWS 帳戶。由於 root 使用者可以在您的帳戶中執行敏感作業，因此新增此額外的驗證層可協助您更好地保護您的帳戶。有多種類型的 MFA 可供使用。

如需針對根使用者啟動 MFA 的指示，請參閱為中的使用者啟用 MFA 裝置AWS在IAM 使用者指南。

第 2 部分：在 IAM 身分中心建立管理使用者

完成之後第 1 部分：設置一個新的AWS 帳戶，以下步驟將幫助您設置AWS 帳戶管理使用者的存取權，這將用來執行日常工作。

> **Note**
>
> 本主題提供成功設定管理員存取權的最低必要步驟AWS 帳戶並在 IAM 身分中心建立管理使用者。如需其他資訊，請參閱開始使用在AWS IAM Identity Center使用者指南。

主題

步驟 1：啟用 IAM 身分中心

> **Note**
>
> 如果您沒有為 root 使用者啟動多重要素驗證 (MFA)，請完成步驟 3：為您的AWS 帳戶根使用者在您繼續之前。

啟用 IAM 身分識別中心

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。
2. 打開IAM 身分中心主控台。
3. 下啟用 IAM 身分識別中心，選擇啟用。
4. IAM 身分識別中心需要AWS Organizations。如果您尚未設定組織，則必須選擇是否擁有AWS為您創建一個。選擇創建AWS組織以完成此過程。

AWS Organizations會自動傳送驗證電子郵件至與您管理帳戶相關聯的電子郵件地址。在您收到驗證電子郵件之前，可能會有一些延遲的時間。請在 24 小時內驗證您的電子郵件地址。

> **Note**
>
> 如果您使用的是多帳戶環境，建議您設定委派管理。透過委派管理，您可以限制需要存取管理帳戶的人數AWS Organizations。如需詳細資訊，請參閱委派管理在AWS IAM Identity Center使用者指南。

步驟 2：選擇身分識別來源

IAM 身分中心中的身分識別來源會定義管理使用者和群組的位置。您可以選擇下列其中一項作為身分識別來源：

- IAM 身分識別中心目錄— 首次啟用 IAM 身分中心時，系統會自動將 IAM 身分中心目錄設定為預設身分識別來源。您可以在這裡建立使用者和群組，並將其存取層級指派給 AWS 帳戶和應用程式。
- 活動目錄— 如果您想要繼續使用 AWS 目錄服務管理 AWS 受管 Microsoft AD 目錄中的使用者，或是您在作用中目錄 (AD) 中的自我管理目錄，請選擇此選項。
- 外部識別提供者— 如果您想要管理外部身分識別提供者 (IdP) (例如 Okta 或 Azure 作用中目錄) 中的使用者，請選擇此選項。

啟用 IAM 身分中心後，您必須選擇身分識別來源。您選擇的身分識別來源會決定 IAM 身分中心在何處搜尋需要單一登入存取權的使用者和群組。選擇身分識別來源後，您將建立或指定使用者，並將系統管理權限指派給您AWS 帳戶。

> **Important**
>
> 如果您已經在 Active Directory 或外部身分識別提供者 (IdP) 中管理使用者和群組，建議您在啟用 IAM 身分中心並選擇身分識別來源時考慮連線此身分識別來源。在您在預設 Identity Center 目錄中建立任何使用者和群組並進行任何指派之前，應該先完成此動作。如果您已經在一個身分識別來源中管理使用者和群組，變更為其他身分識別來源可能會移除您在 IAM Identity Center 中設定的所有使用者和群組指派。如果發生這種情況，所有使用者 (包括 IAM Identity Center 中的系統管理使用者) 都將失去對他們的單一登入存取權AWS 帳戶和應用程序。

主題

連線使用中目錄或其他 IdP 並指定使用者

如果您已經在使用 Active Directory 或外部身分識別提供者 (IdP)，下列主題將協助您將目錄連線到 IAM 身分識別中心。

您可以連接AWS Managed Microsoft AD目錄、作用中目錄中的自我管理目錄，或具有 IAM 身分識別中心的外部 IdP。如果您打算連接AWS Managed Microsoft AD目錄或作用中目錄中的自我管理目錄，請確定您的 Active Directory 組態符合中的先決條件作用中目錄或外部 IdP。

> **Note**
>
> 我們強烈建議您啟用多重要素驗證，做為安全性最佳作法。如果您打算連接AWS Managed Microsoft AD目錄或活動目錄中的自我管理目錄，並且您沒有使用 RADIUS MFAAWS Directory Service，在 IAM 身分中心啟用 MFA。如果您打算使用外部身分識別提供者，請注意外部 IdP (而非 IAM 身分中心) 會管理 MFA 設定。IAM 身分中心中的 MFA 不支援外部使用 IdPs。如需詳細資訊，請參閱啟用 MFA在AWS IAM Identity Center使用者指南。

AWS Managed Microsoft AD

1. 檢閱中的指引連接到微軟活動目錄。
2. 按照中的步驟操作連接目錄AWS Managed Microsoft AD前往 IAM 身分識別中心。
3. 設定作用中目錄，以將您要授與管理權限的使用者同步至 IAM 身分識別中心。如需詳細資訊，請參閱將管理使用者同步至 IAM 身分中心。

作用中目錄中的自我管理目錄

1. 檢閱中的指引連接到微軟活動目錄。
2. 按照中的步驟操作將作用中目錄中的自我管理目錄連線到 IAM 身分識別中心。
3. 設定作用中目錄，以將您要授與管理權限的使用者同步至 IAM 身分識別中心。如需詳細資訊，請參閱在 IAM 身分中心同步處理系統管理使用者。

外部 IdP

1. 檢閱中的指引連線至外部身分識別提供者。
2. 按照中的步驟操作如何連線至外部身分識別提供者。
3. 將您的 IdP 設定為將使用者佈建至 IAM 身分中心。

> **Note**
>
> 在您將所有員工身分從 IdP 設定到 IAM 身分中心的自動化群組式佈建之前，建議您先將要授予管理許可的一位使用者同步至 IAM 身分中心。

將管理使用者同步至 IAM 身分中心

將目錄連線到 IAM Identity Center 後，您可以指定要授與管理權限的使用者，然後將該使用者從目錄同步到 IAM 身分中心。

1. 打開IAM 身分中心主控台。
2. 選擇 Settings (設定)。
3. 在「」設定頁面上，選擇識別來源」頁籤上，選擇動作，然後選擇管理同步。
4. 在「」管理同步頁面上，選擇使用者」標籤，然後選擇新增使用者和群組。
5. 在「」使用者標籤的下使用者，請輸入確切的使用者名稱，然後選擇新增。
6. 下新增的使用者和群組，執行下列動作：
   a. 確認已指定要授與管理權限的使用者。
   b. 選取使用者名稱左側的核取方塊。
   c. 選擇 Submit (提交)。
7. 在管理同步頁面中，您指定的使用者會顯示在同步範圍內的使用者列表。
8. 在導覽窗格中，選擇 使用者 。
9. 在「」使用者頁面中，您指定的使用者可能需要一些時間才會顯示在清單中。選擇重新整理圖示以更新使用者清單。

此時，您的使用者無法存取管理帳戶。您可以透過建立系統管理權限集並將使用者指派給該權限集，來設定此帳戶的管理存取權限。

下一步： 步驟 3：建立系統管理權限集

使用預設目錄並在 IAM 身分中心建立使用者

首次啟用 IAM 身分中心時，系統會自動將 IAM 身分中心目錄設定為預設身分識別來源。完成下列步驟，以在 IAM 身分中心建立使用者。

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。
2. 打開IAM 身分中心主控台。
3. 請按照中的步驟操作新增使用者以建立使用者。

   當您指定使用者詳細資訊時，您可以傳送包含密碼設定指示的電子郵件 (這是預設選項)，或產生一次性密碼。如果您傳送電子郵件，請務必指定可存取的電子郵件地址。
4. 新增使用者之後，請返回此程序。如果您保留預設選項來傳送包含密碼設定說明的電子郵件，請執行下列動作：

   a. 您將收到一封包含主題的電子郵件邀請加入AWS單一登入。打開電子郵件並選擇接受邀請。

   b. 在「」新用戶註冊頁面上，輸入並確認密碼，然後選擇設定新密碼。

   > **Note**
   >
   > 確保保存您的密碼。您稍後將需要它步驟 5：登入AWS使用您的管理憑據訪問門戶。

此時，您的使用者無法存取管理帳戶。您可以透過建立系統管理權限集並將使用者指派給該權限集，來設定此帳戶的管理存取權限。

下一步： 步驟 3：建立系統管理權限集

步驟 3：建立系統管理權限集

權限集會儲存在 IAM 身分中心，並定義使用者和群組必須存取的存取層級AWS 帳戶。執行下列步驟來建立授與系統管理權限的權限集。

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。
2. 打開IAM 身分中心主控台。

3. 在「IAM 身分中心」導覽窗格的下多帳戶權限，選擇權限集。
4. 選擇 Create permission set (建立許可集合)。
5. 對於步驟 1：選取權限集類型，在「」選取權限集類型頁面中，保留默認設置並選擇下一步。預設設定會授與完整存取權AWS服務和資源使用AdministratorAccess預先定義的權限集。

> **Note**
>
> 預先定義的AdministratorAccess權限集使用AdministratorAccess AWS受管理的策略。

6. 對於步驟 2：指定權限集詳細資料，在「」指定權限集詳細資料頁面中，保留默認設置並選擇下一步。預設設定會將工作階段限制為一小時。
7. 對於步驟 3：檢閱並建立，在「」檢閱和建立頁面中，執行下列動作：

    1. 檢閱權限集類型並確認其為AdministratorAccess。
    2. 檢閱AWS管理策略並確認它是AdministratorAccess。
    3. 選擇 建立 。

步驟 4：設定AWS 帳戶管理使用者的存取

若要設定AWS 帳戶IAM 身分中心中的管理使用者存取權，您必須將該使用者指派給AdministratorAccess權限集。

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。
2. 打開IAM 身分中心主控台。
3. 在導覽窗格中的多帳戶權限，選擇AWS 帳戶。
4. 在「」AWS 帳戶頁面中，會出現組織的樹狀檢視清單。選取旁邊的核取方塊AWS 帳戶您要指派管理存取權的目標。如果您的組織中有多個帳戶，請選取管理帳戶旁邊的核取方塊。
5. 選擇指派使用者或群組。
6. 對於步驟 1：選取使用者和群組，在「」將使用者和群組指派給」***AWS-###***「頁面中，執行下列動作：

    1. 在「」使用者」頁籤上，選取您要授與管理權限的使用者。

        若要篩選結果，請開始在搜尋方塊中輸入您想要的使用者名稱。
    2. 確認選取正確的使用者之後，請選擇下一步。

7. 對於步驟 2：選取權限集，在「」將權限集指派給」***AWS-###***「頁面，下權限集」中，選取AdministratorAccess權限集。
8. 選擇 下一步。
9. 對於步驟 3：檢閱並提交，在「」檢閱作業並將其提交給」***AWS-###***「頁面中，執行下列動作：

    1. 檢閱選取的使用者和權限集。
    2. 在您確認已將正確的使用者指派給AdministratorAccess權限集, 選擇提交。

    > **Important**
    >
    > 使用者指派程序可能需要幾分鐘的時間才能完成。保持此頁面開啟狀態，直到程序順利完成為止。

10. 如果符合下列任一條件，請依照中的步驟執行啟用 MFA若要為 IAM 身分中心啟用 MFA：

    - 您使用預設的身分識別中心目錄做為身分識別來源。
    - 您正在使用AWS Managed Microsoft AD目錄或活動目錄中的自我管理目錄作為您的身分識別來源，而且您沒有使用 RADIUS MFAAWS Directory Service。

    > **Note**
    >
    > 如果您使用外部身分識別提供者，請注意，外部 IdP (而非 IAM 身分中心) 會管理 MFA 設定。IAM 身分中心中的 MFA 不支援外部使用IdPs。

當您為管理使用者設定帳戶存取權時，IAM Identity Center 會建立對應的 IAM 角色。此角色由 IAM 身分中心控制，建立於相關AWS 帳戶，並將權限集中指定的原則附加至角色。

步驟 5：登入AWS使用您的管理憑據訪問門戶

請完成下列步驟，確認您可以登入AWS使用系統管理使用者的認證存取入口網站，並且您可以存取 AWS 帳戶。

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。
2. 開啟 AWS IAM Identity Center 主控台 https://console.aws.amazon.com/singlesignon/。
3. 在導覽窗格中，選擇 Dashboard (儀表板)。

4. 在「」儀表板頁面，下方設定摘要，複製AWS存取入口網站網址。
5. 打開一個單獨的瀏覽器，粘貼AWS訪問您複製的門戶網址，然後按輸入。
6. 使用下列其中一種方式登入：

   - 如果您使用 Active Directory 或外部身分識別提供者 (IdP) 做為身分識別來源，請使用您指派給AdministratorAccess在 IAM 身分中心中設定的權限。
   - 如果您使用預設的 IAM Identity Center 目錄做為身分識別來源，請使用您在建立使用者時指定的使用者名稱和為該使用者指定的新密碼登入。
7. 在您登入之後，AWS 帳戶圖示會出現在入口網站中。
8. 當您選取AWS 帳戶圖示時，會顯示與該帳戶相關聯的帳戶名稱、帳戶 ID 和電子郵件地址。
9. 選擇要顯示的帳號名稱AdministratorAccess權限集，然後選取管理主控台鏈接到右側AdministratorAccess。

   當您登入時，指派給使用者的權限集名稱會顯示為AWS存取入口網站。因為您已將此使用者指派給AdministratorAccess權限集，角色將出現在AWS訪問門戶網站為：AdministratorAccess/###
10. 如果您被重定向到AWS管理主控台時，您已成功完成設定AWS 帳戶。繼續執行步驟 10。
11. 切換至您用來登入的瀏覽器AWS Management Console並設定 IAM 身分中心，然後從您的AWS帳戶根使用者。

    > **Important**
    >
    > 強烈建議您在登入時遵守使用系統管理使用者認證的最佳作法AWS訪問門戶，並且您不使用 root 用戶憑據進行日常任務。

若要允許其他使用者存取您的帳戶和應用程式，以及管理 IAM 身分中心，請僅透過 IAM 身分中心建立和指派權限集。

疑難排AWS 帳戶建立問題

使用此處的資訊可協助您疑難排解與建立相關的問題AWS 帳戶。

問題

- 我沒有收到來自的電話AWS驗證我的新帳戶
- 當我嘗試驗證我的錯誤時，出現有關「嘗試失敗的最大次數」的錯誤AWS 帳戶通過電話
- 已經超過 24 小時，我的帳戶尚未激活

我沒有收到來自的電話AWS驗證我的新帳戶

當你創建一個AWS 帳戶，您必須提供可以接收 SMS 簡訊或語音通話的電話號碼。您可以指定用來驗證號碼的方法。

如果您沒有收到訊息或來電，請確認下列事項：

- 您在註冊過程中輸入了正確的電話號碼，並選擇了正確的國家/地區代碼。
- 如果您使用的是行動電話，請確定您有行動電話訊號可接收簡訊或通話。
- 您為您輸入的資訊付款方式是正確的。

如果您沒有收到 SMS 短信或致電完成身份驗證過程，AWS Support可以幫助您激活AWS 帳戶手動。使用下列步驟：

1. 請確保您可以在電話號碼您為您提供的AWS 帳戶。
2. 打開AWS Support安慰，然後選擇建立案例。
   a. 選擇帳戶和帳單支援。
   b. 對於类型，選取帳號。
   c. 對於類別，選取激活。
   d. 在案例描述部分中，提供您可以到達的日期和時間。
   e. 在聯絡選項區段中，選取聊天為了聯絡方式。
   f. 選擇 Submit (提交)。

> **Note**
>
> 您可以使用以下方式建立案例AWS Support即使你AWS 帳戶未啟動。

當我嘗試驗證我的錯誤時，出現有關「嘗試失敗的最大次數」的錯誤AWS 帳戶通過電話

AWS Support可以幫助您手動激活您的帳戶。請遵循下列步驟：

1. 登入您的AWS 帳戶使用您在創建帳戶時指定的電子郵件地址和密碼。
2. 打開AWS Support安慰，然後選擇建立案例。
3. 選擇帳戶與帳單支援。
4. 對於类型，選取帳號。
5. 對於類別，選取激活。
6. 在案例描述部分中，提供您可以到達的日期和時間。
7. 在聯絡選項區段中，選取聊天為了聯絡方式。
8. 選擇 Submit (提交)。

AWS Support將與您聯繫並嘗試手動激活您的AWS 帳戶。

已經超過 24 小時，我的帳戶尚未激活

帳戶激活有時可能會延遲。如果該過程需要超過 24 小時，請檢查以下內容：

- 完成帳戶激活過程。

  如果您在新增所有必要資訊之前關閉了註冊程序的視窗，請開啟註冊頁面。選擇登入現有AWS 帳戶，然後使用您為帳戶選擇的電子郵件地址和密碼登入。
- 檢查與您的付款方式相關的資訊。

  在AWS Billing and Cost Management控制台，檢查付款方式對於錯誤。
- 請聯絡您的金融機構。

有時金融機構拒絕來自的授權請求AWS。請聯絡與您的付款方式相關聯的機構，並要求他們核准授權要求AWS。AWS一旦您的金融機構核准授權要求，就會立即取消授權要求，因此您無需支付授權要求的費用。在您的金融機構的結單上，授權請求可能仍會顯示為少量費用（通常為 1 美元）。

- 請檢查您的電子郵件和垃圾郵件文件夾以獲取更多信息。
- 嘗試使用其他瀏覽器。
- 。聯繫AWS Support。

。聯繫AWS Support尋求幫助。提及您已經嘗試過的任何疑難排解步驟。

> **Note**
>
> 不要在任何信件中提供敏感信息，例如信用卡號碼AWS。

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。