使用者指南

AWS IAM Identity Center

AWS IAM Identity Center: 使用者指南

Table of Contents

什麼是 IAM 身分中心？

AWS IAM Identity Center 建議用 AWS 服務 於管理人類使用者對 AWS 資源的存取。在單一位置，您可以在其中指派員工使用者，也稱為workforce identities對多個應用程式 AWS 帳戶 和應用程式的一致存取權。IAM 身分中心不收取額外費用。

透過 IAM 身分中心，您可以建立或連結員工使用者，並集中管理其所有使用者 AWS 帳戶 和應用程式的存取權限。您可以使用多帳戶權限將您的員工使用者存取權指派給。 AWS 帳戶您可以使用應用程式指派，為使用者指派 AWS 受管理和客戶管理應用程式的存取權。

> **Note**
>
> 雖然服務名稱 Single Sig AWS n-On 已淘汰，但在本指南中仍會使用「單一登入」一詞來描述驗證配置，讓使用者一次登入以存取多個應用程式和網站。

IAM 身分識別中心功能

IAM 身分識別中心包含下列核心功能和功能：

管理員工身分

在其中建立或操作工作負載的人類使 AWS 用者也稱為勞動力使用者或員工身分識別。員工使用者是指您允許在組織和內部商務應用程式 AWS 帳戶 中存取的員工或承包商。這些人員可能是構建內部和面向客戶的系統的開發人員，或內部數據庫系統和應用程序的用戶。您可以在 IAM Identity Center 中建立員工使用者和群組，或連線並同步至您自己身分識別來源中的一組現有使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需詳細資訊，請參閱 管理身分識別來源。

管理 IAM 身分中心的執行個體

IAM 身分中心支援兩種類型的執行個體：組織執行個體和帳戶執行個體。組織執行個體是最佳做法。這是唯一可讓您管理存取權的執行個體 AWS 帳戶 ，建議您用於應用程式的所有生產環境。組織執行個體會部署在 AWS Organizations 管理帳戶中，並提供單一點來管理整個 AWS 環境中的使用者存取權。

帳戶實例綁定 AWS 帳戶 到啟用它們的。僅使用 IAM 身分中心的帳戶執行個體來支援特定 AWS 受管應用程式的隔離部署。如需詳細資訊，請參閱 管理 IAM 身分中心的組織和帳戶執行個體。

管理多個存取 AWS 帳戶

透過多帳戶權限，您可以一次規劃並集中實作多個 AWS 帳戶 帳戶的權限，而無需手動設定每個帳戶。您可以根據一般工作職能建立權限，或定義符合安全性需求的自訂權限。然後，您可以將這些權限指派給員工使用者，以控制他們對特定帳戶的存取權。

此選用功能僅適用於組織實例。如果您在環境中使用每個帳戶的 IAM 角色管理，則這兩個系統都可以共存。如果您想嘗試使用多帳戶權限，您可以先在有限的基礎上實施此系統，然後隨著時間的推移遷移更多環境以使用此系統。

管理應用程式的存取

IAM 身分識別中心可讓您簡化應用程式存取管理。透過 IAM 身分中心，您可以在 IAM 身分中心單一登入應用程式授與員工使用者。

AWS 受管理應用

AWS 提供與 IAM 身分中心整合的應用程式，例如 Amazon 受管的 Grafana 和亞馬遜監控。Amazon Redshift這些應用程式可以使用 IAM 身分中心進行身分驗證、目錄服務和受信任的身分傳播。您的使用者受益於一致的單一登入體驗，而且由於應用程式共用使用者、群組和群組成員資格的共同檢視，因此使用者在與其他人共用應用程式資源時也能獲得一致的體驗。您可以將 AWS 受管應用程式設定為直接從相關應用程式主控台內或透過 API 使用 IAM 身分中心。

客戶管理的應用

您可以在 IAM 身分中心單一登入授與員工使用者存取支援 SAML 2.0 聯合身分識別的應用程式。許多常用的 SAML 2.0 應用程式 (例如 Salesforce 和 Microsoft 365) 都可以與 IAM 身分識別中心搭配使用，並可在 IAM 身分中心主控台的應用程式目錄中取得。如果您使用這類應用程式，並在 IAM 身分識別中心中建立使用者和群組，或者您使用 Microsoft Active Directory 網域服務做為身分識別來源，這是一項選用功能，可能會很有幫助。

跨應用程式的可信身分傳播

受信任的身分傳播可為需要存取 AWS 服務中資料的查詢工具和商業智慧 (BI) 應用程式的使用者提供簡化的單一登入體驗。資料存取管理是以使用者的身分為基礎，因此管理員可以根據使用者現有的使用者和群組成員資格授與存取權。使用者對 AWS 服務和其他事件的存取權會記錄在服務特定記錄檔和 CloudTrail 事件中，以便稽核人員知道使用者採取了哪些動作，以及使用者存取的資源。

AWS 為您的使用者存取入口網站

AWS 存取入口網站是一個簡單的入口網站，可讓您的使用者順暢存取所有指派的應用程式 AWS 帳戶 和應用程式。

IAM 身分中心重新命名

2022 年 7 月 26 日，「AWS 單一登入」已重新命名為 AWS IAM Identity Center。對於現有客戶而言，下表旨在說明本指南中因重新命名而更新的一些較常見的術語變更。

舊版術語	目前任期
AWS SSO 使用者或 SSO 使用者	員工使用者或使用者
AWS SSO 使用者入口網站或用戶入口	AWS 訪問門戶
AWS SSO 整合式應用程式	AWS 受管理應用
AWS SSO 目錄	Identity Center 目錄
AWS SSO 存放區或 AWS SSO 身分識別存放區	IAM 身分中心使用的身分存放區

下表說明此重新命名也發生的適用使用者、開發人員和 API 參考指南名稱變更。

舊版指南	目前的指南
AWS 單一登入使用者指南	IAM 身分中心使用者指南
AWS 單一登入 SCIM 實作開發人員指南	IAM 身分識別中心 SCIM 實作開發人員指南
AWS 單一登入 API 參考指南	IAM 身分識別中心 API 參考
AWS 單一登入身分識別存放區 API 參考指	識別身分存放區 API 參
AWS 單一登入 OIDC API 參考指南	身分識別中心 OIDC API 參考
AWS 單一登入入口網站 API 參考指南	IAM 身分中心入口網站 API 參考

舊版命名空間保持不變

出於向後兼容性目的，`sso`和 `identitystore` API 命名空間以及以下相關命名空間保持不變。

- CLI 命令
  - aws configure sso
  - identitystore
  - sso
  - sso-admin
  - sso-oidc
- 包含AWSSSO和AWSIdentitySync前置詞的受管理策略
- 包含sso和的服務端點 identitystore
- AWS CloudFormation包含AWS::SSO前綴的資源
- 服務連結角色：AWSServiceRoleForSSO
- 包含sso和的主控台 URL singlesignon
- 文件網址包含 singlesignon

啟用 AWS IAM Identity Center

完成下列步驟以登入 IAM 身分中心的組織執行個體 AWS Management Console 並啟用組織執行個體。

1. 請執行下列任一項作業，以登入 AWS Management Console。
   - [新增至 AWS (root 使用者)] — 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。在下一頁中，輸入您的密碼。
   - 已在使用 AWS (IAM 登入資料) — 使用具有管理許可的 IAM 登入資料登入。
2. 開啟 IAM 身分中心主控台。
3. 在 [啟用 IAM 身分中心] 下，選擇 [啟用方式] AWS Organizations。
4. 選擇性新增您要與此組織執行個體建立關聯的標籤。
5. 選擇性設定委派管理。

> **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，您可以限制中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。

> **Important**
>
> 依預設，會啟用建立 IAM 身分中心帳戶執行個體的功能。IAM 身分中心的帳戶執行個體包含組織執行個體可用的功能子集。您可以使用服務控制策略來控制使用者是否可以存取此功能。

您是否需要更新防火牆和閘道？

如果您使用網頁內容過濾解決方案 (例如下一代防火牆 (NGFW) 或安全網頁閘道 (SWG) 來篩選對特定網 AWS 域或 URL 端點的存取，則必須將下列網域或 URL 端點新增至網頁內容過濾解決方案允許清單。這樣做可讓您存取您的存 AWS 取入口網站。

- *[Directory ID or alias]*.awsapps.com
- *.aws.dev
- *.awsstatic.com

- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

允許列出網域和 URL 端點的考量

瞭解允許列出 AWS 存取入口網站以外的網域的影響。

- 若要從存取 AWS 帳戶入口網站存取 AWS Management Console、和 IAM 身分中心主控台，您 AWS 必須允許列出其他網域。如需 AWS Management Console 網域清單，請參閱AWS Management Console 入門指南中的疑難排解。
- 若要從存取入口網站 AWS 存取 AWS 受管理的應用程式，您必須允許列出各自的網域。如需指引，請參閱相應的服務文件。
- 這些允許清單涵蓋 AWS 服務。如果您使用外部軟體，例如外部軟體 IdPs (例如Okta和Microsoft Entra ID)，則需要在允許清單中包含其網域。

您現在已準備好設定 IAM 身分中心。啟用 IAM 身分中心時，系統會自動將身分中心目錄設定為預設身分識別來源，這是開始使用 IAM 身分中心的最快方式。如需說明，請參閱使用預設的 IAM 身分中心目錄設定使用者存取。

如果您想進一步了解 IAM 身分中心如何與 Organizations、身分識別來源和 IAM 角色搭配使用，請參閱下列主題。

主題

- 先決條件和考量事項
- 在 IAM 身分中心確認您的身分來源

先決條件和考量事項

下列主題提供設定 IAM 身分中心的必要條件和其他考量事項的相關資訊。

選擇一個注意事項 AWS 區域

您可以在自選支援 AWS 區域 的單一執行個體中啟用 IAM 身分中心執行個體。選擇區域需要根據您的使用案例和公司政策評估您的優先順序。從 IAM Identity Center 存取 AWS 帳戶 和雲端應用程式並不取決於此選擇；不過，存取 AWS 受管理應用程式以及用 AWS Managed Microsoft AD 作身分識別來源的能力，可能取決於此選擇。如需 AWS IAM 身分中心支援的區域清單，請 AWS 一般參考 參閱中的 IAM 身分中心端點和配額。

選擇 AWS 區域.

- 地理位置 — 當您選取地理位置上最接近大多數使用者的區域時，他們對存取入口網站和 AWS 受管理應用程式 (例如 Amazon SageMaker Studio) 的 AWS 存取延遲將較低。
- AWS 受管應用程式的可用性 — AWS 受管應用程式 (例如 Amazon SageMaker) 只能在支援的應用程 AWS 區域 式中運作。在您要搭配使用的 AWS 受管理應用程式所支援的區域中啟用 IAM 身分中心。許多 AWS 受管理應用程式也只能在您啟用 IAM 身分中心的相同區域中運作。
- 數位主權 — 數位主權法規或公司政策可能會強制使用特定項目。 AWS 區域請諮詢貴公司的法律部門。
- 身分識別來源 — 如果您使用 AWS Managed Microsoft AD 或 AD Connector 做為身分識別來源，則其主區域必須與您啟用 IAM 身分中心的區域相符。 AWS 區域
- 預設情況下停用區域 — AWS 最初預設 AWS 區域 為啟用所有新功能，這會自動讓您的使用者在任何區域中建立資源。 AWS 帳戶 現在，當 AWS 添加新區域時，默認情況下在所有帳戶中禁用其使用。如果您在預設停用的區域中部署 IAM 身分中心，則必須在要管理 IAM 身分中心存取權的所有帳戶中啟用此區域。即使您不打算在這些帳戶中在該區域中建立任何資源，這也是必要的。

  您可以為組織中目前帳戶啟用 [區域]，而且您必須對稍後可能新增的新帳戶重複此動作。如需指示，請參閱使用 AWS Organizations 者指南中的啟用或停用組織中的區域。若要避免重複這些額外步驟，您可以選擇在預設啟用的區域中部署 IAM 身分中心。作為參考，預設會啟用下列「區域」：

  - 美國東部 (俄亥俄)
  - 美國東部 (維吉尼亞北部)
  - 美國西部 (奧勒岡)
  - 美國西部 (加利佛尼亞北部)
  - Europe (Paris)

- 南美洲 (聖保羅)
- 亞太區域 (孟買)
- 歐洲 (斯德哥爾摩)
- 亞太區域 (首爾)
- 亞太區域 (東京)
- 歐洲 (愛爾蘭)
- 歐洲 (法蘭克福)
- 歐洲 (倫敦)
- 亞太區域 (新加坡)
- 亞太區域 (悉尼)
- 加拿大 (中部)
- 亞太區域 (大阪)

- 跨區域通話 — 在某些區域，IAM 身分中心可能會呼叫不同區域的 Amazon 簡易電子郵件服務以傳送電子郵件。在這些跨區域呼叫中，IAM 身分中心會將特定使用者屬性傳送至其他區域。如需關於區域的詳細資訊，請參閱AWS IAM Identity Center 區域可用性。

交換 AWS 區域

您只能透過刪除目前的執行個體並在其他區域建立新執行個體來切換 IAM 身分中心區域。如果您已透過現有執行個體啟用 AWS 受管應用程式，則應先刪除該應用程式，然後再刪除 IAM 身分中心。您必須在新執行個體中重新建立使用者、群組、權限集、應用程式和指派。您可以使用 IAM 身分中心帳戶和應用程式指派 API 取得組態的快照，然後使用該快照在新區域中重建您的組態。您可能還需要透過新執行個體的管理主控台重新建立某些 IAM 身分中心設定。如需刪除 IAM 身分中心的指示，請參閱刪除您的 IAM 身分中心組態。

IAM 身分中心建立的 IAM 角色配額

IAM 身分中心會建立 IAM 角色，為使用者提供資源的權限。當您指派權限集時，IAM 身分中心會在每個帳戶中建立對應的 IAM 角色，並將權限集中指定的政策附加到這些角色。IAM Identity Center 會管理角色，並允許您找到的授權使用者擔任該角色，方法是使用 AWS 存取入口網站或。 AWS CLI當您修改權限集時，IAM 身分中心會確保相應地更新對應的 IAM 政策和角色。

如果您已在中設定 IAM 角色 AWS 帳戶，建議您檢查帳戶是否接近 IAM 角色的配額。每個帳戶的 IAM 角色預設配額為 1000 個角色。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詳細資訊，請參閱《Service Quotas 使用者指南》中的要求增加配額。

> **Note**
>
> 如果您正在查看已使用 IAM 身分中心的帳戶中的 IAM 角色，您可能會注意到開頭為的角色名稱“AWSReservedSSO_”。這些是 IAM 身分中心服務在帳戶中建立的角色，它們來自為帳戶指派權限集。

IAM 身分識別中心和 AWS Organizations

AWS Organizations 建議使用 (但不是必要) 與 IAM 身分中心搭配使用。如果您尚未設定組織，則不必這麼做。啟用 IAM 身分中心時，您將選擇是否使用啟用服務 AWS Organizations。當您設定組織時，設定 AWS 帳戶 組織的會成為組織的管理帳戶。的根使用者現在 AWS 帳戶 是組織管理帳戶的擁有者。 AWS 帳戶 您邀請加入組織的任何額外資訊都是成員帳戶。管理帳戶會建立管理成員帳號的組織資源、組織單位和策略。權限由管理帳戶委派給成員帳戶。

> **Note**
>
> 建議您啟用 IAM 身分中心 AWS Organizations，以便建立 IAM 身分中心的組織執行個體。我們建議使用組織執行個體的最佳做法，因為它支援 IAM Identity Center 的所有功能，並提供集中管理功能。如需詳細資訊，請參閱 管理 IAM 身分中心的組織和帳戶執行個體。

如果您已設定 AWS Organizations 並打算將 IAM 身分中心新增至組織，請確定已啟用所有 AWS Organizations 功能。當您建立組織時，根據預設會啟用所有功能。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 Identity Center，您必須以具有管理登入資料的使用者身 AWS Management Console 分或根使用者身分登入 AWS Organizations 管理帳戶來登入管理帳戶來登入 (除非沒有其他管理使用者，否則不建議使用)。使用 AWS Organizations 成員帳戶的管理登入資料登入時，無法啟用 IAM 身分中心。如需詳細資訊，請參閱《AWS Organizations 使用指南》中的〈建立和管理 AWS 組織〉。

在 IAM 身分中心確認您的身分來源

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。啟用 IAM 身分中心後，請確認您使用的是您選擇的身分來源。

確認您的身分來源

1. 開啟 IAM 身分中心主控台。
2. 在 [儀表板] 頁面的 [建議設定步驟] 區段下方，選擇 [確認您的身分識別來源]。您也可以選擇設定並選擇身分識別來源索引標籤來存取此頁面。
3. 如果您要保留指派的身分識別來源，則不會執行任何動作。如果您想要變更它，請選擇 [動作]，然後選擇 [變更身分識別來源]。

   您可以選擇下列其中一項作為身分識別來源：

   Identity Center 目錄

   首次啟用 IAM 身分中心時，系統會自動將身分識別中心目錄設定為預設身分識別來源。如果您尚未使用其他外部身分識別提供者，則可以開始建立使用者和群組，並將其存取層級指派給您 AWS 帳戶 和應用程式。如需使用此身分識別來源的自學課程，請參閱〈使用預設的 IAM 身分中心目錄設定使用者存取。

   Active Directory

   如果您已經使用 AWS Directory Service 或中的自我管理 AWS Managed Microsoft AD 目錄管理目錄中的使用者和群組Active Directory (AD)，建議您在啟用 IAM Identity Center 時連線該目錄。請勿在預設的身分識別中心目錄中建立任何使用者和群組。IAM 身分識別中心會使用提供的連線， AWS Directory Service 將使用者、群組和成員資格資訊從 Active Directory 中的來源目錄同步至 IAM 身分識別中心身分存放區。如需詳細資訊，請參閱 Connect 至目Microsoft AD 錄。

   > **Note**
   >
   > IAM 身分識別中心不支援以 Samba4 為基礎的 Simple AD 做為身分識別來源。

   外部識別提供者

   對於外部身分識別提供者 (IdPs) (例如Okta或)Microsoft Entra ID，您可以使用 IAM 身分中心 IdPs 透過安全性聲明標記語言 (SAML) 2.0 標準來驗證身分。SAML 通訊協定不提供查詢 IdP

以瞭解使用者和群組的方法。透過將這些使用者和群組佈建到 IAM 身分中心，讓 IAM 身分中心了解這些使用者和群組。如果您的 IdP 支援 SCIM，您可以使用跨網域身分識別管理系統 (SCIM) 2.0 通訊協定，將使用者和群組資訊從 IdP 自動佈建 (同步處理) 到 IAM 身分中心。否則，您可以在 IAM Identity Center 中手動輸入使用者名稱、電子郵件地址和群組，以手動佈建使用者和群組。

如需設定身分識別來源的詳細指示，請參閱入門教學課程。

> **Note**
>
> 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 身分識別中心) 會管理多因素驗證 (MFA) 設定。IAM 身分中心中的 MFA 不支援外部 IdPs使用。如需詳細資訊，請參閱 提示使用者輸入 MFA。

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。確認或變更身分識別來源後，您將建立或指定使用者，並將系統管理權限指派給您的 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 IAM 身分識別中心的一個身分來源中管理使用者和群組，變更為不同的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 中的管理使用者) 都將失去對其 AWS 帳戶 和應用程式的單一登入存取權。如需詳細資訊，請參閱 變更身分識別來源的考量。

設定身分識別來源後，您可以查詢使用者或群組，以授與他們對雲端應用程式的單一登入 AWS 帳戶存取權，或同時授與兩者。

入門教學課程

每個組織可以有一個身分識別來源，因此請務必花時間測試每個組織具有的功能。

在本節中，您可以選擇下列其中一個教學課程，以您偏好的身分識別來源設定 IAM Identity Center、建立管理使用者，以及設定權限集，讓使用者能夠存取資源。

在開始這些教學課程之前，請先啟用 IAM 身分中心。如需更多詳細資訊，請參閱 啟用 AWS IAM Identity Center。

主題

- 使用預設的 IAM 身分中心目錄設定使用者存取
- 使用作用中目錄做為身分識別來源
- Setting up SCIM provisioning between CyberArk and IAM Identity Center
- 使用和 IAM 身分識別中心設定 SAML Google Workspace 和 SCIM
- 使用 IAM 身分中心與您的JumpCloud目錄平台連線
- 使用和 IAM 身分識別中心設定 SAML Microsoft Entra ID 和 SCIM
- 使用和 IAM 身分識別中心設定 SAML Okta 和 SCIM
- 在OneLogin和 IAM 身分中心之間設定 SCIM 佈建
- 搭配 IAM 身分中心使用Ping Identity產品

使用預設的 IAM 身分中心目錄設定使用者存取

首次啟用 IAM 身分中心時，系統會自動將身分識別中心目錄設定為預設身分識別來源，因此您不需要選擇身分識別來源。如果您的組織使用其他身分識別提供者 (例如 AWS Directory Service for Microsoft Active DirectoryMicrosoft Entra ID、)，或Okta考慮將該身分識別來源與 IAM 身分中心整合，而不是使用預設組態。

目的

在本教學課程中，您將使用預設目錄做為身分識別來源，並設定和測試使用者存取。在此案例中，您可以在 IAM 身分中心管理所有使用者和群組。使用者透過 AWS 存取入口網站登入。本教學課程適用於剛使用 IAM 管理使用者和群組的使用者。 AWS 在接下來的步驟中，您將創建以下內容：

- 名為##沃爾夫的管理用戶

- 一個名為*####*的組
- 名為的權限集 *AdminAccess*

要驗證所有內容都是否正確創建，您將登錄並設置管理用戶的密碼。完成本教學課程後，您可以使用管理使用者在 IAM Identity Center 中新增更多使用者、建立其他權限集，以及設定組織對應用程式的存取權。

如果您尚未啟用 IAM 身分中心，請參閱啟用 AWS IAM Identity Center。

開始之前：

請執行下列任一項作業，以登入 AWS Management Console。

- 新使用者 AWS (root 使用者) — 選擇AWS 帳戶 root 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。在下一頁中，輸入您的密碼。
- 已在使用 AWS (IAM 登入資料) — 使用具有管理許可的 IAM 登入資料登入。

開啟 IAM 身分中心主控台。

步驟 1：新增使用者

1. 在 IAM 身分中心導覽窗格中，選擇 [使用者]，然後選取 [新增使用者]。
2. 在 [指定使用者詳細資訊] 頁面上，完成下列資訊：
   - 使用者名稱-在此自學課程中，輸入 *nikkiw*。

     建立使用者時，請選擇容易記住的使用者名稱。您的使用者必須記住使用者名稱才能登入 AWS 存取入口網站，而您之後無法變更。
   - 密碼-選擇「傳送電子郵件給此使用者，並附上密碼設定指示 (建議選項)」。

     此選項會向使用者傳送一封來自 Amazon Web Services 的電子郵件，其中包含主旨行邀請加入 IAM 身分中心 (AWS 單一登入的後續任務)。電子郵件來自no-reply@signin.aws或no-reply@login.awsapps.com。將這些電子郵件地址新增至核可的寄件人清單。
   - 電子郵件地址-輸入您可以接收電子郵件的使用者電子郵件地址。然後，再次輸入以確認它。每個使用者都必須有唯一的電子郵件地址。
   - 名字-輸入使用者的名字。對於本自學課程，請輸入 *Nikki*。
   - 姓氏-輸入使用者的姓氏。在此自學課程中，輸入 *Wolf*。

- 顯示名稱-預設值為使用者的名字和姓氏。如果您要變更顯示名稱，可以輸入不同的名稱。顯示名稱會顯示在登入入口網站和使用者清單中。
- 如有需要，請填寫選擇性資訊。在本教程中不使用它，您可以稍後進行更改。

3. 選擇下一步。這時系統顯示「向組添加用戶」頁面。我們要創建一個組來分配管理權限，而不是直接給他們 *Nikki*。

   選擇建立群組

   新的瀏覽器標籤隨即開啟，顯示 [建立群組] 頁面。

   a. 在群組詳細資料下的群組名稱中，輸入群組的名稱。我們建議使用可識別群組角色的群組名稱。在本教程中，請輸入####。
   b. 選擇建立群組
   c. 關閉「群組」瀏覽器標籤，以返回「新增使用者」瀏覽器標籤

4. 在「群組」區域中，選取「重新整理」按鈕。#####群組會顯示在清單中。

   選取 [####] 旁邊的核取方塊，然後選擇 [下一步]。

5. 在 [檢閱並新增使用者] 頁面上，確認下列事項：

   - 主要資訊會依您的預期顯示
   - 「組」顯示添加到您創建的組中的用戶

   如需變更，請選擇 Edit (編輯)。當所有詳細資料都正確時，選擇 [新增使用

   通知訊息會通知您已新增使用者。

接下來，您將為管理小組群#####權限，以便 *Nikki* 可以存取資源。

步驟 2：新增管理權限

1. 在「IAM 身分中心」導覽窗格的「多帳戶權限」下，選擇AWS 帳戶。
2. 在AWS 帳戶頁面上，組織結構會在階層中顯示您的組織，並在其下方顯示您的帳戶。選取管理帳戶的核取方塊，然後選取指派使用者或群組。
3. 指派使用者和群組工作流程隨即顯示。它由三個步驟組成：

   a. 對於步驟 1：選取使用者和群組，請選擇您建立的####群組。然後選擇下一步。

b. 針對步驟 2：選取權限集選擇 [建立權限集] 以開啟新索引標籤，引導您完成建立權限集所涉及的三個子步驟。

   i. 對於步驟 1：選取權限集類型，請完成下列步驟：

      - 在權限集類型中，選擇預先定義的權限集。
      - 在預先定義權限集的原則中，選擇AdministratorAccess。

      選擇下一步。

   ii. 針對 [步驟 2: 指定權限集詳細資料]、保留預設設定，然後選擇 [下一步]。

      預設設定會建立名為*AdministratorAccess*工作階段持續時間設為一小時的權限集。您可以在 [權限集名稱] 欄位中輸入新名稱，以變更權限集的名稱。

   iii. 對於步驟 3：檢閱和建立，請確認「權限集」類型是否使用 AWS 受管理的原則AdministratorAccess。選擇建立。在 [權限集] 頁面上會出現通知，通知您已建立權限集。您現在可以在 Web 瀏覽器中關閉此選項卡。

   在 [指派使用者和群組] 瀏覽器索引標籤上，您仍在執行 [步驟 2: 選取啟動建立權限集工作流程的權限集]。

   在「權限集」區域中，選擇「重新整理」按鈕。您建立的*AdministratorAccess*權限集會顯示在清單中。選取該權限集的核取方塊，然後選擇 [下一步]。

c. 在 [步驟 3：檢閱並提交指派] 頁面上，確認已選取*####*群組且已選取*AdministratorAccess*權限集，然後選擇 [提交]。

   頁面會更新並顯示正在設 AWS 帳戶 定您的訊息。等待，直到該過程完成。

   您將返回到該 AWS 帳戶 頁面。通知訊息會通知您已重新佈建，且 AWS 帳戶 已套用更新的權限集。

> **恭喜您！**
>
> 您已成功設定第一個使用者、群組和權限集。

在本教程的下一部分，您將通過登錄到訪問門戶與他們*##################*的 AWS 訪問。立即登出主控台。

步驟 3：測試使用者存取許可

現在 *Nikki Wolf* 是組織中的使用者，他們可以登入並根據其權限集存取被授與權限的資源。要驗證用戶是否正確配置，在下一步中，您將使用 *Nikki #*憑據登錄並設置其密碼。當您在步驟 1 中添加用戶 *Nikki #*時，您選擇了讓 *Nikki* 收到帶有密碼設置說明的電子郵件。現在是時候打開該電子郵件並執行以下操作：

1. 在電子郵件中，選取 [接受邀請] 連結以接受邀請。

   > **Note**
   >
   > 該電子郵件還包括 *Nikki #*用戶名以及用於登錄組織的 AWS 訪問門戶網站 URL。記錄此信息以備 future 使用。

   您將被帶到新用戶註冊頁面，您可以在其中設置 *Nikki #*密碼。
2. 設置 N *ikki #*密碼後，您將導航到登錄頁面。輸入 ***nikkiw*** 並選擇下一步，然後輸入 ***Nikki #***密碼並選擇登錄。
3. AWS 存取入口網站隨即開啟，顯示您可以存取的組織和應用程式。

   選取組織以將其展開至清單， AWS 帳戶 然後選取帳號以顯示可用來存取帳號資源的角色。

   每個權限集都有兩種您可以使用的管理方法：角色或存取金鑰。

   - 角色，例如 *AdministratorAccess*-開啟 AWS Console Home。
   - 存取金鑰-提供可與 AWS CLI 或和 AWS SDK 搭配使用的認證。包括使用自動重新整理的短期登入資料或短期存取金鑰的資訊。如需詳細資訊，請參閱 取得 AWS CLI 或 AWS SDK 的 IAM 身分中心使用者登入資料。
4. 選擇要登入的「角色」連結 AWS Console Home。

您已登入並導覽至 AWS Console Home 頁面。探索主控台並確認您擁有預期的存取權。

後續步驟

現在您已經在 IAM 身分中心建立了管理使用者，您可以：

- 分配應用
- 新增其他使用者

- 將使用者指派至帳號
- 設定其他權限集

> **Note**
>
> 您可以將多個權限集指派給相同的使用者。若要遵循套用最低權限權限的最佳作法，請在建立系統管理使用者之後，建立更嚴格的權限集，並將其指派給相同的使用者。如此一來，您就可以只使 AWS 帳戶 用您需要的權限來存取您的權限，而非系統管理權限。

在您的使用者接受啟用其帳戶的邀請並登入 AWS 存取入口網站後，入口網站中出現的唯一項目僅適用於指派給他們的 AWS 帳戶、角色和應用程式。

> **Important**
>
> 強烈建議您為使用者啟用多因素驗證 (MFA)。如需更多詳細資訊，請參閱 身分識別中心使用者的多因素驗證。

使用作用中目錄做為身分識別來源

如果您要使用目錄AWS Directory Service或 Active AWS Managed Microsoft AD Directory (AD) 中的自我管理目錄中的使用者，您可以變更 IAM 身分中心身分識別來源，以便與這些使用者搭配使用。我們建議您在啟用 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。

若要使用 Active Directory 做為您的身分識別來源，您的組態必須符合下列先決條件：

- 如果您使用的是AWS Managed Microsoft AD，您必須在設定AWS Managed Microsoft AD目錄的相同AWS 區域位置啟用 IAM 身分中心。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。此外，請注意，AWS存取入口網站使用與您的目錄相同的存取 URL。
- 使用位於管理帳戶中的活動目錄：

  您必須在中設定現有的 AD Connector 或AWS Managed Microsoft AD目錄AWS Directory Service，而且必須位於您的AWS Organizations管理帳戶中。您一次只能連線一個 AD Connector 目錄或

一個目錄。AWS Managed Microsoft AD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：

- 將目錄 Connect AWS Managed Microsoft AD 到 IAM 身分中心
- Connect 作用中目錄中的自我管理目錄連線至 IAM 身分識別中心

- 使用位於委派系統管理員帳戶中的作用中目錄：

  如果您計劃啟用 IAM 身分中心委派管理員，並使用 Active Directory 做為您的 IAM 身分中心身分識別來源，則可以使用現有的 AD Connector 或AWS Managed Microsoft AD目錄設定在委派管理員帳戶中的AWS目錄。

  如果您決定將 IAM 身分中心身分識別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，它必須位於管理帳戶中。

本教學課程會引導您完成使用 Active Directory 做為身分識別中心身分識別來源的基本設定。

步驟 1：Connect 活動目錄並指定用戶

如果您已經在使用 Active Directory，下列主題將協助您準備將目錄連線到 IAM 身分識別中心。

> **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。如果您計劃在 Active AWS Managed Microsoft AD Directory 中連線目錄或自我管理的目錄，但並未搭配使用 RADIUS MFAAWS Directory Service，請在 IAM 身分中心啟用 MFA。

AWS Managed Microsoft AD

1. 檢閱中的指引Connect 至目Microsoft AD錄。
2. 請遵循 將目錄 Connect AWS Managed Microsoft AD 到 IAM 身分中心 中的步驟。
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。

活動目錄中的自我管理目錄

1. 檢閱中的指引Connect 至目Microsoft AD錄。

2. 請遵循 Connect 作用中目錄中的自我管理目錄連線至 IAM 身分識別中心 中的步驟。
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。

步驟 2：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. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上選擇 [身分識別來源] 索引標籤，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] 索引標籤，然後選擇 [新增使用者和群組]。
5. 在 [使用者] 索引標籤的 [使用者] 底下，輸入確切的使用者名稱，然後選
6. 在新增的使用者和群組下，執行下列操作：
   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. 選擇提交。
7. 在 [管理同步] 頁面中，您指定的使用者會出現在 [同步範圍內的使用者] 清單中。
8. 在導覽窗格中，選擇使用者 。
9. 在 [使用者] 頁面上，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。如需詳細資訊，請參閱 建立許可集合。

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM 身分中心支援從 CyberArk Directory Platform IAM 身分識別中心自動佈建 (同步) 使用者資訊。此佈建使用系統進行跨網域身分識別管理 (SCIM) 2.0 通訊協定。您可以在CyberArk使用 IAM 身分中心 SCIM 端點和存取權杖中設定此連線。設定 SCIM 同步時，您可CyberArk以在中建立使用者屬性與 IAM 身分中心中指定屬性的對應。這會導致 IAM 身分中心和CyberArk.

本指南以截至 2021 年 8 月CyberArk為止。較新版本的步驟可能會有所不同。本指南包含一些有關透過 SAML 設定使用者驗證的注意事項。

> **Note**
>
> 在開始部署 SCIM 之前，建議您先檢閱. 使用自動佈建的考量 然後繼續檢閱下一節中的其他考量。

主題

必要條件

在開始之前，您將需要以下內容：

- CyberArk訂閱或免費試用。註冊免費試用訪問CyberArk。
- 已啟用 IAM 身分中心的帳戶 (免費)。如需詳細資訊，請參閱啟用 IAM 身分中心。
- 從您的CyberArk帳戶到 IAM 身分中心的 SAML 連線，如 IAM 身分中心的說明CyberArk文件所述。
- 將 IAM 身分中心連接器與您要允許存取的角色、使用者和組織建立關聯 AWS 帳戶。

SCIM 考量

以下是使用 IAM 身分中心CyberArk聯合時的考量事項：

- 只有在應用程式佈建區段中對應的角色才會同步至 IAM 身分中心。
- 佈建指令碼僅在預設狀態下受支援，一旦變更，SCIM 佈建可能會失敗。
  - 只能同步一個電話號碼屬性，預設值為「公司電話」。
- 如果 CyberArk IAM 身分中心應用程式中的角色對應發生變更，預期會出現下列行為：

  - 如果角色名稱已變更，則 IAM 身分中心中的群組名稱不會變更。
  - 如果群組名稱已變更-將在 IAM 身分中心建立新群組，舊群組將保留，但不會有成員。
- 您可以從 CyberArk IAM Identity Center 應用程式設定使用者同步處理和取消佈建行為，確保您為組織設定正確的行為。這些是您可以選擇的選項：
  - 以相同的主參與者名稱覆寫 (或不) Identity Center 目錄中的使用者。
  - 從CyberArk角色中移除使用者時，從 IAM 身分中心取消佈建使用者。
  - 取消佈建使用者行為-停用或刪除。

步驟 1：在 IAM 身分中心啟用佈建

在第一個步驟中，您可以使用 IAM 身分中心主控台啟用自動佈建。

在 IAM 身分中心啟用自動佈建

1. 完成必要條件後，請開啟 IAM 身分中心主控台。
2. 在左側導覽窗格中選擇 [設定]。
3. 在 [設定] 頁面上，找出 [自動佈建資訊] 方塊，然後選擇 [啟用]。這會立即在 IAM 身分中心啟用自動佈建，並顯示必要的 SCIM 端點和存取權杖資訊。
4. 在「輸入自動佈建」對話方塊中，複製下列選項的每個值。稍後在 IdP 中配置佈建時，您將需要貼上這些內容。
   a. SCIM 端點
   b. 訪問令牌
5. 選擇關閉。

現在您已在 IAM 身分中心主控台中設定佈建，您需要使用 CyberArk IAM 身分中心應用程式完成剩餘的工作。這些步驟將在下列程序中說明。

步驟 2：配置佈建 CyberArk

使用 CyberArk IAM 身分中心應用程式中的下列程序，以啟用 IAM 身分中心進行佈建。此程序假設您已將 CyberArk IAM 身分中心應用程式新增至 Web 應用程式下的CyberArk管理主控台。如果您尚未這麼做，請參閱必要條件，然後完成此程序以設定 SCIM 佈建。

若要在中設定佈建 CyberArk

1. 開啟您在設定 SAML CyberArk (應用程式 > Web 應用程式) 時新增的 CyberArk IAM 身分中心應用程式。請參閱 必要條件。
2. 選擇 IAM 身分中心應用程式，然後移至佈建區段。
3. 核取「啟用此應用程式的佈建」方塊，然後選擇「即時模式」。
4. 在先前的程序中，您會從 IAM 身分中心複製 SCIM 端點值。將該值貼到「SCIM 服務 URL」欄位中，在 CyberArk IAM 身分中心應用程式中，將「授權類型」設定為「授權標頭」。確保您刪除了 URL 末尾的正斜線。
5. 將「標頭類型」設定為「承載權杖」。
6. 在上一個程序中，您將存取權杖值複製到 IAM 身分中心。將該值貼到 CyberArk IAM 身分中心應用程式的「承載權杖」欄位中。
7. 按一下驗證以測試並套用組態。
8. 在「同步選項」下，選擇您希望輸出佈建起作用的CyberArk正確行為。您可以選擇覆寫 (或不使用) 具有類似主體名稱和取消佈建行為的現有 IAM Identity Center 使用者。
9. 在「角色對應」下，設定從CyberArk角色的對應，位於目的地群組下的「名稱」欄位至 IAM 身分中心群組。
10. 完成後，請單擊底部的「保存」。
11. 若要驗證使用者是否已成功同步至 IAM 身分中心，請返回 IAM 身分中心主控台，然後選擇 [使用者]。同步處理的使用者CyberArk將顯示在 [使用者] 頁面上。這些使用者現在可以指派給帳戶，並且可以在 IAM 身分中心內連線。

(選擇性) 步驟 3：在 IAM 身分中設CyberArk定存取控制 (ABAC) 的使用者屬性

如果您選擇為 CyberArk IAM 身分中心設定屬性以管理 AWS 資源存取權，則此為選用程序。您在中定義的屬性CyberArk會在 SAML 宣告中傳遞至 IAM 身分中心。然後，您可以在 IAM 身分中心建立權限集，以根據傳遞的屬性來管理存取權CyberArk。

開始此程序之前，您必須先啟用此存取控制的屬性功能。如需如何進行該服務的詳細資訊，請參閱啟用和設定存取控制的屬性。

在CyberArk中設定 IAM 身分中心存取控制的使用者屬性

1. 開啟您在設定 SAML CyberArk (應用程式 > Web 應用程式) 時所安裝的 CyberArk IAM 身分中心應用程式。
2. 移至「S AML 回應」選項。
3. 在「屬性」(Attributes) 下，將相關屬性新增至下列邏輯的表格中：

   a. 屬性名稱是起始的原始屬性名稱CyberArk。

   b. 屬性值是在 SAML 宣告中傳送至 IAM 身分中心的屬性名稱。
4. 選擇 儲存。

(選擇性) 傳遞屬性以進行存取控制

您可以選擇性地使用 IAM 身分中心中的存取控制的屬性功能來傳遞Name屬性設定為的Attribute元素https://aws.amazon.com/SAML/Attributes/AccessControl:**{TagKey}**。此元素可讓您在 SAML 聲明中將屬性做為工作階段標籤傳遞。如需工作階段標籤的詳細資訊，請參閱 IAM 使用者指南 AWS STS中的「傳遞工作階段標籤」。

若要將屬性做為工作階段標籤傳遞，請包含指定標籤值的 AttributeValue 元素。例如，若要傳遞標籤鍵值配對CostCenter = blue，請使用下列屬性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要新增多個屬性，請為每個標籤包含單獨的Attribute元素。

使用和 IAM 身分識別中心設定 SAML Google Workspace 和 SCIM

如果您的組織正在使用，Google Workspace您可以將使用者和群組從 IAM 身分中心整合Google Workspace到 IAM 身分中心，讓他們能夠存取 AWS 資源。您可以將 IAM 身分中心身分來源從預設的 IAM 身分中心身分識別來源變更為，以達成此整合Google Workspace。

使用跨網域身分識別管理系統 (SCIM) 2.0 通訊協定，將來Google Workspace自的使用者資訊同步至 IAM 身分中心。您可以在Google Workspace使用適用於 IAM 身分中心的 SCIM 端點和 IAM 身分中心

承載權杖中設定此連線。設定 SCIM 同步時，您可Google Workspace以在中建立使用者屬性與 IAM 身分中心中指定屬性的對應。此對應符合 IAM 身分中心和Google Workspace. 若要這麼做，您需要設定Google Workspace為 IAM 身分提供者和 IAM 身分中心身分識別提供者。

目的

本教學課程中的步驟有助於引導您在Google Workspace和 AWS之間建立 SAML 連線。稍後，您將使用者從Google Workspace使用 SCIM 同步處理。若要驗證所有項目的設定是否正確，在完成設定步驟後，您將以Google Workspace使用者身分登入並驗證 AWS 資源的存取權。請注意，本教程是基於一個小型Google Workspace目錄測試環境。不包括群組和組織單位等目錄結構。完成本教學課程後，您的使用者將能夠使用您的Google Workspace認證 AWS 存取入口網站。

> **Note**
>
> 要註冊免費試用Google Workspace訪問Google Workspace網Google's站。
> 如果您尚未啟用 IAM 身分中心，請參閱啟用 AWS IAM Identity Center。

考量事項

- 在設定Google Workspace和 IAM 身分中心之間的 SCIM 佈建之前，我們建議您先檢閱使用自動佈建的考量。
- SCIM 自動同步處理目前Google Workspace僅限於使用者佈建。目前不支援自動群組佈建。您可以使用 AWS CLI 身分識別存放區建立群組命令或 AWS Identity and Access Management (IAM) API 手動建立群組。CreateGroup或者，您也可以使用 ssosync 將使用Google Workspace者和群組同步到 IAM 身分中心。
- 每個Google Workspace使用者都必須指定「名字」、「姓氏」、「使用者名稱」和「顯示名稱」值。
- 每個Google Workspace使用者的每個資料屬性只有一個值，例如電子郵件地址或電話號碼。任何具有多個值的使用者將無法同步處理。如果使用者的屬性中有多個值，請先移除重複的屬性，然後再嘗試在 IAM 身分中心佈建使用者。例如，只能同步一個電話號碼屬性，因為預設的電話號碼屬性是「工作電話」，因此即使使用者的電話號碼是住家電話或行動電話，也可以使用「工作電話」屬性來儲存使用者的電話號碼。
- 如果在 IAM 身分中心中停用使用者，但在中仍處於作用中，屬性仍然會同步Google Workspace。
- 如果 Identity Center 目錄中存在具有相同使用者名稱和電子郵件的現有使用者，則會使用 SCIM 從Google Workspace中覆寫該使用者並同步處理該使用者。

- 變更身分識別來源時，還有其他考量事項。如需詳細資訊，請參閱 the section called “從 IAM 身分中心變更為外部 IdP”。

步驟 1Google Workspace：設定 SAML 應用程式

1. 使用具有超級Google管理員權限的帳戶登入管理控制台。
2. 在Google管理控制台的左側導覽面板中，選擇 [應用程式]，然後選擇 [Web 和行動應用程式]。
3. 在新增應用程式下拉式清單中，選取 [搜尋應用程式]。
4. 在搜尋方塊中輸入 Amazon Web Services，然後從清單中選取 Amazon Web Services (SAML) 應用程式。
5. 在Google身分識別提供者詳細資訊-Amazon Web Services 頁面上，您可以執行下列任一項作業：

   a. 下載 IdP 中繼資料。

   b. 複製 SSO URL、實體 ID URL 和憑證資訊。

   在步驟 2 中，您將需要 XML 檔案或 URL 資訊。
6. 在移至Google管理主控台的下一個步驟之前，請將此頁面保持開啟狀態，然後移至 IAM 身分中心主控台。

步驟 2：IAM 身分中心和Google Workspace：變更 IAM 身分中心身分來源，並設定Google Workspace為 SAML 身分識別提供者

1. 使用具有管理權限的角色登入 IAM 身分中心主控台。
2. 在左側導覽窗格中選擇 [設定]。
3. 在 [設定] 頁面上，選擇 [動作]，然後選擇 [變更身分識別來源]。

   - 如果您尚未啟用 IAM 身分中心，請參閱以取得啟用 IAM 身分識別中心詳細資訊。首次啟用和存取 IAM 身分中心後，您將到達儀表板，您可以在其中選取 [選擇您的身分來源]。
4. 在 [選擇身分識別來源] 頁面上，選取 [外部身分識別提供者]，然後選擇 [下
5. 將開啟 [設定外部身分識別提供者] 頁 要完成此頁面和步驟 1 中的Google Workspace頁面，您需要完成以下操作：

   - 在 IAM 身分中心主控台的身分識別提供者中繼資料區段下，您需要執行下列任一項作業：

     i. 在 IAM 身分中心主控台中，將 GoogleSAML 中繼資料做為 IdP SAML 中繼資料上傳。

ii. 將 GoogleSSO URL 複製並粘貼到 IdP 登錄 URL 字段中，將簽Google發者 URL 複製並粘貼到 IdP 頒發者 URL 字段中，然後將Google證書作為 Id P 證書上傳。

6. 在 IAM 身分中心主控台的 [身分提供者中繼資料] 區段中提供中繼資料後，請複製AWS 存取入口網站登入 URL、IAM 身分宣告消費者服務 (ACS) URL 和 IAM 身分中心簽發者 URL。Google您需要在下一個步驟中在Google管理控制台中提供這些 URL。
7. 使用 IAM 身分中心主控台保持頁面開啟狀態，然後返回Google管理主控台。您應該在 Amazon Web Services-服務提供商詳細信息頁面上。選取繼續。
8. 在服務提供者詳細資料頁面上，輸入 ACS URL、實體 ID 和起始 URL 值。您在上一個步驟中複製了這些值，可以在 IAM 身分中心主控台中找到這些值。

   - 將 IAM 身分中心宣告用戶服務 (ACS) URL 貼到 ACS URL 欄位
   - 將 IAM 身分中心簽發者 URL 貼到「實體 ID」欄位中。
   - 將AWS 存取入口網站登入 URL 貼到 [開始 URL] 欄位中。

9. 在 [服務提供者詳細資料] 頁面上，依下列方式完成 [名稱 ID] 下的欄位：

   - 對於名稱 ID 格式，選取電子郵件
   - 針對名稱 ID，選取基本資訊 > 主要電子郵件

10. 選擇繼續。
11. 在 [屬性對應] 頁面的 [屬性] 底下，選擇 [新增對應]，然後在 [Google目錄屬性] 底下設定這些欄位：

    - 對於`https://aws.amazon.com/SAML/Attributes/RoleSessionName`應用程序屬性，從Google Directory屬性中選擇字段基本信息，主要電子郵件。
    - 針對`https://aws.amazon.com/SAML/Attributes/Role`應用程式屬性，選取任何Google Directory屬性。Google目錄屬性可以是部門。

12. 選擇完成
13. 返回 IAM 身分中心主控台，然後選擇 [下一步]。在 [檢閱並確認] 頁面上，檢閱資訊，然後在提供的空格中輸入 AC CEPT。選擇 [變更識別來源]。

您現在可以在中啟用 Amazon Web Services 應用程式，以Google Workspace便將您的使用者佈建到 IAM 身分中心。

步驟 3Google Workspace：啟用應用

1. 返回Google管理控制台和您的應用程序，該 AWS IAM Identity Center 應用程序可在應用程序和 Web 和移動應用程序下找到。
2. 在「使用者存取」旁的「使用者存取」面板中，選擇向下箭頭以展開「使用者存取權」以顯示「服務狀態」面板。
3. 在 [服務狀態] 面板中，為所有人選擇 [開啟]，然後選擇 [儲存]。

> **Note**
>
> 為了協助維護最低權限的原則，我們建議您在完成本教學課程後，將所有人的 [服務] 狀態變更為 [關閉]。只有需要存取權的使用者才 AWS 應啟用服務。您可以使用Google Workspace群組或組織單位授與使用者存取特定子集的使用者。

步驟 4：IAM 身分中心：設定 IAM 身分中心自動佈建

1. 返回 IAM 身分中心主控台。
2. 在 [設定] 頁面上，找出 [自動佈建資訊] 方塊，然後選擇 [啟用]。這會立即在 IAM 身分中心啟用自動佈建，並顯示必要的 SCIM 端點和存取權杖資訊。
3. 在「輸入自動佈建」對話方塊中，複製下列選項的每個值。在本教學課程的步驟 5 中，您將輸入這些值以在中配置自動佈建Google Workspace。

   - SCIM 端點
   - 訪問令牌

   > **Warning**
   >
   > 這是您唯一可以取得 SCIM 端點和存取權杖的時間。請務必先複製這些值，然後再繼續前進。

4. 選擇關閉。

現在您已在 IAM 身分中心主控台中設定佈建，在下一個步驟中，您將在中設定 auto 佈建Google Workspace。

步驟 5Google Workspace：設定 auto 佈建

1. 返回Google管理控制台，您可以在 AWS IAM Identity Center 應用程式和 Web 和行動應用程式下找到您的應用程式。在「自動啟動設定」段落中，選擇設定自動佈建。
2. 在上一個程序中，您會在 IAM 身分中心主控台中複製存取權杖值。將該值粘貼到訪問令牌字段中，然後選擇繼續。此外，在先前的程序中，您會複製 IAM 身分中心主控台中的 SCIM 端點值。將該值貼到「端點 URL」欄位中。請確定您移除 URL 結尾的正斜線，然後選擇 [繼續]。
3. 確認所有強制性 IAM 身分中心屬性 (標有 * 的屬性) 都對應至Google Cloud Directory屬性。如果不是，請選擇向下箭頭並對映至適當的屬性。選擇繼續。
4. 在佈建範圍區段中，您可以選擇包含Google Workspace目錄的群組，以提供對 Amazon Web Services 應用程式的存取權。略過此步驟，然後選取 [繼續]。
5. 在取消佈建段落中，您可以選擇如何回應移除使用者存取權的不同事件。對於每種情況，您可以指定在取消佈建開始之前的時間長度：

   - 24 小時內
   - 一天后
   - 七天后
   - 使用三十天后

   每種情況都有一個時間設置，用於何時暫停帳戶的訪問以及何時刪除帳戶。

   > **Tip**
   >
   > 刪除使用者帳戶之前，請務必設定多於暫停使用者帳戶的時間。

6. 選擇 Finish (完成)。您將返回 Amazon Web Services 應用程序頁面。
7. 在「自動佈建」區段中，開啟切換開關，將其從「非作用中」變更為「作用中」。

   > **Note**
   >
   > 如果未為使用者開啟 IAM 身分中心，則會停用啟用滑桿。選擇 [使用者存取權限]，然後開啟應用程式以啟用滑桿。

8. 在確認對話方塊中，選擇「開啟」。
9. 若要確認使用者已成功同步至 IAM 身分中心，請返回 IAM 身分中心主控台，然後選擇 [使用者]。[使用者] 頁面會列出由 SCIM 建立的Google Workspace目錄中的使用者。如果尚未列出使用者，

則可能是佈建仍在進行中。佈建最多可能需要 24 小時，但在大多數情況下，佈建可能會在幾分鐘內完成。確保每隔幾分鐘刷新一次瀏覽器窗口。

選取使用者並檢視其詳細資訊。這些資訊應與目Google Workspace錄中的資訊相符。

> **恭喜您！**
>
> 您已成功設定Google Workspace和之間的 SAML 連線，並 AWS 且已驗證自動佈建正在運作。您現在可以在 IAM 身分中將這些使用者指派給帳戶和應用程式。在本教學課程中，在下一個步驟中，讓我們將其中一位使用者授與管理帳戶的管理權限，指定其中一位使用者為 IAM Identity Center 管理員。

步驟 6：IAM 身分中心：授與Google Workspace使用者帳戶存取權

1. 返回 IAM 身分中心主控台。在「IAM 身分中心」導覽窗格的「多帳戶權限」下，選擇AWS 帳戶。
2. 在AWS 帳戶頁面上，組織結構會在階層中顯示您的組織根目錄，並在其下方顯示您的帳戶。選取管理帳戶的核取方塊，然後選取 [指派使用者或群組]。
3. 指派使用者和群組工作流程隨即顯示。它由三個步驟組成：

   a. 對於步驟 1：選取使用者和群組，請選擇要執行管理員工作職能的使用者。然後選擇下一步。

   b. 針對步驟 2：選取權限集選擇 [建立權限集] 以開啟新索引標籤，逐步引導您完成建立權限集所涉及的三個子步驟。

      i. 對於步驟 1：選取權限集類型，請完成下列步驟：

         - 在 [權限集類型] 中，選擇 [預先定義的權限集
         - 在預先定義權限集的原則中，選擇AdministratorAccess。

         選擇下一步。

      ii. 針對 [步驟 2: 指定權限集詳細資料]、保留預設設定，然後選擇 [下一步]。

         預設設定會建立名為*AdministratorAccess*工作階段持續時間設定為一小時的權限集。

      iii. 對於步驟 3：檢閱和建立，請確認「權限集」類型是否使用 AWS 受管理的原則AdministratorAccess。選擇建立。在 [權限集] 頁面上會出現通知，通知您已建立權限集。您現在可以在 Web 瀏覽器中關閉此選項卡。

iv. 在 [指派使用者和群組] 瀏覽器索引標籤上，您仍在執行 [步驟 2: 選取啟動建立權限集工作流程的權限集] 中。

v. 在「權限集」區域中，選擇「重新整理」按鈕。您建立的*AdministratorAccess*權限集會顯示在清單中。選取該權限集的核取方塊，然後選擇 [下一步]。

c. 對於步驟 3：檢閱並提交檢閱選取的使用者和權限集，然後選擇 [提交]。

頁面會更新並顯示正在設 AWS 帳戶 定您的訊息。等待，直到該過程完成。

您將返回到該 AWS 帳戶 頁面。通知訊息會通知您已重新佈建，且 AWS 帳戶 已套用更新的權限集。當用戶登錄時，他們將有選擇*AdministratorAccess*角色的選項。

> **Note**
>
> SCIM 自動同步處理Google Workspace僅支援佈建使用者。目前不支援自動群組佈建。您無法使用建立使用Google Workspace者群組 AWS Management Console。佈建使用者後，您可以使用 AWS CLI 身分識別存放區建立群組命令或 IAM API 建立群組。CreateGroup

步驟 7Google Workspace：確認Google Workspace使用者存取 AWS 資源

1. 使用測試Google使用者帳戶登入。若要瞭解如何將使用者新增至Google Workspace，請參閱Google Workspace文件。
2. 選擇Google apps啟動器（華夫餅乾）圖標。
3. 捲動至 App 清單底部的自訂應Google Workspace用程式所在位置。顯示兩個應用程序 Amazon Web Services 和AWS 訪問門戶網站。
4. 選AWS 取存取入口網站應用程式。您已登入入口網站，可以看到 AWS 帳戶 圖示。展開該圖示以查看使用者可以存取的 AWS 帳戶 清單。在本教程中，您只使用一個帳戶，因此展開圖標僅顯示一個帳戶。

> **Note**
>
> 如果您選取 Amazon Web Services 應用程式，您將收到 SAML 錯誤訊息。該應用程式適用於已佈建為 IAM 使用Google Workspace者的使用者，本教學課程會在 IAM 身分中將您Google Workspace的使用者佈建為使用者。

5. 選取帳戶以顯示使用者可用的權限集。在本教學課程中，您建立了AdministratorAccess權限集。

6. 權限集旁邊是該權限集可用存取類型的連結。建立權限集時，您已指定同時啟用管理主控台和程式設計存取，因此會出現這兩個選項。選取管理主控台以開啟 AWS Management Console。
7. 使用者已登入主控台。

(選擇性) 傳遞屬性以進行存取控制

您可以選擇性地使用 IAM 身分中心中的存取控制的屬性功能來傳遞Name屬性設定為的Attribute元素https://aws.amazon.com/SAML/Attributes/AccessControl:**{TagKey}**。此元素可讓您在 SAML 聲明中將屬性做為工作階段標籤傳遞。如需工作階段標籤的詳細資訊，請參閱 IAM 使用者指南 AWS STS中的「傳遞工作階段標籤」。

若要將屬性做為工作階段標籤傳遞，請包含指定標籤值的 AttributeValue 元素。例如，若要傳遞標籤鍵值配對CostCenter = blue，請使用下列屬性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要新增多個屬性，請為每個標籤包含單獨的Attribute元素。

後續步驟

現在，您已在 IAM 身分中心設定Google Workspace為身分識別提供者並佈建使用者，您可以：

- 使用 AWS CLI 身分識別存放區建立群組命令或 IAM API 為CreateGroup您的使用者建立群組。

  將存取權指派給 AWS 帳戶 和應用程式時，群組非常有用。您可以將權限授予群組，而不是個別指派每個使用者。稍後，當您從群組中新增或移除使用者時，使用者會動態取得或失去指派給群組之帳戶和應用程式的存取權。
- 根據工作職能設定權限，請參閱建立權限集。

  權限集定義了使用者和群組對的存取層級 AWS 帳戶。權限集會儲存在 IAM 身分中心，並且可以佈建至一或多個 AWS 帳戶。您可以為使用者指派多個許可集合。

> **Note**
>
> 身為 IAM 身分中心管理員，您偶爾需要以較新的 IdP 憑證取代較舊的憑證。例如，當憑證的到期日臨近時，您可能需要取代 IdP 憑證。以較新的憑證取代舊憑證的程序稱為憑證輪替。請務必檢閱如何管理的 SAML 憑證Google Workspace。

使用 IAM 身分中心與您的JumpCloud目錄平台連線

IAM 身分中心支援將使用者資訊從JumpCloud目錄平台自動佈建 (同步處理) 到 IAM 身分中心。此佈建使用系統進行跨網域身分識別管理 (SCIM) 2.0 通訊協定。您可以在JumpCloud使用 IAM 身分中心 SCIM 端點和存取權杖中設定此連線。設定 SCIM 同步時，您可JumpCloud以在中建立使用者屬性與 IAM 身分中心中指定屬性的對應。這會導致 IAM 身分中心和JumpCloud.

本指南以截至 2021 年 6 月JumpCloud為止。較新版本的步驟可能會有所不同。本指南包含一些有關透過 SAML 設定使用者驗證的注意事項。

下列步驟將逐步說明如何使用 SCIM 通訊協定啟用從 JumpCloud IAM 身分中心自動佈建使用者和群組。

> **Note**
>
> 在開始部署 SCIM 之前，建議您先檢閱. 使用自動佈建的考量 然後繼續檢閱下一節中的其他考量。

主題

必要條件

在開始之前，您將需要以下內容：

- JumpCloud訂閱或免費試用。註冊免費試用訪問JumpCloud。
- 已啟用 IAM 身分中心的帳戶 (免費)。如需詳細資訊，請參閱啟用 IAM 身分中心。
- 從您的JumpCloud帳戶到 IAM 身分中心的 SAML 連線，如 IAM 身分中心的說明JumpCloud文件所述。
- 將 IAM 身分中心連接器與您要允許存取AWS帳戶的群組建立關聯。

SCIM 考量

以下是將JumpCloud聯合用於 IAM 身分中心時的考量事項。

- 只有與中的「AWS單一登入」連接器相關聯的群組才JumpCloud會與 SCIM 同步處理。
- 只能同步一個電話號碼屬性，預設值為「公司電話」。
- JumpCloud目錄中的使用者必須將名字和姓氏設定為透過 SCIM 同步至 IAM 身分中心。
- 如果 IAM 身分中心中的使用者已停用，但仍在中啟用，則屬性仍會同步JumpCloud。
- 您可以取消勾選連接器中的 [啟用使用者群組和群組成員資格的管理]，選擇僅針對使用者資訊啟用 SCIM 同步。
- 如果 Identity Center 目錄中有具有相同使用者名稱和電子郵件的現有使用者，則會覆寫該使用者並與來自JumpCloud的 SCIM 同步處理。

步驟 1：在 IAM 身分中心啟用佈建

在第一個步驟中，您可以使用 IAM 身分中心主控台啟用自動佈建。

在 IAM 身分中心啟用自動佈建

1. 完成必要條件後，請開啟 IAM 身分中心主控台。
2. 在左側導覽窗格中選擇 [設定]。
3. 在 [設定] 頁面上，找出 [自動佈建資訊] 方塊，然後選擇 [啟用]。這會立即在 IAM 身分中心啟用自動佈建，並顯示必要的 SCIM 端點和存取權杖資訊。
4. 在「輸入自動佈建」對話方塊中，複製下列選項的每個值。稍後在 IdP 中配置佈建時，您將需要貼上這些內容。
   a. SCIM 端點
   b. 訪問令牌
5. 選擇關閉。

現在您已在 IAM 身分中心主控台中設定佈建，您需要使用 JumpCloud IAM 身分中心連接器完成剩餘的工作。下列程序將說明這些步驟。

步驟 2：配置佈建 JumpCloud

使用 JumpCloud IAM 身分中心連接器中的下列程序，以啟用 IAM 身分中心進行佈建。此程序假設您已將 JumpCloud IAM 身分中心連接器新增至JumpCloud管理入口網站和群組。如果您尚未這麼做，請參閱必要條件，然後完成此程序以設定 SCIM 佈建。

若要在中設定佈建 JumpCloud

1. 開啟您在為 JumpCloud (使用者身份驗證 > JumpCloud IAM 身分中心) 設定 SAML 時安裝的 IAM 身分中心連接器。請參閱 必要條件。
2. 選擇 IAM 身分中心連接器，然後選擇第三個索引標籤身分管理。
3. 如果您想要群組進行 SCIM 同步，請核取此應用程式中啟用使用者群組和群組成員資格管理的核取方塊。
4. 點擊配置。
5. 在先前的程序中，您會在 IAM 身分中心複製 SCIM 端點值。將該值貼到 JumpCloud IAM 身分中心連接器的「基本 URL」欄位中。確保刪除 URL 末尾的正斜線。
6. 在上一個程序中，您將存取權杖值複製到 IAM 身分中心。將該值貼到 JumpCloud IAM 身分中心連接器的 [權杖金鑰] 欄位中。
7. 按一下啟用以套用組態。
8. 確定您已啟動單一登入旁邊有綠色指示燈。
9. 移至第四個索引標籤使用者群組，並勾選您要使用 SCIM 佈建的群組。
10. 完成後，請單擊底部的「保存」。
11. 若要驗證使用者是否已成功同步至 IAM 身分中心，請返回 IAM 身分中心主控台，然後選擇 [使用者]。已同步處理的使用者JumpCloud會顯示在 [使用者] 頁 這些使用者現在可以指派到 IAM 身分中心內的帳戶。

(選用) 步驟 3：在JumpCloud中設定 IAM 身分中心存取控制的使用者屬性

如果您選擇為 JumpCloud IAM 身分中心設定屬性以管理AWS資源存取權，則此為選用程序。您在中定義的屬性JumpCloud會在 SAML 宣告中傳遞至 IAM 身分中心。然後，您可以在 IAM 身分中心建立權限集，以根據傳遞的屬性來管理存取權JumpCloud。

開始此程序之前，您必須先啟用存取控制的屬性功能。如需如何執行此作業的詳細資訊，請參閱啟用和設定存取控制的屬性。

在JumpCloud中設定 IAM 身分中心存取控制的使用者屬性

1. 開啟您在為 JumpCloud (使用者身份驗證 > JumpCloud IAM 身分中心) 設定 SAML 時安裝的 IAM 身分中心連接器。
2. 選擇 IAM 身分中心連接器。然後，選擇第二個選項卡 IAM 身份中心。
3. 在此索引標籤底部，您可以使用「使用者屬性對應」，選擇「新增屬性」，然後執行下列動作：您必須針對要新增以在 IAM Identity Center 中使用的每個屬性執行這些步驟以進行存取控制。

   a. 在「服務提供屬性名稱」欄位中，輸入「`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**`.`取代**`AttributeName`**為 IAM 身分中心」預期的屬性名稱。例如 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**。

   b. 在「JumpCloud屬性名稱」欄位中，從JumpCloud目錄中選擇使用者屬性。例如，電子郵件（工作）。
4. 選擇儲存。

(選擇性) 傳遞屬性以進行存取控制

您可以選擇性地使用 IAM 身分中心中的存取控制的屬性功能來傳遞Name屬性設定為的Attribute元素`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**。此元素可讓您在 SAML 聲明中將屬性做為工作階段標籤傳遞。如需工作階段標籤的詳細資訊，請參閱 IAM 使用者指南AWS STS中的「傳遞工作階段標籤」。

若要將屬性做為工作階段標籤傳遞，請包含指定標籤值的 `AttributeValue` 元素。例如，若要傳遞標籤鍵值配對`CostCenter = blue`，請使用下列屬性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要新增多個屬性，請為每個標籤包含單獨的Attribute元素。

使用和 IAM 身分識別中心設定 SAML Microsoft Entra ID 和 SCIM

AWS IAM Identity Center支援與安全性宣告標記語言 (SAML) 2.0 整合，以及使用跨網域身分識別管理 (SCIM) 2.0 通訊協定的系統，將使用者和群組資訊從 Microsoft Entra ID (先前稱為Azure Active Directory或Azure AD) 自動佈建 (同步處理) 至 IAM 身分中心。

目的

在本教學課程中，您將設定測試實驗室，並在和 IAM 身分中心之間設定 SAML 連線Microsoft Entra ID 和 SCIM 佈建。在初始準備步驟期間，您將在兩個方向建立測試使用者 (Nikki Wolf) Microsoft Entra ID 和 IAM 身分中心，您將使用這些中心來測試 SAML 連線。稍後，作為 SCIM 步驟的一部分，您將建立不同的測試使用者 (Richard Roe)，以確認中的新屬性Microsoft Entra ID是否如預期同步至 IAM 身分中心。

必要條件

您必須先設定下列項目，才能開始使用本教學課程：

- 一個Microsoft Entra ID租客 如需詳細資訊，請參閱快速入門：在 Microsoft 網站上設定租用戶。
- AWS IAM Identity Center已啟用的帳戶。如需詳細資訊，請參閱AWS IAM Identity Center使用指南中的啟用 IAM 身分中心。

步驟 1：準備您的 Microsoft 租戶

在此步驟中，您將逐步介紹如何安裝和設定您的AWS IAM Identity Center企業應用程式，並將存取權指派給新建立的Microsoft Entra ID測試使用者。

Step 1.1 >

步驟 1.1：在中設定AWS IAM Identity Center企業應用程式 Microsoft Entra ID

在此程序中，您可以在中安裝AWS IAM Identity Center企業應用程式Microsoft Entra ID。稍後您將需要此應用程式來設定您的 SAML 連AWS線。

1. 至少以雲端應用程式管理員身分登入 Microsoft Entra 系統管理中心。
2. 導覽至身分識別 > 應用程式 > 企業應用程式，然後選擇 [新增應用程式
3. 在 [瀏覽 Microsoft 項目庫] 頁面上，在搜尋方塊**AWS IAM Identity Center**中輸入。
4. AWS IAM Identity Center從結果區域中選取。

5. 選擇建立。

Step 1.2 >

步驟 1.2：建立測試使用者 Microsoft Entra ID

Nikki Wolf 是您將在此過程中創建的Microsoft Entra ID測試用戶的名稱。

1. 在 Microsoft Entra 系統管理中心主控台中，瀏覽至身分識別 > 使用者 > 所有使用者。
2. 選取 [新增使用者]，然後選擇畫面頂端的 [建立新使用者]。
3. 在 [使用者主要名稱] 中，輸入 **NikkiWolf**，然後選取您偏好的網域和擴充功能。例如，NikkiWolf@ #如。
4. 在顯示名稱中，輸入**NikkiWolf**。
5. 在密碼中，輸入強式密碼或選取眼睛圖示以顯示自動產生的密碼，然後複製或記下顯示的值。
6. 選擇「內容」，在「名字」中輸入**Nikki**。在姓氏中，輸入**Wolf**。
7. 選擇 [檢閱 + 建立]，然後選擇 [建立]。

Step 1.3

步驟 1.3：在將權限分配給 Nikki 之前測試她的經驗 AWS IAM Identity Center

在此過程中，您將驗證什麼 Nikki 可以成功登錄到她的 Microsoft 我的帳戶門戶。

1. 在同一瀏覽器中，打開一個新標籤，轉到「我的帳戶」門戶登錄頁面，然後輸入 Nikki 的完整電子郵件地址。例如，NikkiWolf@ #如。
2. 出現提示時，輸入 Nikki 的密碼，然後選擇「登入」。如果這是自動產生的密碼，系統會提示您變更密碼。
3. 在「需要採取處理行動」頁面上，選擇「稍後詢問」以略過其他安全性方法的提示。
4. 在 [我的帳戶] 頁面的左側導覽列中，選擇 [我的應用程式]。請注意，除了增益集之外，此時不會顯示任何應用程式。您將添加一個AWS IAM Identity Center應用程序，該應用程序將在稍後的步驟中顯示在此處

Step 1.4

步驟 1.4：將權限分配給尼克 Microsoft Entra ID

現在，您已經驗證了 Nikki 可以成功訪問「我的帳戶」門戶，請使用此過程將其用戶分配給該AWS IAM Identity Center應用程序。

1. 在 Microsoft Entra 系統管理中心主控台中，瀏覽至身分識別 > 應用程式 > 企業應用程式，然後AWS IAM Identity Center從清單中選擇。
2. 在左側，選擇 [使用者和群組]。
3. 選擇 Add user/group (新增使用者/群組)。您可以忽略說明群組無法指派的訊息。此自學課程不會使用群組進行指派。
4. 在「新增指定」頁面的「使用者」下，選擇「無選取項目」。
5. 選取 NikkiWolf，然後選擇 [選取]。
6. 在「新增指派」頁面上，選擇指派。 NikkiWolf 現在會顯示在指派給AWS IAM Identity Center應用程式的使用者清單中。

步驟 2：準備您的AWS帳戶

在此步驟中，您將逐步介紹如何使用IAM Identity Center來設定存取權限 (透過權限集)、手動建立對應的 Nikki Wolf 使用者，並指派必要的權限來管理中AWS的資源。

Step 2.1 >

步驟 2.1：在中建立 RegionalAdmin 權限集 IAM Identity Center

此權限集將用於授予 Nikki 從「AWS帳戶」頁面中管理區域所需的必要帳戶權限。AWS Management Console默認情況下，拒絕查看或管理 Nikki 帳戶任何其他信息的所有其他權限。

1. 開啟 IAM 身分中心主控台。
2. 在 [多帳戶權限] 下，選擇 [權限集]。
3. 選擇 Create permission set (建立許可集合)。
4. 在 [選取權限集類型] 頁面上，選取 [自訂權限集]，然後選擇 [下一步]。
5. 選取 [內嵌原則] 將其展開，然後使用下列步驟建立權限集的原則：

   a. 選擇新增陳述式來建立政策聲明。

   b. 在 [編輯對帳單] 底下，從清單中選取 [帳戶]，然後選擇下列核取方塊。

      - **`ListRegions`**
      - **`GetRegionOptStatus`**

- **DisableRegion**
- **EnableRegion**

c. 在 Add a resource (新增資源) 旁邊，選擇 Add (新增)。

d. 在 [新增資源] 頁面的 [資源類型] 下，選取 [所有資源]，然後選擇 [新增資源]。確認您的政策如下所示：

```
{
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions",
                "account:DisableRegion",
                "account:EnableRegion",
                "account:GetRegionOptStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. 選擇下一步。
7. 在 [指定權限集詳細資料] 頁面上的 [權限集名稱] 下，輸入 **RegionalAdmin**，然後選擇 [下一步]。
8. 在 Review and create (檢閱和建立) 頁面上，選取 Create (建立)。您應該RegionalAdmin會看到顯示在權限集清單中。

Step 2.2 >

步驟 2.2：建立對應的 NikkiWolf 使用者 IAM Identity Center

由於 SAML 通訊協定未提供查詢 IdP (Microsoft Entra ID) 以及在 IAM 身分中心自動建立使用者的機制，因此請使用下列程序在 IAM 身分中心手動建立使用者，以鏡像 Nikki Wolfs 使用者的核心屬性。Microsoft Entra ID

1. 開啟 IAM 身分中心主控台。

2. 選擇 [使用者]，選擇 [新增使用者]，然後提供下列資訊：

   a. 對於 [使用者名稱] 和 [電子郵件地址] — 輸入**############ NikkiWolf @ ##### # .####** Microsoft Entra ID例如，NikkiWolf@ #如。

   b. 確認電子郵件地址 — 重新輸入上一步的電子郵件地址

   c. 名字 — 輸入 **Nikki**

   d. 姓氏 — 輸入 **Wolf**

   e. 顯示名稱 — 輸入 **Nikki Wolf**

3. 選擇「下一步」兩次，然後選擇「新增用戶

4. 請選擇 Close (關閉)。

Step 2.3

步驟 2.3：將 Nikki 分配給中設置的 RegionalAdmin 權限 IAM Identity Center

AWS 帳戶在這裡，您可以找到尼克將管理區域，然後分配成功訪問門戶所需的必要權限。AWS

1. 開啟 IAM 身分中心主控台。

2. 在「多帳戶權限」下，選擇AWS 帳戶。

3. 選取您要授與 Nikki 管理區域存取權的帳戶名稱 (例如##) 旁邊的核取方塊，然後選擇 [指派使用者和群組]。

4. 在 [指派使用者和群組] 頁面上，選擇 [使用者] 索引標籤，尋找並勾選 Nikki 旁邊的核取方塊，然後選擇 [下一步]。

步驟 3：設定並測試您的 SAML 連線

在此步驟中，您可以使用AWS IAM Identity Center企業應用程式以及 IAM 身分中心中Microsoft Entra ID的外部 IdP 設定來設定 SAML 連線。

Step 3.1 >

步驟 3.1：從 IAM 身分中心收集所需的服務提供者中繼資料

在此步驟中，您將從 IAM Identity Center 主控台中啟動 [變更身分識別來源] 精靈，並擷取中繼資料檔案以及Microsoft Entra ID在下一個步驟中設AWS定連線時所需輸入的特定登入 URL。

1. 在 IAM 身分中心主控台中，選擇 [設定]。

2. 在 [設定] 頁面上，選擇 [識別來源] 索引標籤，然後選擇 [動作] > [變更身分識別來源]
3. 在 [選擇身分識別來源] 頁面上，選取 [外部身分識別提供者]，然後選擇 [下
4. 在 [設定外部身分識別提供者] 頁面的 [服務提供者中繼資料] 下，選擇 [下載中繼資料檔案] 以將其下載到您
5. 在同一部分中，找到AWS訪問門戶登錄 URL 值並將其複制。在下一個步驟中出現提示時，您將需要輸入此值。
6. 保持此頁面處於開啟狀態，然後移至下一個步驟 (**Step 3.2**) 以在中設定AWS IAM Identity Center企業應用程式Microsoft Entra ID。稍後，您將返回此頁面以完成該過程。

Step 3.2 >

步驟 3.2：配置AWS IAM Identity Center企業應用程序 Microsoft Entra ID

此程序會使用您在上一個步驟中取得的中繼資料檔案和登入 URL 的值，在 Microsoft 端建立一半的 SAML 連線。

1. 在 Microsoft Entra 系統管理中心主控台中，瀏覽至身分識別 > 應用程式 > 企業應用程式，然後選擇AWS IAM Identity Center。
2. 選擇左側的 [單一登入]。
3. 在「使用 SAML 設定單一登入」頁面上，選擇「上傳中繼資料檔案」，選擇資料夾圖示，選取您在上一個步驟中下載的服務提供者中繼資料檔案，然後選擇「新增」。
4. 在「基本 SAML 組態」頁面上，確認識別碼和回覆 URL 值現在都指向開頭為AWS的端點。`https://<REGION>.signin.aws.amazon.com/platform/saml/`
5. 在 [登入 URL (選用)] 底下，貼上您在上一個步驟 (**Step 3.1**) 複製的存AWS取入口網站登入 URL 值，選擇 [儲存]，然後選擇 [X] 以關閉視窗。
6. 如果系統提示您測試單一登入AWS IAM Identity Center，請選擇否，稍後再測試。您將在稍後的步驟中進行此驗證。
7. 在「使用 SAML 設定單一登入」頁面的「SAML 憑證」區段的「同盟中繼資料 XML」旁，選擇「下載」，將中繼資料檔案儲存至您的系統。在下一個步驟中出現提示時，您將需要上傳此檔案。

Step 3.3 >

步驟 3.3：在中設定Microsoft Entra ID外部 IdP AWS IAM Identity Center

在這裡，您將返回 IAM 身分中心主控台中的 [變更身分識別來源] 精靈，以完成中 SAML 連線的下半部分。AWS

1. 返回您**Step 3.1**在 IAM 身分中心主控台中保持開啟狀態的瀏覽器工作階段。
2. 在 [設定外部身分識別提供者] 頁面的 [身分識別提供者中繼資料] 區段的 [IdP SAML 中繼資料] 下，選擇 [選擇檔案] 按鈕，然後選取您在上一個步驟中下載的身分識別提供者Microsoft Entra ID中繼資料檔案，然後選擇 [開啟]。
3. 選擇下一步。
4. 閱讀免責聲明並準備繼續之後，請輸入**ACCEPT**。
5. 選擇 [變更身分識別來源] 以套用變更。

Step 3.4 >

步驟 3.4：測試尼克被重定向到AWS訪問門戶

在此程序中，您將使用 Nikki 的認證登入 Microsoft 的「我的帳戶」入口網站來測試 SAML 連線。經過身份驗證後，您將選擇將 Nikki 重定向到AWS訪問門戶的AWS IAM Identity Center應用程序。

1. 轉到「我的帳戶」門戶登錄頁面，然後輸入 Nikki 的完整電子郵件地址。例如，***NikkiWolf***@#如。
2. 出現提示時，輸入 Nikki 的密碼，然後選擇「登入」。
3. 在 [我的帳戶] 頁面的左側導覽列中，選擇 [我的應用程式]。
4. 在「我的應用程式」頁面上，選取名為的應用程式AWS IAM Identity Center。這應該會提示您進行額外的驗證。
5. 在微軟的登入頁面上，選擇您的 NikkiWolf 認證。如果系統再次出現驗證提示，請再次選擇您的 NikkiWolf 認證。這會自動將您重新導向至AWS存取入口網站。

> **Tip**
>
> 如果您未成功重新導向，請檢查以確定您輸入的AWS存取入口網站登入 URL 值與您複製來源的值**Step 3.2**相符**Step 3.1**。

6. 確認您看到顯示「AWS帳戶」圖示。

> **Tip**
>
> 如果頁面空白且未顯示「AWS帳戶」圖示，請確認 Nikki 已成功指派給RegionalAdmin權限集 (請參閱 **Step 2.3**)。

Step 3.5

步驟 3.5：測試尼克的訪問級別以管理她 AWS 帳戶

在此步驟中，您將檢查以確定 Nikki 的訪問級別以管理她AWS 帳戶的「區域」設置。Nikki 應該只有足夠的管理員權限才能從「帳戶」頁面管理區域。

1. 在AWS存取入口網站中，選擇「AWS帳戶」圖示 以展開帳戶清單。選擇圖示後，與您已定義權限集的任何帳戶相關聯的帳戶名稱、帳戶 ID 和電子郵件地址都會顯示出來。
2. 選擇您套用權限集的帳戶名稱 (例如##) (請參閱 **Step 2.3**)。這將擴大 Nikki 可以選擇來管理其帳戶的權限集列表。
3. 接下來，RegionalAdmin選擇 [管理主控台]，以承擔您在RegionalAdmin權限集中定義的角色。這會將您重定向到AWS Management Console主頁。
4. 在主機右上角，選擇您的帳戶名稱，然後選擇 [帳戶]。這將帶您進入「帳戶」頁面。請注意，此頁面上的所有其他區段都會顯示一則訊息，指出您沒有檢視或修改這些設定的必要權限。
5. 在 [帳戶] 頁面上，向下捲動至 [區域] AWS區段。選取表格中任何可用「區域」的核取方塊。請注意，Nikki 確實具有必要的權限來啟用或禁用她的帳戶的區域列表按照預期。

> **做得很好！**
>
> 步驟 1 到步驟 3 可協助您成功實作和測試 SAML 連線。現在，若要完成教學課程，我們建議您繼續執行步驟 4 以實作自動佈建。

步驟 4：設定並測試您的 SCIM 同步

在此步驟中，您將使用 SCIM v2.0 通訊協定從 Microsoft Entra ID IAM 身分中心設定使用者資訊的自動佈建 (同步處理)。您可以在Microsoft Entra ID使用適用於 IAM 身分中心的 SCIM 端點以及 IAM 身分中心自動建立的承載權杖中設定此連線。

設定 SCIM 同步時，您可Microsoft Entra ID以在中建立使用者屬性與 IAM 身分中心中指定屬性的對應。這會導致 IAM 身分中心和Microsoft Entra ID.

下列步驟將逐步說明如何使用中的 IAM 身分中心應用程式，對主要位於 IAM 身分中心的使用者啟用自動佈建Microsoft Entra ID。Microsoft Entra ID

Step 4.1 >

步驟 4.1：建立第二個測試使用者 Microsoft Entra ID

出於測試目的，您將在中創建一個新用戶（Richard Roe）Microsoft Entra ID。稍後，在您設定 SCIM 同步處理之後，您將測試此使用者和所有相關屬性是否已成功同步至 IAM 身分中心。

1. 在 Microsoft Entra 系統管理中心主控台中，瀏覽至身分識別 > 使用者 > 所有使用者。
2. 選取 [新增使用者]，然後選擇畫面頂端的 [建立新使用者]。
3. 在 [使用者主要名稱] 中，輸入 **RichRoe**，然後選取您偏好的網域和擴充功能。例如，RichRoe@ #如。
4. 在顯示名稱中，輸入**RichRoe**。
5. 在密碼中，輸入強式密碼或選取眼睛圖示以顯示自動產生的密碼，然後複製或記下顯示的值。
6. 選擇 [內容]，然後提供下列值：
   - 名字-輸入 **Richard**
   - 姓氏-輸入 **Roe**
   - Job 稱-輸入 **Marketing Lead**
   - 部門-輸入 **Sales**
   - 員工識別碼-輸入 **12345**
7. 選擇 [檢閱 + 建立]，然後選擇 [建立]。

Step 4.2 >

步驟 4.2：在 IAM 身分中心啟用自動佈建

在此程序中，您將使用 IAM 身分中心主控台，為來自 IAM 身分中心的使用者和群組啟用自動佈建。Microsoft Entra ID

1. 開啟 IAM 身分中心主控台，然後在左側導覽窗格中選擇 [設定]。
2. 在 [設定] 頁面的 [身分識別來源] 索引標籤下，請注意佈建方法已設定為手動。
3. 找到 [自動佈建資訊] 方塊，然後選擇 [啟用]。這會立即在 IAM 身分中心啟用自動佈建，並顯示必要的 SCIM 端點和存取權杖資訊。
4. 在「輸入自動佈建」對話方塊中，複製下列選項的每個值。當您在中配置佈建時，您需要在下一個步驟中貼上這些步驟Microsoft Entra ID。

   a. SCIM 端點-例如，https://scim。 *####-2. #### #/111111111-2222-3333-4444-5555555555 /scim/V2/*

   b. 存取權杖-選擇顯示權杖以複製值。
5. 選擇關閉。
6. 在 [身分識別來源] 索引標籤下，請注意佈建方法現在已設定為 SCIM。

Step 4.3 >

步驟 4.3：在中配置自動佈建 Microsoft Entra ID

現在您已經準備好 RichRoe 測試使用者，並且已在 IAM 身分中心中啟用 SCIM，您可以繼續在中設定 SCIM 同步處理設定。Microsoft Entra ID

1. 在 Microsoft Entra 系統管理中心主控台中，瀏覽至身分識別 > 應用程式 > 企業應用程式，然後選擇AWS IAM Identity Center。
2. 選擇佈建，在管理下，再次選擇佈建。
3. 在佈建模式中，選取自動。
4. 在 [管理員認證] 下的 [租用戶 URL] 中，貼上您先前複製的 SCIM 端點 URL 值。**Step 4.1**在秘密權杖中，貼上存取權杖值。
5. 選擇 Test Connection (測試連接)。您應該會看到一則訊息，指出已成功授權測試的認證可以啟用佈建。
6. 選擇儲存。
7. 在 [管理] 下，選擇 [使用者和群組]，然後選擇 [新增使用者/群組]。
8. 在「新增指定」頁面的「使用者」下，選擇「無選取項目」。
9. 選取 RichRoe，然後選擇 [選取]。

10. 在 Add Assignment (新增指派) 頁面上，選擇 Assign (指派)。
11. 選擇 [概觀]，然後選擇 [開始佈建]。

Step 4.4

步驟 4.4：確認同步處理已發生

在本節中，您將驗證 Richard 的使用者已成功佈建，以及所有屬性都顯示在 IAM 身分中心。

1. 在 IAM 身分中心主控台中，選擇 [使用者]。
2. 在 [使用者] 頁面上，您應該會看到您的RichRoe使用者已顯示。請注意，「建立者」欄中的值設定為 SCIM。
3. 在「設定檔」下選擇 RichRoe，確認下列屬性是否已複製來源Microsoft Entra ID。

   - 名字-**`Richard`**
   - 姓氏-**`Roe`**
   - 部門-**`Sales`**
   - 標題-**`Marketing Lead`**
   - 員工編號-**`12345`**

   現在 Richard 的使用者已在 IAM 身分中心建立，您可以將其指派給任何權限集，以便控制他對您AWS資源的存取層級。例如，您可以指派RichRoe給先前用來授與 Nikki 管理區域的權限集 (請參閱 **`Step 2.3`**)，然後使**`Step 3.5`**用來測試其存取層級。**`RegionalAdmin`**

> **恭喜您！**
>
> 您已成功設定 Microsoft 之間的 SAML 連線，並AWS且已驗證自動佈建正在運作，讓所有項目保持同步。現在，您可以應用所學到的知識，以更順暢地設置您的生產環境。

Microsoft Entra ID在生產環境中使用 SCIM 的考量

以下是相關的重要考量，可Microsoft Entra ID能會影響您計劃如何使用 SCIM v2 通訊協定在生產環境中使用 IAM 身分中心實作自動佈建。

> **Note**
>
> 在開始部署 SCIM 之前，我們建議您先檢閱使用自動佈建的考量。

存取控制的屬性

用於存取控制的屬性用於決定身分識別來源中誰可以存取您的AWS資源的權限原則。如果從中的使用者移除屬性Microsoft Entra ID，該屬性將不會從 IAM 身分中心的對應使用者中移除。這是中的已知限制Microsoft Entra ID。如果使用者的屬性變更為不同 (非空白) 值，則該變更會同步至 IAM 身分中心。

巢狀群組

Microsoft Entra ID使用者佈建服務無法讀取或佈建巢狀群組中的使用者。只有屬於明確指派之群組直接成員的使用者才能讀取和佈建。 Microsoft Entra ID不會以遞迴方式解壓縮間接指派的使用者或群組 (屬於直接指派之群組成員的使用者或群組) 的群組成員資格。如需詳細資訊，請參閱文件中的以指派為基礎的範圍設定。Microsoft Entra ID

動態群組

Microsoft Entra ID使用者佈建服務可以讀取和佈建動態群組中的使用者。請參閱以下範例，瞭解使用動態群組時的使用者和群組結構，以及這些使用者和群組在 IAM 身分中心中的顯示方式。這些使用者和群組是透過 SCIM 從 Microsoft Entra ID IAM 身分中心佈建

例如，如果動態群組的Microsoft Entra ID結構如下所示：

1. A 組，成員為 ua1，ua2
2. B 組成員為 ub1
3. C 組，其成員為 uc1
4. 規定包括 A、B、C 組成員的 K 組
5. 群組 L，其規則包括 B 和 C 組成員

透過 SCIM 將使用者和群組資訊從 IAM 身分中心佈建Microsoft Entra ID到 IAM 身分中心後，結構將如下所示：

1. A 組，成員為 ua1，ua2
2. B 組成員為 ub1
3. C 組，其成員為 uc1

4. K 組成員為 ua1、ua2、ub1、uc1
5. 群組 L，其成員為 ub1，uc1

使用動態群組設定自動佈建時，請記住下列考量事項。

- 動態群組可以包含巢狀群組。不過，Microsoft Entra ID佈建服務不會平面化巢狀群組。例如，如果動態群組具有下列Microsoft Entra ID結構：
  - 群組 A 是群組 B 的父系。
  - A 組有 ua1 作為成員。
  - B 組有 ub1 作為成員。

包含群組 A 的動態群組只會包含群組 A (也就是 ua1) 的直接成員。它不會遞歸包含 B 組的成員。

- 動態群組不能包含其他動態群組。如需詳細資訊，請參閱Microsoft Entra ID文件中的預覽限制。

疑難排解 SCIM 問題 Microsoft Entra ID

如果您遇到使用Microsoft Entra ID者未同步至 IAM 身分中心的問題，可能是因為當新使用者新增至 IAM 身分中心時，IAM 身分中心已標記語法問題。您可以檢查Microsoft Entra ID稽核記錄檔是否有失敗事件，例如`'Export'`. 此事件的「狀態原因」 會說明：

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is
 unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

您也可以檢AWS CloudTrail查失敗的事件。這可以通過 CloudTrail 使用以下過濾器在事件歷史記錄控制台中搜索來完成：

```
"eventName":"CreateUser"
```

CloudTrail 事件中的錯誤將說明以下內容：

```
"errorCode": "ValidationException",
        "errorMessage": "Currently list attributes only allow single item“
```

最終，此例外意味著從傳遞的其中一個值Microsoft Entra ID包含的值超過預期的值。這裡的解決方案是查看中用戶的屬性Microsoft Entra ID，確保沒有包含重複值。重複值的一個常見例子是具有多個值

存在於聯繫電話，如移動，工作和傳真。雖然單獨的值，它們都傳遞給 IAM 身份中心下的單一父屬性 PhoneNu mbers。

如需 SCIM 疑難排解的一般秘訣，請參閱IAM 身分中心問題疑難排解。

步驟 5：(選擇性) 設定 ABAC

現在您已成功設定 SAML 和 SCIM，您可以選擇性地選擇設定以屬性為基礎的存取控制 (ABAC)。ABAC 是一種授權策略，根據屬性定義權限。

使用時Microsoft Entra ID，您可以使用下列兩種方法之一來設定 ABAC 以搭配 IAM 身分中心使用。

Method 1

方法 1：在Microsoft Entra ID中設定 IAM 身分中心存取控制的使用者屬性

在下列程序中，您將決定 IAM 身分中心Microsoft Entra ID應使用哪些屬性來管理AWS資源的存取權。定義完成後，Microsoft Entra ID會透過 SAML 宣告將這些屬性傳送至 IAM 身分中心。然後，您將需要建立許可集合在 IAM 身分中心根據傳遞的屬性管理存取權限Microsoft Entra ID。

開始此程序之前，您必須先啟用此存取控制的屬性功能。如需如何進行該服務的詳細資訊，請參閱啟用和設定存取控制的屬性。

1. 在 Microsoft Entra 系統管理中心主控台中，瀏覽至身分識別 > 應用程式 > 企業應用程式，然後選擇AWS IAM Identity Center。
2. 選擇 Single sign-on (單一登入)。
3. 在「屬性與聲明」區段中，選擇 「編輯」。
4. 在「屬性與宣告」頁面上，執行下列動作：
   a. 選擇 [新增索賠]
   b. 對於名稱，輸入 `AccessControl:`*`AttributeName`*。以 IAM 身分中心預期的屬性名稱取代*`AttributeName`*。例如 `AccessControl:`**`Department`**。
   c. 針對 Namespace (命名空間)，輸入 **`https://aws.amazon.com/SAML/Attributes`**。
   d. 針對 Source (來源)，選擇 Attribute (屬性)。
   e. 對於「來源」屬性，請使用下拉式清單來選擇使用Microsoft Entra ID者屬性。例如 `user.`**`department`**。
5. 針對需要在 SAML 宣告中傳送至 IAM 身分中心的每個屬性重複上述步驟。

6. 選擇儲存。

Method 2

方法 2：使用 IAM 身分中心設定 ABAC

使用此方法時，您可以使用 IAM 身分中心中的存取控制的屬性功能來傳遞Name屬性設定為的Attribute元素https://aws.amazon.com/SAML/Attributes/AccessControl:**{TagKey}**。您可以使用此元素將屬性作為 SAML 宣告中的工作階段標籤傳遞。如需工作階段標籤的詳細資訊，請參閱 IAM 使用者指南AWS STS中的「傳遞工作階段標籤」。

若要將屬性做為工作階段標籤傳遞，請包含指定標籤值的 AttributeValue 元素。例如，若要傳遞標籤鍵值配對CostCenter = blue，請使用下列屬性：

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要新增多個屬性，請為每個標籤包含單獨的Attribute元素。

使用和 IAM 身分識別中心設定 SAML Okta 和 SCIM

您可以使用跨網域身分識別管理 (SCIM) 2.0 版通訊協定的系統，Okta將使用者和群組資訊自動佈建 (同步) 至 IAM 身分中心。若要在中設定此連線Okta，請將 SCIM 端點用於 IAM 身分中心，以及由 IAM 身分中心自動建立的承載權杖。設定 SCIM 同步時，您可Okta以在中建立使用者屬性與 IAM 身分中心中指定屬性的對應。此對應會比對 IAM 身分中心和您的Okta.

Okta透過 SCIM 連線至 IAM 身分中心時，支援下列佈建功能：

- 建立使用者 — 指派給中 IAM 身分中心應用程式的使用者會在 IAM 身分中心佈建。Okta
- 更新使用者屬性 — 在 IAM 身分中心中指派給 IAM 身分中心應用程式的使Okta用者的屬性變更會更新。
- 停用使用者 — 在 Okta IAM 身分中心中停用從中的 IAM 身分中心應用程式取消指派的使用者。
- 群組推送 — 中的群組 (及其成員) Okta 會同步至 IAM 身分中心。

> **Note**
>
> 為了將Okta和 IAM 身分中心的管理開銷降到最低，我們建議您指派和推送群組，而不是個別使用者。

如果您尚未啟用 IAM 身分中心，請參閱啟用 AWS IAM Identity Center。

目的

在本教學課程中，您將逐步瞭解如何設定與 Okta IAM 身分中心的 SAML 連線。稍後，您將使用 SCIM 從Okta同步處理使用者。在此案例中，您可以管理中的所有使用者和群組Okta。使用者透過入Okta口網站登入。若要驗證所有項目的設定是否正確，在完成設定步驟後，您將以Okta使用者身分登入並驗證 AWS 資源的存取權。

> **Note**
>
> 您可以註冊已安裝 Okta's IAM 身分中心應用程式的Okta帳戶 (免費試用)。對於付費Okta產品，您可能需要確認您的Okta授權支援生命週期管理或啟用輸出佈建的類似功能。將 SCIM 設定為 IAM 身分中心時，可能需要這些功能。Okta

開始之前

在設定Okta和 IAM 身分中心之間的 SCIM 佈建之前，我們建議您先檢閱使用自動佈建的考量。

開始之前，請先確認以下項目：

- 每個Okta使用者都必須指定「名字」、「姓氏」、「使用者名稱」和「顯示名稱」值。
- 每個Okta使用者的每個資料屬性只有一個值，例如電子郵件地址或電話號碼。任何具有多個值的使用者將無法同步處理。如果使用者的屬性中有多個值，請先移除重複的屬性，然後再嘗試在 IAM 身分中心佈建使用者。例如，只能同步一個電話號碼屬性，因為預設的電話號碼屬性是「工作電話」，因此即使使用者的電話號碼是住家電話或行動電話，也可以使用「工作電話」屬性來儲存使用者的電話號碼。
- 如果您更新使用者的地址，您必須有指定的街道地址、城市、州、郵遞區號和國家代碼值。如果在同步處理時未為Okta使用者指定這些值中的任何一個，則不會佈建使用者 (或對使用者的變更)。

> **Note**
>
> 不支援授權和角色屬性，且無法與 IAM 身分中心同步。
> 目前不支援針對指派和群組推送使用相Okta同的群組。若要在Okta和 IAM 身分中心之間維持一致的群組成員資格，請建立單獨的群組並將其設定為將群組推送至 IAM 身分中心。

步驟 1：從您的帳戶取得 SAML 中繼資料 Okta

1. 登入Okta admin dashboard，展開 [應用程式]，然後選取 [應用程式]。
2. 在 Applications (應用程式) 頁面上，選擇 Browse App Catalog (瀏覽應用程式目錄)。
3. 在搜尋方塊中輸入 AWS IAM Identity Center，選取要新增 IAM 身分中心應用程式的應用程式。
4. 選取 [登入] 索引標籤。
5. 在「SAML 簽署憑證」下，選取「動作」，然後選取「檢視 IdP 中繼資料」。新的瀏覽器標籤隨即開啟，顯示 XML 檔案的文件樹狀結構。從選擇所有的 XML，`</md:EntityDescriptor>`並`<md:EntityDescriptor>`將其複製到一個文本文件。
6. 將文字檔另存為`metadata.xml`。

保持Okta admin dashboard開啟狀態，您將在稍後的步驟中繼續使用該主控台。

步驟 2：設定Okta為 IAM 身分中心的身分識別來源

1. 以具有管理權限的使用者身分開啟 IAM 身分中心主控台。
2. 在左側導覽窗格中選擇 [設定]。
3. 在 [設定] 頁面上，選擇 [動作]，然後選擇 [變更身分識別來源]。
4. 在選擇身分識別來源下，選取外部身分識別提供者，然後選擇下一步。
5. 在設定外部身分識別提供者下，執行下列操作：

   a. 在「服務提供者中繼資料」下，選擇「下載中繼資料檔案」以下載 IAM Identity Center 中繼資料檔案，並將其儲存在系統 您將在本教學課程Okta稍後提供 IAM 身分中心 SAML 中繼資料檔案。

   將下列項目複製到文字檔案中以方便存取：

   - IAM 身分中心聲明消費者服務 (ACS) 網址
   - IAM 身分識別中心發行者 URL

在本教學課程稍後，您將需要這些值。

b. 在身分識別提供者中繼資料下的 IdP SAML 中繼資料下，選取 [選擇檔案]，然後選取您在上一個步驟中建立的`metadata.xml`檔案。

c. 選擇下一步。

6. 閱讀免責聲明並準備繼續之後，請輸入 AC CEPT。
7. 選擇 [變更識別來源]。

讓 AWS 主控台保持開啟狀態，您將在下一個步驟繼續使用該主控台。

8. 返回Okta admin dashboard並選取 AWS IAM Identity Center 應用程式的「登入」索引標籤，然後按一下「編輯」。
9. 在「進階登入設定」 下輸入下列項目：

- 對於 ACS URL，請輸入您為 IAM 身分中心聲明消費者服務 (ACS) URL 複製的值
- 對於發行者 URL，請輸入您為 IAM 身分中心簽發者 URL 複製的值
- 對於應用程式使用者名稱格式，請從下拉式功能表中選取其中一個

讓您選擇的值對每個使用者都是唯一的。對於本教程，請選擇 Okta 用戶名

10. 選擇儲存。

您現在可以從 Okta IAM 身分中心佈建使用者。保持Okta admin dashboard開啟狀態，然後返回 IAM 身分中心主控台進行下一個步驟。

步驟 3：提供使用者 Okta

1. 在 [設定] 頁面的 IAM Identity Center 主控台中，找出 [自動佈建資訊] 方塊，然後選擇 [啟用]。這樣可在 IAM 身分中心自動佈建，並顯示必要的 SCIM 端點和存取權杖資訊。
2. 在「輸入自動佈建」對話方塊中，複製下列選項的每個值：

- SCIM 端點
- 訪問令牌

稍後在本教學課程中，您將輸入這些值以在中配置佈建Okta。

3. 選擇關閉。
4. 返回Okta admin dashboard並瀏覽至 IAM 身分中心應用程式。

5. 在 IAM 身分中心應用程式頁面上，選擇 [佈建] 索引標籤，然後在左側導覽中的 [設定] 下方選擇 [整合]。
6. 選擇 [編輯]，然後選取 [啟用 API 整合] 旁的核取方塊以啟用佈建。
7. 使Okta用您先前在本教學課程中複製的 IAM 身分中心的 SCIM 佈建值進行設定：

   a. 在「基礎 URL」欄位中，輸入 SCIM 端點值。確保您刪除了 URL 末尾的正斜線。

   b. 在「API 權杖」欄位中，輸入存取權杖值。
8. 選擇「測試 API 認證」以驗證輸入的認證是否有效。

   訊息已AWS IAM Identity Center 成功驗證！ 顯示器。
9. 選擇儲存。您會導覽至 「設定」 區域，並選取「整合」。
10. 在 [設定] 下，選擇 [至應用程式]，然後針對您要啟用的每個 [佈建至應用程式] 功能選取 [啟用] 核取方塊。對於此自學課程，請選取所有選項。
11. 選擇儲存。

您現在可以使用 IAM 身分中心同步處理使用者。Okta

步驟 4：使用 IAM 身分中心同步處理使用者 Okta

根據預設，不會將任何群組或使用者指派給您的 Okta IAM 身分中心應用程式。啟動設定群組會提供屬於群組成員的使用者。完成下列步驟，以使用 IAM 身分中心同步群組和使用者。

1. 在 OktaIAM 身分中心應用程式頁面中，選擇指派索引標籤。您可以將人員和群組指派給 IAM 身分中心應用程式。

   a. 若要指派人員：

      - 在 [指派] 頁面中，選擇 [指派]，然後選擇 [指派給人員]。
      - 選擇您想要存取 IAM 身分中心應Okta用程式的使用者。選擇「指派」，選擇「儲存並返回」，然後選擇「完成」。

      這會啟動將使用者佈建至 IAM 身分中心的程序。

   b. 若要指派群組：

      - 在 [指派] 頁面中，選擇 [指派]，然後選擇 [指派給群組]。
      - 選擇您想要存取 IAM 身分中心應用程式的Okta群組。選擇「指派」，選擇「儲存並返回」，然後選擇「完成」。

這會啟動將群組中的使用者佈建至 IAM 身分識別中心的程序。

> **Note**
>
> 如果群組的其他屬性不存在於所有使用者記錄中，您可能需要為群組指定其他屬性。為群組指定的屬性會覆寫任何個別屬性值。

2. 選擇「植入群組」頁標。選擇包含您指派給 IAM 身分中心應用程式之所有群組的群組。Okta選擇儲存。

   群組及其成員推送至 IAM 身分中心後，群組狀態會變更為「作用中」。

3. 返回 [指派] 索引標籤。

4. 如果您的使用者不是您推送至 IAM 身分中心的群組成員，請使用下列步驟個別新增使用者：

   在 [指派] 頁面中，選擇 [指派]，然後選擇 [指派給人員]。

5. 選擇您想要存取 IAM 身分中心應Okta用程式的使用者。選擇「指派」，選擇「儲存並返回」，然後選擇「完成」。

   這會啟動將個別使用者佈建至 IAM 身分識別中心的程序。

> **Note**
>
> 您也可以從的 [應用 AWS IAM Identity Center 程式] 頁面，將使用者和群組指派給應用程式Okta admin dashboard。若要執行此操作，請選取 [設定] 圖示，然後選擇 [指派給使用者] 或 [指派給群組]，然後指定使用者或群組。

6. 返回 IAM 身分中心主控台。在左側導覽列中，選取 [使用者]，您應該會看到由您的使Okta用者填入的使用者清單。

> **恭喜您！**
>
> 您已成功設定Okta和之間的 SAML 連線，並 AWS 且已驗證自動佈建正在運作。您現在可以在 IAM 身分中將這些使用者指派給帳戶和應用程式。在本教學課程中，在下一個步驟中，讓我們將其中一位使用者授與管理帳戶的管理權限，指定其中一位使用者為 IAM Identity Center 管理員。

步驟 5：授予Okta使用者帳戶存取權

1. 在「IAM 身分中心」導覽窗格的「多帳戶權限」下，選擇AWS 帳戶。
2. 在AWS 帳戶頁面上，組織結構會在階層中顯示您的組織根目錄，並在其下方顯示您的帳戶。選取管理帳戶的核取方塊，然後選取 [指派使用者或群組]。
3. 指派使用者和群組工作流程隨即顯示。它由三個步驟組成：

   a. 對於步驟 1：選取使用者和群組，請選擇要執行管理員工作職能的使用者。然後選擇下一步。

   b. 針對步驟 2：選取權限集選擇 [建立權限集] 以開啟新索引標籤，逐步引導您完成建立權限集所涉及的三個子步驟。

      i. 對於步驟 1：選取權限集類型，請完成下列步驟：

         - 在 [權限集類型] 中，選擇 [預先定義的權限集
         - 在預先定義權限集的原則中，選擇AdministratorAccess。

         選擇下一步。

      ii. 針對 [步驟 2: 指定權限集詳細資料]、保留預設設定，然後選擇 [下一步]。

         預設設定會建立名為*AdministratorAccess*工作階段持續時間設定為一小時的權限集。

      iii. 對於步驟 3：檢閱和建立，請確認「權限集」類型是否使用 AWS 受管理的原則AdministratorAccess。選擇建立。在 [權限集] 頁面上會出現通知，通知您已建立權限集。您現在可以在 Web 瀏覽器中關閉此選項卡。

      在 [指派使用者和群組] 瀏覽器索引標籤上，您仍在執行 [步驟 2: 選取啟動建立權限集工作流程的權限集] 中。

      在「權限集」區域中，選擇「重新整理」按鈕。您建立的*AdministratorAccess*權限集會顯示在清單中。選取該權限集的核取方塊，然後選擇 [下一步]。

   c. 對於步驟 3：檢閱並提交檢閱選取的使用者和權限集，然後選擇 [提交]。

      頁面會更新並顯示正在設 AWS 帳戶 定您的訊息。等待，直到該過程完成。

      您將返回 AWS 帳戶 頁面。通知訊息會通知您已重新佈建，且 AWS 帳戶 已套用更新的權限集。當用戶登錄時，他們將有選擇角色的選項*AdministratorAccess*。

> **Note**
>
> 來自 SCIM 自動同步處理Okta僅支援佈建使用者；不會自動佈建群組。您無法Okta使用 AWS Management Console. 佈建使用者之後，您可以使用 CLI 或 API 作業建立群組

步驟 6：確認Okta使用者存取 AWS 資源

1. 使用測試Okta dashboard使用者帳戶登入。
2. 在「我的應用程式」下選取AWS IAM Identity Center圖示。
3. 您已登入入口網站，可以看到 AWS 帳戶 圖示。展開該圖示以查看使用者可以存取的 AWS 帳戶清單。在本教程中，您只使用一個帳戶，因此展開圖標僅顯示一個帳戶。
4. 選取帳戶以顯示使用者可用的權限集。在本教學課程中，您建立了AdministratorAccess權限集。
5. 權限集旁邊是該權限集可用存取類型的連結。建立權限集時，您已指定同時啟用管理主控台和程式設計存取，因此會出現這兩個選項。選取管理主控台以開啟 AWS Management Console。
6. 使用者已登入主控台。

(選擇性) 傳遞屬性以進行存取控制

您可以選擇性地使用 IAM 身分中心中的存取控制的屬性功能來傳遞Name屬性設定為的`Attribute`元素`https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`。此元素可讓您在 SAML 聲明中將屬性做為工作階段標籤傳遞。如需工作階段標籤的詳細資訊，請參閱 IAM 使用者指南 AWS STS中的「傳遞工作階段標籤」。

若要將屬性做為工作階段標籤傳遞，請包含指定標籤值的 `AttributeValue` 元素。例如，若要傳遞標籤鍵值配對`CostCenter = blue`，請使用下列屬性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要新增多個屬性，請為每個標籤包含單獨的`Attribute`元素。

後續步驟

現在，您已在 IAM 身分中心設定Okta為身分識別提供者並佈建使用者，您可以：

- 授與存取權 AWS 帳戶，請參閱指派使用者存取權給 AWS 帳戶。
- 授予雲端應用程式的存取權，請參閱在 IAM 身分中心主控台中指派應用程式的使用者存取權。
- 根據工作職能設定權限，請參閱建立權限集

在OneLogin和 IAM 身分中心之間設定 SCIM 佈建

IAM 身分中心支援使用跨網域身分識別管理 (SCIM) 2.0 版通訊協定的系統，OneLogin將使用者和群組資訊從 IAM 身分中心自動佈建 (同步)。您可以在中設定此連線OneLogin，並使用 IAM 身分中心的 SCIM 端點，以及 IAM 身分中心自動建立的承載權杖。設定 SCIM 同步時，您可OneLogin以在中建立使用者屬性與 IAM 身分中心中指定屬性的對應。這會導致 IAM 身分中心和OneLogin.

下列步驟將逐步說明如何使用 SCIM 通訊協定啟用從 OneLogin IAM 身分中心自動佈建使用者和群組。

> **Note**
>
> 在開始部署 SCIM 之前，建議您先檢閱. 使用自動佈建的考量

主題

必要條件

在開始之前，您將需要以下內容：

- 一個OneLogin帳戶。如果您沒有現有帳戶，則可以從該OneLogin網站獲得免費試用或開發人員帳戶。

- 已啟用 IAM 身分中心的帳戶 (免費)。如需詳細資訊，請參閱啟用 IAM 身分中心。
- 從您的OneLogin帳戶到 IAM 身分中心的 SAML 連線。如需詳細資訊，請參閱AWS合作夥伴網路部落格AWS上的啟用OneLogin和之間的單一登入。

步驟 1：在 IAM 身分中心啟用佈建

在第一個步驟中，您可以使用 IAM 身分中心主控台啟用自動佈建。

在 IAM 身分中心啟用自動佈建

1. 完成必要條件後，請開啟 IAM 身分中心主控台。
2. 在左側導覽窗格中選擇 [設定]。
3. 在 [設定] 頁面上，找出 [自動佈建資訊] 方塊，然後選擇 [啟用]。這會立即在 IAM 身分中心啟用自動佈建，並顯示必要的 SCIM 端點和存取權杖資訊。
4. 在「輸入自動佈建」對話方塊中，複製下列選項的每個值。稍後當您在 IdP 中配置佈建時，您將需要貼上這些內容。
   a. SCIM 端點
   b. 訪問令牌
5. 選擇關閉。

您現在已在 IAM 身分中心主控台中設定佈建。現在，您需要使用OneLogin管理控制台執行剩餘的工作，如下列程序所述。

步驟 2：配置佈建 OneLogin

在OneLogin管理主控台中使用下列程序，啟用 IAM 身分中心和 IAM 身分中心應用程式之間的整合。此程序假設您已在OneLogin中設定 SAML 驗證的AWS單一登入應用程式。如果您尚未建立此 SAML 連線，請在繼續之前執行此動作，然後返回此處以完成 SCIM 佈建程序。如需設定 SAML 的詳細資訊 OneLogin，請參閱AWS合作夥伴網路部落格AWS上的啟用OneLogin和之間的單一登入。

若要在中設定佈建 OneLogin

1. 登入OneLogin，然後瀏覽至 [應用程式] > [應用程式]。
2. 在 [應用程式] 頁面上，搜尋您先前建立的應用程式，以形成與 IAM 身分中心的 SAML 連線。選擇它，然後從左側導航欄中選擇配置。

3. 在先前的程序中，您會在 IAM 身分中心複製 SCIM 端點值。將該值貼到中的「SCIM 基礎 URL」欄位OneLogin。確保您刪除了 URL 末尾的正斜線。此外，在先前的程序中，您會在 IAM 身分中心複製存取權杖值。將該值貼到中的「SCIM 承載權杖」欄位。OneLogin
4. 在「API 連線」旁，按一下「啟用」，然後按一下「儲存」以完成設定。
5. 在左側導覽列中，選擇佈建。
6. 選取 [啟用授權]、[建立使用者]、[刪除使用者] 和 [更新使用者] 的核取方塊，然後選擇 [儲存]。
7. 在左側導覽列中，選擇 [使用者]。
8. 按一下「更多動作」並選擇「同步登入」。您應該會收到「使用AWS單一登入同步處理使用者」訊息。
9. 再按一下 [更多動作]，然後選擇 [重新套用權利文件對應] 您應該會收到正在重新套用對應的訊息。
10. 此時，佈建程序應該會開始。若要確認這一點，請瀏覽至「活動」>「事件」，然後監視進度。成功的佈建事件以及錯誤應該會出現在事件串流中。
11. 若要確認您的使用者和群組是否已成功同步至 IAM 身分中心，請返回 IAM 身分中心主控台，然後選擇 [使用者]。同步處理的使用者OneLogin會顯示在「使用者」頁面上。您也可以在「群組」頁面上檢視已同步處理的群組。
12. 若要將使用者變更自動同步至 IAM Identity Center，請導覽至佈建頁面，找到執行此動作前需要管理員核准區段，取消選取建立使用者、刪除使用者和/或更新使用者，然後按一下儲存。

(選用) 步驟 3：在中設定使用者屬性，以OneLogin便在 IAM 身分中心進行存取控制

OneLogin如果您選擇設定要在 IAM 身分中心用來管理AWS資源存取權限的屬性，則此為選用程序。您在中定義的屬性OneLogin會在 SAML 宣告中傳遞至 IAM 身分中心。然後，您將在 IAM 身分中心建立權限集，以根據傳遞的屬性來管理存取權限OneLogin。

開始此程序之前，您必須先啟用此存取控制的屬性功能。如需如何進行該服務的詳細資訊，請參閱啟用和設定存取控制的屬性。

在OneLogin中設定 IAM 身分中心存取控制的使用者屬性

1. 登入OneLogin，然後瀏覽至 [應用程式] > [應用程式]。
2. 在 [應用程式] 頁面上，搜尋您先前建立的應用程式，以形成與 IAM 身分中心的 SAML 連線。選擇它，然後從左側導航欄中選擇參數。
3. 在「必要參數」區段中，針對要在 IAM 身分中心使用的每個屬性執行下列動作：

a. 選擇 [+]。

b. 在 [欄位名稱] 中`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**，輸入您在 IAM 身分中心預期的屬性名稱，並取代**`AttributeName`**為該屬性的名稱。例如 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**。

c. 在 [旗標] 底下，核取 [包含在 SAML 宣告中] 旁邊的方塊，然後選擇 [儲存]。

d. 在「值」字段中，使用下拉列表來選擇用OneLogin戶屬性。例如，「部門」。

4. 選擇儲存。

(選擇性) 傳遞屬性以進行存取控制

您可以選擇性地使用 IAM 身分中心中的存取控制的屬性功能來傳遞`Name`屬性設定為的`Attribute`元素`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**。此元素可讓您在 SAML 聲明中將屬性做為工作階段標籤傳遞。如需工作階段標籤的詳細資訊，請參閱 IAM 使用者指南AWS STS中的「傳遞工作階段標籤」。

若要將屬性做為工作階段標籤傳遞，請包含指定標籤值的 `AttributeValue` 元素。例如，若要傳遞標籤鍵值配對`CostCenter = blue`，請使用下列屬性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要新增多個屬性，請為每個標籤包含單獨的`Attribute`元素。

故障診斷

以下內容可協助您疑難排解在使用設定自動佈建時可能遇到的一些常見問題OneLogin。

群組未佈建至 IAM 身分中心

依預設，群組可能不會從佈建OneLogin到 IAM 身分中心。請確定您已在中啟用 IAM 身分中心應用程式的群組佈建OneLogin。若要這麼做，請登入OneLogin管理主控台，然後檢查並確認已在 IAM 身分中心應用程式 (IAM 身分中心應用程式 > 參數 > 群組) 的屬性下選取 [包含在使用者佈建] 選項。如需有關

如何在中建立群組的詳細資訊OneLogin，包括如何在 SCIM 中將OneLogin角色作為群組同步處理，請參閱OneLogin網站。

儘管所有設置都正確，但沒有任何內容從 OneLogin IAM 身份中心同步

除了上述有關管理員核准的注意事項之外，您還需要重新套用權利對應，許多組態變更才會生效。您可以在「應用程式 > 應用程式 > IAM 身分中心應用程式 > 更多動作」 中找到。您可以在「活動」>「事件」下查看大多數動作的OneLogin詳細資料和記錄，包括同步處理事件。

我已刪除或停用中的群組OneLogin，但仍出現在 IAM 身分中心

OneLogin目前不支援群組的 SCIM DELETE 作業，這表示該群組仍然存在於 IAM 身分中心。因此，您必須直接從 IAM 身分中心移除群組，以確保該群組的 IAM 身分中心中的任何對應許可都會遭到移除。

我在 IAM 身份中心中刪除了一個組，而沒有先刪除它OneLogin，現在我遇到了用戶/組同步問題

若要解決此情況，請先確定中沒有任何冗餘群組佈建規則或組態OneLogin。例如，直接指派給應用程式的群組，以及發佈至相同群組的規則。接下來，刪除 IAM 身分中心中的任何不需要的群組。最後OneLogin，在中重新整理權利 (IAM 身分中心應用程式 > 佈建 > 權利)，然後重新套用權利對應 (IAM 身分識別中心應用程式 > 更多動作)。若要避免 future 後發生此問題，請先進行變更以停止佈建群組OneLogin，然後從 IAM 身分中心刪除該群組。

搭配 IAM 身分中心使用Ping Identity產品

下列Ping Identity產品已透過 IAM 身分中心測試。

主題

- PingFederate
- PingOne

PingFederate

IAM 身分中心支援將PingFederate產品的使用者和群組資訊自動佈建 (同步處理) Ping Identity (以下稱為「Ping」) 進入 IAM 身分中心。此佈建使用系統進行跨網域身分識別管理 (SCIM) 2.0 通訊協定。您可以在PingFederate使用 IAM 身分中心 SCIM 端點和存取權杖中設定此連線。設定 SCIM 同步時，您可PingFederate以在中建立使用者屬性與 IAM 身分中心中指定屬性的對應。這會導致 IAM 身分中心和PingFederate.

本指南以 10.2 PingFederate 版為基礎。其他版本的步驟可能會有所不同。如需有關如何針Ping對其他版本的 IAM 身分中心設定佈建的詳細資訊，請聯絡PingFederate。

下列步驟將逐步說明如何使用 SCIM 通訊協定啟用從 PingFederate IAM 身分中心自動佈建使用者和群組。

> **Note**
>
> 在開始部署 SCIM 之前，建議您先檢閱. 使用自動佈建的考量 然後繼續檢閱下一節中的其他考量。

主題

必要條件

在開始之前，您將需要以下內容：

- 工作PingFederate伺服器。如果您沒有現有的PingFederate伺服器，您可以從 Ping Identity 網站取得免費試用或開發人員帳戶。試用版包含授權與軟體下載，以及相關文件。
- 您伺服器上安裝的 PingFederate IAM 身分中心連接PingFederate器軟體複本。如需如何取得此軟體的詳細資訊，請參閱 P ing Identity 網站上的 IAM 身分中心連接器。
- 已啟用 IAM 身分中心的帳戶 (免費)。如需詳細資訊，請參閱啟用 IAM 身分中心。
- 從您的執行個PingFederate體到 IAM 身分中心的 SAML 連線。如需有關如何設定此連線的指示，請參閱PingFederate文件。總而言之，建議的路徑是使用 IAM 身分中心連接器在中設定「瀏覽器 SSO」PingFederate，並使用兩端的「下載」和「匯入」中繼資料功能，在PingFederate和 IAM 身分中心之間交換 SAML 中繼資料。

其他考量

以下是有關PingFederate此問題的重要考量，可能會影響您使用 IAM 身分中心實作佈建的方式。

- 如果從中設定的資料存放區中的使用者移除屬性 (例如電話號碼)PingFederate，該屬性將不會從 IAM Identity Center 中的對應使用者中移除。這是PingFederate's佈建程式實作中的已知限制。如果使用者的屬性變更為不同 (非空白) 值，則該變更會同步至 IAM 身分中心。

步驟 1：在 IAM 身分中心啟用佈建

在第一個步驟中，您可以使用 IAM 身分中心主控台啟用自動佈建。

在 IAM 身分中心啟用自動佈建

1. 完成必要條件後，請開啟 IAM 身分中心主控台。
2. 在左側導覽窗格中選擇 [設定]。
3. 在 [設定] 頁面上，找出 [自動佈建資訊] 方塊，然後選擇 [啟用]。這會立即在 IAM 身分中心啟用自動佈建，並顯示必要的 SCIM 端點和存取權杖資訊。
4. 在「輸入自動佈建」對話方塊中，複製下列選項的每個值。稍後在 IdP 中配置佈建時，您將需要貼上這些內容。
   a. SCIM 端點
   b. 訪問令牌
5. 選擇關閉。

現在您已在 IAM Identity Center 主控台中設定佈建，您必須使用PingFederate管理主控台完成剩餘的工作。，下列程序說明這些步驟。

步驟 2：配置佈建 PingFederate

在PingFederate管理主控台中使用下列程序，以啟用 IAM 身分中心和 IAM 身分中心連接器之間的整合。此程序假設您已安裝 IAM 身分中心連接器軟體。如果您尚未這麼做，請參閱必要條件，然後完成此程序以設定 SCIM 佈建。

> **Important**
>
> 如果您的PingFederate伺服器先前尚未設定輸出 SCIM 佈建，您可能需要變更組態檔案才能啟用佈建。如需詳細資訊，請參閱Ping文件。總而言之，您必須將pingfederate-<version>/pingfederate/bin/run.properties檔案中的`pf.provisioner.mode`設定修改為 `OFF` (預設值) 以外的值，並在目前執行時重新啟動伺服器。例如，`STANDALONE`如果您目前沒有使用的高可用性組態，則可以選擇使用PingFederate。

若要在中設定佈建 PingFederate

1. 登入PingFederate管理主控台。
2. 從頁面頂端選取應用程式，然後按一下 SP 連線。
3. 找到您先前建立以與 IAM 身分中心形成 SAML 連線的應用程式，然後按一下連線名稱。
4. 從靠近頁面頂端的深色導覽標題中選取「連線類型」。您應該會看到瀏覽器 SSO 已從先前的 SAML 組態中選取。否則，您必須先完成這些步驟，然後才能繼續。
5. 選取輸出佈建核取方塊，選擇 IAM 身分識別中心雲端連接器做為類型，然後按一下儲存。如果 IAM 身分中心雲端連接器未顯示為選項，請確定您已安裝 IAM 身分中心連接器，並已重新啟動 PingFederate伺服器。
6. 重複按一下 [下一步]，直到到達 [輸出佈建] 頁面為止，然後按一下 [設定佈建] 按鈕。
7. 在先前的程序中，您會在 IAM 身分中心複製 SCIM 端點值。將該值貼到主PingFederate控台的 SCIM URL 欄位中。確保您刪除了 URL 末尾的正斜線。此外，在先前的程序中，您會在 IAM 身分中心複製存取權杖值。將該值粘貼到PingFederate控制台的「訪問令牌」字段中。按一下 Save (儲存)。
8. 在「通道組態 (設定通道)」頁面上，按一下「建立」。
9. 輸入此新啟動設定通道的通道名稱 (例如**`AWSIAMIdentityCenterchannel`**)，然後按下一步。
10. 在 [來源] 頁面上，選擇要用於連線至 IAM 身分中心的作用中資料存放區，然後按 [下一步]。

    > **Note**
    >
    > 如果尚未設定資料來源，則必須立即進行設定。有關如何在中選擇和配置資料來源的資訊，請參閱Ping產品文件PingFederate。

11. 在「來源設定」頁面上，確認您的安裝所有值都正確無誤，然後按一下「下一步」。
12. 在 [來源位置] 頁面上，輸入適合您資料來源的設定，然後按 [下一步]。例如，如果使用活動目錄作為 LDAP 目錄：

    a. 輸入 AD 樹系的基本 DN (例如**`DC=myforest,DC=mydomain,DC=com`**)。
    b. 在使用者 > 群組 DN 中，指定包含要佈建至 IAM 身分中心之所有使用者的單一群組。如果沒有這類單一群組存在，請在 AD 中建立該群組，返回此設定，然後輸入對應的 DN。
    c. 指定是否要搜尋子群組 (巢狀搜尋)，以及任何必要的 LDAP 篩選器。
    d. 在 [群組] > [群組 DN] 中，指定包含要佈建至 IAM 身分中心之所有群組的單一群組。在許多情況下，這可能與您在 [使用者] 區段中指定的 DN 相同。視需要輸入巢狀搜尋和篩選值。

13. 在 [屬性對應] 頁面上，確定下列事項，然後按 [下一步]：

a. 「user Name」欄位必須對應至格式化為電子郵件的「屬性」(user@domain.com)。它也必須符合使用者將用來登入 Ping 的值。此值會在聯合身分驗證期間填入 SAML `nameId` 宣告中，並用於在 IAM 身分中心與使用者進行比對。例如，使用「使用中目錄」時，您可以選擇指定`UserPrincipalName`為「使用 user Name」。

b. 其他以 * 為尾碼的欄位必須對應至您的使用者非空值的屬性。

14. 在「啟用與摘要」頁面上，將「通道狀態」 設定為「作用中」，以便在儲存設定後立即啟動同步。
15. 確認頁面上的所有組態值都正確無誤，然後按一下「完成」。
16. 在「管理頻道」頁面上，按一下「儲存」。
17. 此時，佈建會開始。若要確認活動，您可以檢視預設位於PingFederate伺服器pingfederate-<version>/pingfederate/log目錄中的 provisioner.log 檔案。
18. 若要驗證使用者和群組是否已成功同步至 IAM 身分中心，請返回 IAM 身分中心主控台，然後選擇 [使用者]。已同步處理的使用者PingFederate會顯示在 [使用者] 頁 您也可以在「群組」頁面上檢視同步處理的群組。

(選用) 步驟 3：在「IAM 身分中心」中設定 PingFed erate 中的使用者屬性以進行存取控制

PingFederate如果您選擇設定要在 IAM 身分中心用來管理AWS資源存取權限的屬性，則此為選用程序。您在中定義的屬性PingFederate會在 SAML 宣告中傳遞至 IAM 身分中心。然後，您將在 IAM 身分中心建立權限集，以根據傳遞的屬性來管理存取PingFederate。

開始此程序之前，必須先啟用此存取控制的屬性功能。如需如何進行該服務的詳細資訊，請參閱啟用和設定存取控制的屬性。

在PingFederate中設定 IAM 身分中心存取控制的使用者屬性

1. 登入PingFederate管理主控台。
2. 從頁面頂端選擇應用程式，然後按一下 SP 連線。
3. 找到您先前建立以與 IAM 身分中心形成 SAML 連線的應用程式，然後按一下連線名稱。
4. 從頁面頂端附近的深色導覽標題中選擇「瀏覽器 SSO」。然後點擊配置瀏覽器 SSO。
5. 在 [設定瀏覽器 SSO] 頁面上，選擇宣告建立，然後按一下設定宣告建立。
6. 在「設定宣告建立」頁面上，選擇「屬性合約」。
7. 在「屬性合約」頁面的「延伸合約」區段下，執行下列步驟來新增屬性：

a. 在文字方塊中`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**，輸入「IAM 身分中心」中要使**`AttributeName`**用的屬性名稱取代。例如 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**。

b. 針對「屬性名稱格式」，選擇urn:oasis:names:tc:SAML:2.0:attrname-format:uri。

c. 選擇 [新增]，然後選擇 [下一步]。

8. 在「驗證來源對應」頁面上，選擇您的應用程式設定的轉接器執行個體。

9. 在「屬性合約履行」頁面上，選擇「屬性合約」的「來源」(資料倉庫) 和「值」(資料倉庫屬性) *`https://aws.amazon.com/SAML/Attributes/AccessControl:`****`Department`***。

> **Note**
>
> 如果尚未設定資料來源，則需要立即進行設定。有關如何在中選擇和配置資料來源的資訊，請參閱Ping產品文件PingFederate。

10. 重複按一下 [下一步]，直到到達 [啟用與摘要] 頁面為止，然後按一下 [儲存]。

(選擇性) 傳遞屬性以進行存取控制

您可以選擇性地使用 IAM 身分中心中的存取控制的屬性功能來傳遞Name屬性設定為的`Attribute`元素`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**。此元素可讓您在 SAML 聲明中將屬性做為工作階段標籤傳遞。如需工作階段標籤的詳細資訊，請參閱 IAM 使用者指南AWS STS中的「傳遞工作階段標籤」。

若要將屬性做為工作階段標籤傳遞，請包含指定標籤值的 `AttributeValue` 元素。例如，若要傳遞標籤鍵值配對`CostCenter = blue`，請使用下列屬性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要新增多個屬性，請為每個標籤包含單獨的`Attribute`元素。

PingOne

IAM 身分中心支援將PingOne產品中的使用者資訊自動佈建 (同步處理) Ping Identity (以下稱為「Ping」) 進入 IAM 身分中心。此佈建使用系統進行跨網域身分識別管理 (SCIM) 2.0 通訊協定。您可以在PingOne使用 IAM 身分中心 SCIM 端點和存取權杖中設定此連線。設定 SCIM 同步時，您可PingOne以在中建立使用者屬性與 IAM 身分中心中指定屬性的對應。這會導致 IAM 身分中心和 PingOne.

本指南根據截至 2020 年 10 月PingOne為止。較新版本的步驟可能會有所不同。如需有關如何針 Ping對其他版本的 IAM 身分中心設定佈建的詳細資訊，請聯絡PingOne。本指南也包含一些有關透過 SAML 設定使用者驗證的注意事項。

下列步驟將逐步說明如何使用 SCIM 通訊協定啟PingOne用從 IAM 身分中心自動佈建使用者。

> **Note**
>
> 在開始部署 SCIM 之前，建議您先檢閱. 使用自動佈建的考量 然後繼續檢閱下一節中的其他考量。

主題

必要條件

在開始之前，您將需要以下內容：

- PingOne訂閱或免費試用，同時具有聯合驗證和佈建功能。如需有關如何取得免費試用的詳細資訊，請參閱Ping Identity網站。
- 已啟用 IAM 身分中心的帳戶 (免費)。如需詳細資訊，請參閱啟用 IAM 身分中心。

- PingOneIAM 身分中心應用程式已新增至您的PingOne管理入口網站。您可以從應用程式目錄取得 PingOne IAM 身分中心PingOne應用程式。如需一般資訊，請參閱從Ping Identity網站上的應用程式類別目錄新增應用程式。
- 從您的執行個PingOne體到 IAM 身分中心的 SAML 連線。將 PingOne IAM 身分中心應用程式新增至PingOne管理入口網站後，您必須使用該應用程式設定從PingOne執行個體到 IAM 身分中心的 SAML 連線。使用兩端的「下載」和「匯入」中繼資料功能，在PingOne和 IAM 身分中心之間交換 SAML 中繼資料。如需有關如何設定此連線的指示，請參閱PingOne文件。

其他考量

以下是有關PingOne此問題的重要考量，可能會影響您使用 IAM 身分中心實作佈建的方式。

- 自 2020 年 10 月PingOne起，不支援透過 SCIM 佈建群組。如Ping需 SCIM 中的群組支援的最新資訊，請連絡。PingOne
- 在PingOne管理入口網站停用佈建PingOne之後，可繼續佈建使用者。如果您需要立即終止佈建，請刪除相關的 SCIM 承載權杖，並/或自動佈建在 IAM 身分中心停用。
- 如果從中設定的資料存放區中移除使用者的屬性PingOne，則該屬性將不會從 IAM Identity Center 中的對應使用者中移除。這是PingOne's佈建程式實作中的已知限制。如果修改屬性，變更將同步至 IAM 身分中心。
- 以下是有關 SAML 組態的重要注意事項：PingOne
  - IAM 身分識別中心僅支援`emailaddress`一種`NameId`格式。這表示您需要為中的 SAML_THEME 對應選擇目錄中PingOne唯一且格式化為電子郵件 /UPN 的使用者屬性 (例如 user@domain.com)。 PingOne電子郵件 (Work) 是一個合理的值，可用於PingOne內建目錄的測試組態。
  - 電子郵件地址包含 + 字元的使用者可能無法登入 IAM 身分中心，但出現`'SAML_215'`或等錯誤`'Invalid input'`。PingOne若要修正此問題，請在中PingOne，針對「屬性對應」中的 SAML_ SUBLE 對應選擇「進階」選項。然後設置名稱 ID 格式發送到 SP：urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress在下拉菜單中。

步驟 1：在 IAM 身分中心啟用佈建

在第一個步驟中，您可以使用 IAM 身分中心主控台啟用自動佈建。

在 IAM 身分中心啟用自動佈建

1. 完成必要條件後，請開啟 IAM 身分中心主控台。

2. 在左側導覽窗格中選擇 [設定]。
3. 在 [設定] 頁面上，找出 [自動佈建資訊] 方塊，然後選擇 [啟用]。這會立即在 IAM 身分中心啟用自動佈建，並顯示必要的 SCIM 端點和存取權杖資訊。
4. 在「輸入自動佈建」對話方塊中，複製下列選項的每個值。稍後在 IdP 中配置佈建時，您將需要貼上這些內容。
   a. SCIM 端點
   b. 訪問令牌
5. 選擇關閉。

現在您已在 IAM 身分中心主控台中設定佈建，您需要使用 PingOne IAM 身分中心應用程式完成剩餘的工作。下列程序將說明這些步驟。

步驟 2：配置佈建 PingOne

使用 PingOne IAM 身分中心應用程式中的下列程序，以啟用 IAM 身分中心進行佈建。此程序假設您已將 PingOne IAM 身分中心應用程式新增至PingOne管理入口網站。如果您尚未這麼做，請參閱必要條件，然後完成此程序以設定 SCIM 佈建。

若要在中設定佈建 PingOne

1. 開啟您在設定 SAML PingOne (應用程式 > 我的應用程式) 時所安裝的 PingOne IAM 身分中心應用程式。請參閱 必要條件。
2. 捲動至頁面底部。在「使用者啟動設定」下，選擇完整連結以導覽至連線的使用者啟動設定組態。
3. 在 [啟動設定指示] 頁面上，選擇 [繼續下一步]。
4. 在先前的程序中，您會在 IAM 身分中心複製 SCIM 端點值。將該值貼到 PingOne IAM 身分中心應用程式的 SCIM URL 欄位中。確保您刪除了 URL 末尾的正斜線。此外，在先前的程序中，您會在 IAM 身分中心複製存取權杖值。將該值貼到身分識別中心應PingOne用程式的 ACCESS_TOKEN 欄位中。
5. 對於 REMOVE_ACTION，請選擇「已停用」或「已刪除」(如需詳細資訊，請參閱頁面上的說明文字)。
6. 在「屬性對應」頁面上，依照本頁面其他考量先前的指示，選擇要用於 SAML_THEMBER (NameId) 宣告的值。然後選擇「繼續下一步」。
7. 在「PingOne應用程式自訂-IAM 身分中心」頁面上，進行所需的自訂變更 (選用)，然後按一下繼續進行下一步。

8. 在「群組存取」頁面上，選擇包含您要啟用用於佈建和 IAM 身分中心單一登入之使用者的群組。選擇「繼續下一步」。
9. 捲動至頁面底部，然後選擇完成以開始佈建。
10. 若要驗證使用者是否已成功同步至 IAM 身分中心，請返回 IAM 身分中心主控台，然後選擇 [使用者]。同步處理的使用者PingOne將顯示在 [使用者] 頁面上。這些使用者現在可以指派到 IAM 身分中心內的帳戶和應用程式。

    請記住，PingOne不支援透過 SCIM 佈建群組或群組成員資格。聯繫以Ping獲取更多信息。

(選用) 步驟 3：在中設定使用者屬性，以PingOne便在 IAM 身分中心進行存取控制

PingOne如果您選擇設定 IAM 身分中心的屬性以管理AWS資源存取權，則此為選用程序。您在中定義的屬性會PingOne在 SAML 宣告中傳遞至 IAM 身分中心。然後，您可以在 IAM 身分中心建立權限集，以根據傳遞的屬性來管理存取權PingOne。

開始此程序之前，您必須先啟用此存取控制的屬性功能。如需如何進行該服務的詳細資訊，請參閱啟用和設定存取控制的屬性。

在PingOne中設定 IAM 身分中心存取控制的使用者屬性

1. 開啟您在設定 SAML PingOne (應用程式 > 我的應用程式) 時所安裝的 PingOne IAM 身分中心應用程式。
2. 選擇編輯，然後選擇繼續下一步，直到您進入「屬性對應」頁面。
3. 在 [屬性對應] 頁面上，選擇 [新增屬性]，然後執行下列動作。您必須針對要新增以在 IAM 身分中心用於存取控制的每個屬性執行這些步驟。

    a. 在「應用程式屬性」欄位中，輸入`https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`*。以 IAM 身分中心預期的屬性名稱取*`AttributeName`*代。例如 `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**。

    b. 在 Identity Bridge 屬性或常值欄位中，從PingOne目錄中選擇使用者屬性。例如，電子郵件（工作）。
4. 選擇 [下一步] 幾次，然後選擇 [完成]。

(選擇性) 傳遞屬性以進行存取控制

您可以選擇性地使用 IAM 身分中心中的存取控制的屬性功能來傳遞Name屬性設定為的Attribute元素https://aws.amazon.com/SAML/Attributes/AccessControl:**{TagKey}**。此元素可讓您在 SAML 聲明中將屬性做為工作階段標籤傳遞。如需工作階段標籤的詳細資訊，請參閱 IAM 使用者指南AWS STS中的「傳遞工作階段標籤」。

若要將屬性做為工作階段標籤傳遞，請包含指定標籤值的 AttributeValue 元素。例如，若要傳遞標籤鍵值配對CostCenter = blue，請使用下列屬性。

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

如果您需要新增多個屬性，請為每個標籤包含單獨的Attribute元素。

開始使用 IAM 身分中心的常見任務

如果您是 IAM 身分中心的新使用者，開始使用服務的基本工作流程為：

1. 如果您使用的是 IAM 身分中心的組織執行個體，或者如果您使用 IAM 身分中心的帳戶執行個體，AWS 帳戶 請登入管理帳戶的主控台並導覽至 IAM 身分中心主控台。
2. 從 IAM 身分中心主控台選取用於儲存使用者和群組身分的目錄。IAM 身分中心預設為您提供一個目錄，您可以用來設定使用者存取權限。如果您偏好使用其他身分識別來源，可以連線您的 Active Directory 或外部身分識別提供者。
3. 針對組織執行個體，請選取組織中 AWS 帳戶的帳戶，然後從目錄中選取使用者或群組，以及要授與使用者的權限，以指派使用者存取權限。
4. 提供使用者存取應用程式的方式：
   a. 透過從應用程式目錄中選擇其中一個預先整合的應用程式，或新增您自己的 SAML 2.0 應用程式，來設定客戶管理的 SAML 2.0 應用程式。
   b. 設定應用程式屬性。
   c. 將應用程式的存取權指派給使用者。我們建議您透過群組成員資格來指派使用者存取權，而非新增個別使用者權限。透過群組，您可以授與或拒絕使用者群組的權限，而不必將這些權限套用至每個使用者。如果使用者移至不同的組織，您只需將該使用者移至不同的群組即可。然後，使用者會自動接收新組織所需的權限。
5. 如果您使用預設的 IAM 身分中心目錄，請告知使用者如何登入 AWS 存取入口網站。IAM 身分中心的新使用者必須先啟用其使用者登入資料，才能用來登入 AWS 存取入口網站。如需詳細資訊，請參閱AWS 登入 使用者指南中的登入 AWS 存取入口網站

本節中的主題可協助您熟悉在完成 IAM 身分中心初始設定之後執行的一般工作。

如果您尚未啟用 IAM 身分中心，請參閱啟用 AWS IAM Identity Center。

主題

- 建立許可集合
- 為 IAM 身分中心使用者指派 AWS 帳戶 存取權
- 使用您的 IAM 身分中心登 AWS 入資料登入存取入口網站
- 指派群組的 AWS 帳戶 存取權
- 設定應用程式的單一登入存取權
- 檢視使用者和群組指派

建立許可集合

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。您建立的第一個權限集是系統管理權限集。如果您已完成其中入門教學課程一個已建立您的系統管理權限集。使用此程序建立權限集，如 IAM 使用者指南中的AWS 受管工作職能政策主題中所述。

1. 請執行下列任一項作業，以登入 AWS Management Console。
   - [新增至 AWS (root 使用者)] — 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。在下一頁中，輸入您的密碼。
   - 已在使用 AWS (IAM 登入資料) — 使用具有管理許可的 IAM 登入資料登入。
2. 開啟 IAM 身分中心主控台。
3. 在「IAM 身分中心」導覽窗格的「多帳戶權限」下，選擇「權限集」。
4. 選擇 Create permission set (建立許可集合)。
   a. 在 [選取權限集類型] 頁面的 [權限集類型] 區段中，選擇 [預先定義的權限集]。
   b. 在 [預先定義權限集的原則] 區段中，選擇下列其中一項：
      - AdministratorAccess
      - 帳單
      - DatabaseAdministrator
      - DataScientist
      - NetworkAdministrator
      - PowerUserAccess
      - ReadOnlyAccess
      - SecurityAudit
      - SupportUser
      - SystemAdministrator
      - ViewOnlyAccess
5. 在 [指定權限集詳細資料] 頁面上，保留預設設定，然後選擇 [下一步]。預設設定會將工作階段限制為一小時。
6. 在「檢閱並建立」頁面上，確認下列項目：
   1. 對於步驟 1：選取權限集類型，會顯示您選擇的權限集類型。
   2. 對於步驟 2：定義權限集詳細資訊，會顯示所選權限集的名稱。

3. 選擇建立。

建立套用最低權限權限的權限集

若要遵循套用最低權限權限的最佳作法，建立系統管理權限集之後，您可以建立更嚴格的權限集，並將其指派給一或多個使用者。在上一個程序中建立的權限集，可讓您評估使用者所需資源存取量的起點。若要切換至最低權限許可，您可以執行 IAM Access Analyzer 來監視具有 AWS 受管政策的主體。瞭解他們正在使用哪些權限之後，您可以撰寫自訂原則或產生僅具有團隊所需權限的原則。

使用 IAM 身分中心，您可以將多個權限集指派給同一位使用者。您的系統管理使用者也應該被指派其他、更具限制性的權限集。這樣，他們只能使用所需 AWS 帳戶 的權限來訪問您的，而不是始終使用其管理權限。

例如，如果您是開發人員，在 IAM Identity Center 中建立管理使用者之後，您可以建立授與許可的新`PowerUserAccess`權限集，然後將該權限集指派給您自己。與使用`AdministratorAccess`權限的管理權限集不同，權限集不允許管理 IAM 使用者和群組。`PowerUserAccess` 當您登入 AWS 存取入口網站以存取您的 AWS 帳戶時，您可以選擇`PowerUserAccess`而不是在`AdministratorAccess`帳戶中執行開發工作。

請謹記以下幾點考量：

- 若要快速開始建立更嚴格的權限集，請使用預先定義的權限集而非自訂權限集。

  使用預先定義的權限集 (使用預先定義的權限)，您可以從可用原則清單中選擇單一 AWS 受管理的原則。每個原則都會授與特定層級的 AWS 服務和資源存取權，或是一般工作職能的權限。如需這些原則的相關資訊，請參閱工作職能的AWS 受管理原則。
- 您可以設定權限集的工作階段持續時間，以控制使用者登入的時間長度 AWS 帳戶。

  當使用者聯合到其 AWS 帳戶 並使用 AWS 管理主控台或 AWS 命令列介面 (AWS CLI) 時，IAM Identity Center 會使用權限集上的工作階段持續時間設定來控制工作階段的持續時間。根據預設，[工作階段持續時間] 的值會決定使用者在將使用者登出工作階段 AWS 帳戶 之前 AWS 可登入的時間長度，會設定為一小時。您可以指定 12 小時的最大值。如需詳細資訊，請參閱 設定工作階段期。
- 您也可以設定 AWS 存取入口網站工作階段持續時間，以控制員工使用者登入入口網站的時間長度。

  根據預設，工作階段持續時間上限的值 (決定員工使用者在必須重新驗證之前可登入 AWS 存取入口網站的時間長度) 為八小時。您可以指定 90 天的最大值。如需詳細資訊，請參閱 設定 AWS 存取入口網站和 IAM 身分中心整合應用程式的工作階段持續時間。
- 當您登入 AWS 存取入口網站時，請選擇提供最低權限權限的角色。

您建立並指派給使用者的每個權限集，都會在 AWS 存取入口網站中顯示為可用角色。當您以該使用者身分登入入口網站時，請選擇與限制最嚴格的權限集合相對應的角色，而AdministratorAccess不是在帳戶中執行工作。

- 您可以將其他使用者新增至 IAM 身分中心，並將現有或新的權限集指派給這些使用者。

  如需詳細資訊，請參閱，指派群組的 AWS 帳戶 存取權。

為 IAM 身分中心使用者指派 AWS 帳戶 存取權

若要為 AWS 帳戶 IAM 身分中心使用者設定存取權限，您必須將該使用者指派給 AWS 帳戶 和權限集。

1. 請執行下列任一項作業，以登入 AWS Management Console。
   - [新增至 AWS (root 使用者)] — 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。在下一頁中，輸入您的密碼。
   - 已在使用 AWS (IAM 登入資料) — 使用具有管理許可的 IAM 登入資料登入。
2. 開啟 IAM 身分中心主控台。
3. 在功能窗格中的 [多帳戶權限] 下，選擇 AWS 帳戶[。
4. 在AWS 帳戶頁面上，會顯示組織的樹狀檢視清單。選取您要指派存取權的 AWS 帳戶 旁邊的核取方塊。如果您要設定 IAM 身分中心的管理存取權限，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 ## ##***] 頁面上，執行下列動作：
   1. 在 [使用者] 索引標籤上，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 [指派權限集給 [***AWS ## ##***] 頁面的 [權限集] 下，選取權限集，以定義使用者和群組對此的存取層級 AWS 帳戶。
8. 選擇下一步。
9. 對於步驟 3：複查並提交，請在「複查並提交指派至" ***AWS ## name*** "頁面上，執行下列動作：
   1. 檢閱選取的使用者和權限集。

2. 確認已將正確的使用者指派給權限集之後，請選擇 [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，直到程序順利完成為止。

10. 如果適用以下任一情況，請遵循中的步驟啟提示使用者輸入 MFA用 IAM 身分中心的 MFA：

- 您使用預設的身分識別中心目錄做為身分識別來源。
- 您使用的 AWS Managed Microsoft AD 目錄或自我管理目錄中的目錄做為您的身分識別來源，而且您沒有使用 RADIUS MFA 與. AWS 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 IdPs使用。

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，會在相關資訊中建立 AWS 帳戶，並將權限集中指定的政策附加至該角色。

使用您的 IAM 身分中心登 AWS 入資料登入存取入口網站

AWS 存取入口網站可讓 IAM 身分中心使用者透過入口網站存取其所有指派 AWS 帳戶 和應用程式的單一登入存取權。

完成下列步驟，以確認 IAM 身分中心使用者可以登入 AWS 存取入口網站並存取 AWS 帳戶。

1. 請執行下列任一項作業，以登入 AWS Management Console。

- [新增至 AWS (root 使用者)] — 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。在下一頁中，輸入您的密碼。
- 已使用 AWS (IAM 登入資料) — 使用您的 IAM 登入資料登入並選取管理員角色。

2. 開啟 IAM 身分中心主控台。
3. 在導覽窗格中，選擇 Dashboard (儀表板)。
4. 在 [儀表板] 頁面的 [設定摘要] 下，選擇 AWS 存取入口網站 URL。

5. 使用下列任一方式登入：

   - 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 Active Directory 或 IdP 使用者的認證登入。
   - 如果您使用預設的 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來登入。

1. 在「帳戶」選項卡中，找到您的 AWS 帳戶 並將其展開。
2. 這時系統顯示您可用的角色。例如，如果您同時獲指派權限集和帳單權限集，這些角色就會顯示在 AWS 存取入口網站中。AdministratorAccess選擇您要用於工作階段的 IAM 角色名稱。
3. 如果您被重新導向至 AWS 管理主控台，則表示您已成功完成設定 AWS 帳戶.

> **Note**
>
> 如果您沒有看到任何AWS 帳戶列出的內容，表示該使用者可能尚未指派給該帳戶的權限集。如需將使用者指派至權限集的指示，請參閱指派使用者存取權給 AWS 帳戶。

現在您已確認可以使用 IAM Identity Center 登入資料登入，請切換至用來登入 AWS Management Console 並從根使用者或 IAM 使用者登入資料登出的瀏覽器。

> **Important**
>
> 強烈建議您在登入 AWS 存取入口網站時使用 IAM Identity Center 管理使用者的登入資料來執行管理工作，而不是使用 IAM 使用者或根使用者登入資料。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。若要讓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。

指派群組的 AWS 帳戶 存取權

在 IAM Identity Center 中建立管理使用者並建立其他權限集後，您可以使用這些權限來執行具有最低權限的工作，您 AWS 帳戶 就可以為使用者群組提供存取權。

建議您直接將存取權指派給群組，而非個別使用者。例如，如果您根據組織單位建立群組和權限集，如果使用者移至不同的組織單位，您只需將該使用者移至不同的群組，他們就會自動收到新組織單位所需的權限，並失去先前組織單位的權限。

將使用者群組存取權指派給 AWS 帳戶

1. 開啟 IAM 身分中心主控台。

> **Note**
>
> 如果您的身分識別來源是 AWS Managed Microsoft AD 確定 IAM 身分中心主控台使用 AWS Managed Microsoft AD 目錄所在的區域，然後再進行下一個步驟。

2. 在功能窗格中的 [多帳戶權限] 下，選擇 AWS 帳戶[。
3. 在此AWS 帳戶頁面上，會出現組織的樹狀檢視清單。選取您要指派單一登入存取權的一或多 AWS 帳戶 個旁邊的核取方塊。

> **Note**
>
> 每個權限集最多可以選取 AWS 帳戶 10 個。

4. 選擇 [指派使用者或群組]。
5. 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-account-name*] 頁面上，選取 [群組] 索引標籤，然後選擇一或多個群組。

   若要篩選結果，請開始在搜尋方塊中輸入您要的群組名稱。

   若要顯示您選取的群組，請選擇 [選取的使用者和群組] 旁邊的橫向三角形。

   確認選取正確的群組後，請選擇 [下一步]。
6. 對於步驟 2: 選取權限集，在 [將權限集指派給 [*AWS-account-name*] 頁面上，選取一或多個權限集

> **Note**
>
> 如果您在開始此程序之前未建立所需的權限集，請選擇 [建立權限集]，然後遵循中的步驟建立許可集合。建立要套用的權限集之後，請在 IAM Identity Center 主控台中返回AWS 帳戶並遵循指示進行操作，直到到達「步驟 2：選取權限集」為止。當您執行此步驟時，請選取您建立的新權限集，然後繼續執行此程序的下一個步驟。

   確認選取正確的權限集之後，請選擇 [下一步]。

7. 對於步驟 3：複查並提交，請在「複查並提交指定至」***AWS-###############***作：

   1. 檢閱選取的群組和權限集。
   2. 確認選取正確的群組和權限集之後，請選擇 [提交]。

> **Important**
>
> 群組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，直到程序順利完成為止。

> **Note**
>
> 您可能需要授與使用者或群組在 AWS Organizations 管理帳戶中操作的權限。由於這是一個高度權限的帳戶，因此額外的安全限制要求您必須擁有 IAM FullAccess 政策或同等許可，然後才能進行設定。 AWS 組織中的任何成員帳戶都不需要這些額外的安全性限制。

或者，您可以使用AWS CloudFormation建立和指派權限集，以及將使用者指派給這些權限集。然後，使用者可以登入 AWS 存取入口網站或使用 AWS Command Line Interface (AWS CLI) 命令。

設定應用程式的單一登入存取權

IAM 身分中心支援兩種應用程式類型： AWS 受管應用程式和客戶受管應用程式

AWS 受管理的應用程式是直接從相關應用程式主控台內或透過應用程式 API 進行設定。

客戶受管應用程式必須新增至 IAM 身分中心主控台，並為 IAM 身分中心和服務提供者設定適當的中繼資料。您可以從支援 SAML 2.0 的常用應用程式目錄中進行選擇，也可以設定自己的 SAML 2.0 應用程式或 OAuth 2.0 應用程式。

設定應用程式的單一登入存取權限的組態步驟會因應用程式類型而有所不同。

設定 AWS 受管理的應用程式

AWS 亞馬遜受管的 Grafana 和 Amazon Monitron 等受管應用程式與 IAM 身分中心整合，可用於身分驗證和目錄服務。若要設定 AWS 受管應用程式與 IAM Identity Center 搭配使用，您必須直接從主控台為適用的服務設定應用程式，或者您必須使用應用程式 API。

從應用程式目錄設定應用程式

您可以從 IAM 身分中心主控台的常用應用程式目錄中選取 SAML 2.0 應用程式。使用此程序，在 IAM 身分中心和應用程式的服務提供者之間設定 SAML 2.0 信任關係。

從應用程式類別目錄設定應用程式

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 選擇「客戶管理」標籤。
4. 選擇新增應用程式。
5. 在 [選取應用程式類型] 頁面的 [設定] 偏好設定下，選擇 [我要從目錄中選取應用程式]。
6. 在 [應用程式類別目錄] 下，開始在搜尋方塊中輸入您要新增的應用程式名稱。
7. 當應用程式出現在搜尋結果中時，請從清單中選擇該應用程式的名稱，然後選擇 [下一步]。
8. 在 [設定應用程式] 頁面上，[顯示名稱] 和 [說明] 欄位會預先填入應用程式的相關詳細資訊。您可以編輯此資訊。
9. 在 IAM 身分中心中繼資料下，執行下列動作：

    a. 在 IAM 身分中心 SAML 中繼資料檔案下，選擇 [下載] 以下載身分識別提供者中繼資料。

    b. 在 [IAM 身分中心憑證] 下方，選擇 [下載憑證] 以下載身分提供者憑證。

    > **Note**
    >
    > 稍後當您從服務供應商的網站設定應用程式時，您將需要這些檔案。請遵循該供應商的說明執行。

10. (選擇性) 在應用程式屬性下，您可以指定應用程式啟動 URL、轉送狀態和工作階段持續時間。如需詳細資訊，請參閱 在 IAM 身分中心主控台中設定應用程式屬性。
11. 在應用程式中繼資料下，執行下列其中一個動作

    a. 如果您有中繼資料檔案，請選擇「上傳應用程式 SAML 中繼資料檔案」。然後，選擇選擇要查找的文件並選擇元數據文件。

    b. 如果您沒有中繼資料檔案，請選擇「手動輸入中繼資料值」，然後提供「應用程式 ACS URL」和「應用程式 SAML」對象值。

12. 選擇提交。您將被帶到剛剛添加的應用程序的詳細信息頁面。

設定您自己的 SAML 2.0 應用程式

使用此程序，在 IAM 身分中心和您自己的 SAML 2.0 應用程式的服務提供者之間設定您自己的 SAML 2.0 信任關係。開始此程序前，請確定您具有服務供應商的憑證和中繼資料交換檔案，以便完成信任的設定。

若要設定您自己的 SAML 2.0 應用程式

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 選擇「客戶管理」標籤。
4. 選擇新增應用程式。
5. 在 [選取應用程式類型] 頁面的 [設定] 偏好設定下，選擇 [我有要設定的應用程式]。
6. 在「應用程式類型」下，選擇「SAML 2.0」。
7. 選擇下一步。
8. 在 [設定應用程式] 頁面的 [設定應用程式] 下，輸入應用程式的顯示名稱，例如**MyApp**。然後，輸入「描述」。
9. 在 IAM 身分中心中繼資料下，執行下列動作：
   a. 在 IAM 身分中心 SAML 中繼資料檔案下，選擇 [下載] 以下載身分識別提供者中繼資料。
   b. 在 [IAM 身分中心憑證] 下方，選擇 [下載] 以下載身分提供者憑證。

   > **Note**
   > 稍後在您從服務供應商的網站設定自訂應用程式時，將需要這些檔案。

10. (選擇性) 在應用程式屬性下，您也可以指定應用程式啟動 URL、轉送狀態和工作階段持續時間。如需詳細資訊，請參閱 在 IAM 身分中心主控台中設定應用程式屬性。
11. 在 [應用程式中繼資料] 下方，選擇 [手動輸入您的 然後，提供「應用程式 ACS URL」和「應用程式 SAML」對象值。
12. 選擇提交。您將被帶到剛剛添加的應用程序的詳細信息頁面。

在您設定應用程式之後，您的使用者可以根據您指派的權限，從他們的 AWS 存取入口網站存取您的應用程式。

如果您有支援 OAuth 2.0 的客戶管理應用程式，而您的使用者需要從這些應用程式存取 AWS 服務，則可以使用受信任的身分傳播。透過受信任的身分傳播，使用者可以登入應用程式，而且該應用程式可以在要求中傳遞使用者身分，以存取 AWS 服務中的資料。如需詳細資訊，請參閱 將受信任的身分傳播與客戶管理的應用。

如需支援的應用程式類型的詳細資訊，請參閱管理應用程式的存取。

檢視使用者和群組指派

您可以從 [使用者和群組] 頁面查看誰有權存取 IAM 身分中心的內容。使用此程序可檢視使用者對 AWS 帳戶、權限集、應用程式和群組所具有的存取層級。

1. 開啟 IAM 身分中心主控台。
2. 根據您要編輯使用者群組還是個別指派的使用者群組，選擇「使用者」或「群組」。
3. 從清單中選擇使用者或群組。
4. 選擇是否要檢視帳戶指定、應用程式指派或群組指派：

   - AWS 帳戶和權限集指派
     1. 選擇 Accounts (帳戶) 標籤。
     2. 從清單中選取帳戶以檢視使用者和群組權限集指派。
     3. 選取要檢視的權限集，以檢視原則和指派詳細資料。
   - 應用指派
     1. 選擇 [應用程式] 索引標籤，以檢視指派給使用者或群組的應用程式。
     2. 從清單中選取應用程式，以檢視指派項目詳細資訊。
   - 群組指派
     1. 在「使用者」頁面中，選擇「群組」標籤。
     2. 選取群組以檢視使用者的群組指派。

管理 IAM 身分中心的組織和帳戶執行個體

執行個體是 IAM 身分中心的單一部署。IAM 身分中心有兩種類型的執行個體：組織執行個體和帳戶執行個體。

AWS 帳戶 可啟用 IAM 身分中心的類型

若要啟用 IAM 身分中心，請使用下列其中一個登入資料登入，視您要建立的執行個體類型而定： AWS Management Console

- 您的 AWS Organizations 管理帳戶 (建議使用) — 建立 IAM 身分中心的組織執行個體時必須使用。針對整個組織的多帳戶權限和應用程式指派，使用組織執行個體。
- 您的 AWS Organizations 成員帳戶 — 用於建立 IAM 身分中心的帳戶執行個體，以啟用該成員帳戶內的應用程式指派。組織中可以存在具有成員層級執行個體的一或多個帳戶。
- 獨立 AWS 帳戶 — 用於建立 IAM 身分中心的組織執行個體或帳戶執行個體。獨立版 AWS 帳戶 不由管理 AWS Organizations。只有一個 IAM Identity Center 執行個體可以與獨立執行個體建立關聯，AWS 帳戶 而且您可以將該執行個體用於該獨立應用程式指派 AWS 帳戶。

功能	AWS Organizations 管理帳戶中的執行個體 (建議)	成員帳戶中的執行個體	獨立執行個體 AWS 帳戶
管理使用者	是	是	是
AWS 存取入口網站，以單一登入存取 AWS 受管理的應用程式	是	是	是
OAuth 2.0 (OIDC) 客戶管理的應用程式	是	是	是

功能	AWS Organizations 管理帳戶中的執行個體 (建議)	成員帳戶中的執行個體	獨立執行個體 AWS 帳戶
多帳戶權限	是	否	否
AWS 存取入口網站，以單一登入存取您的 AWS 帳戶	是	否	否
客戶管理的應用程式	是	否	否
委派管理員可以管理實例	是	否	否

主題

- IAM 身分中心的組織執行個體
- IAM 身分中心的帳戶執行個體
- 在 IAM 身分中心主控台中啟用帳戶執行個體
- 使用服務控制策略控制帳戶實例的創建
- 建立 IAM 身分中心的帳戶執行個體

IAM 身分中心的組織執行個體

當您與 IAM 身分中心一起啟用時 AWS Organizations，您正在建立 IAM 身分中心的組織執行個體。您的組織執行個體必須在您的管理帳戶中啟用，而且您可以透過單一組織執行個體集中管理使用者和群組的存取。中的每個管理帳戶只能有一個組織實例 AWS Organizations。

如果您在 2023 年 11 月 15 日之前啟用了 IAM 身分中心，則您擁有 IAM 身分中心的組織執行個體。

何時使用組織實例

組織執行個體是啟用 IAM 身分中心的主要方法，在大多數情況下，建議使用組織執行個體。組織執行個體提供下列優點：

- Sup@@ port IAM 身分中心的所有功能 — 包括管理組織 AWS 帳戶 中多個人的許可，以及將存取權指派給客戶受管理的應用程式。
- 減少管理點數量 — 組織執行個體擁有單一管理點，即管理帳戶。我們建議您啟用組織執行個體，而不是帳戶執行個體，以減少管理點的數量。
- 控制帳戶執行個體的建立 — 只要您尚未在選擇加入區域中的組織部署 IAM Identity Center 的執行個體 (AWS 區域 預設為停用)，您就可以控制是否可由組織中的成員帳戶建立帳戶執行個體。

IAM 身分中心的帳戶執行個體

透過 IAM 身分中心的帳戶執行個體，您可以部署 AWS 受支援的受管理應用程式和以 OIDC 為基礎的客戶受管應用程式。帳戶執行個體利用 IAM Identity Center 員工身分識別和存取入口網站功能 AWS 帳戶，支援單一應用程式的隔離部署。

帳戶執行個體繫結至單一執行個體， AWS 帳戶 並且僅用於管理相同帳戶和中受支援應用程式的使用者和群組存取 AWS 區域。每個帳戶執行個體只能使用一個 AWS 帳戶。您可以從下列任一項目建立帳戶執行個體：

- 中的成員帳戶 AWS Organizations。
- 不受管理 AWS 帳戶 的獨立版 AWS Organizations。

成員帳戶的可用性限制

如果符合下列條件，您可以在組織的成員帳戶中部署帳戶執行個體：

- 在 2023 年 11 月 15 日之前，您的組織並未部署 IAM 身分中心的執行個體。
- 在 2023 年 11 月 15 日之前，您的組織已經部署了 IAM 身分中心的執行個體，而且您的管理員已啟用成員帳戶建立 IAM 身分中心的帳戶執行個體。
- 您的管理員尚未建立可防止成員帳戶建立帳戶執行個體的服務控制政策。
- 無論如何，您都沒有在同一個帳戶中擁有 IAM 身分中心的執行個體 AWS 區域。
- 您正在無法使用 IAM 身分中心的 AWS 區域 地方工作。如需「區域」的資訊，請參閱AWS IAM Identity Center 區域可用性。

主題

何時使用帳戶執行個體

在大多數情況下，建議使用組織實例。只有在下列其中一種情況適用時，才應使用帳戶執行個體：

- 您想要對 AWS 受支援的受管理應用程式執行臨時試用，以判斷應用程式是否符合您的業務需求。
- 您沒有計劃在整個組織中採用 IAM 身分中心，但您想要支援一或多個 AWS 受管理的應用程式。
- 您擁有 IAM Identity Center 的組織執行個體，但是想要將 AWS 受支援的受管理應用程式部署到與組織執行個體中使用者不同的隔離使用者集。

> **Important**
>
> 如果您打算使用 IAM 身分中心支援多個帳戶中的應用程式，請建立組織執行個體，且不要使用帳戶執行個體。

帳戶實例考量

帳戶執行個體是專為特殊使用案例所設計，提供組織執行個體可用的功能子集。建立帳戶執行個體之前，請考慮下列事項：

- 帳戶執行個體不支援權限集，因此不支援存取 AWS 帳戶。

- 您無法將帳戶執行個體轉換為組織執行個體。
- 您無法將帳戶執行個體合併至組織執行個體。
- 僅選擇AWS 受管理應用支持帳戶實例。
- 針對隔離的使用者使用帳戶執行個體，這些使用者只會在單一帳戶中使用應用程式，並在所使用的應用程式存留
- 附加至帳戶執行個體的應用程式必須保持連結至帳戶執行個體，直到您刪除應用程式及其資源為止。
- 帳戶實例必須保留在 AWS 帳戶 其創建的位置。

AWS 支援帳戶執行個體的受管應用

請參閱AWS 受管理應用以了解哪些 AWS 受管應用程式支援 IAM 身分中心的帳戶執行個體。驗證使用 AWS 受管理應用程式建立帳戶執行個體的可用性。

在 IAM 身分中心主控台中啟用帳戶執行個體

如果您在 2023 年 11 月 15 日之前啟用 IAM 身分中心，則您擁有 IAM 身分中心的組織執行個體，且會員帳戶建立帳戶執行個體的功能預設為停用。您可以透過啟用中的帳戶實例功能，選擇您的成員帳戶是否可以建立帳戶實例 AWS Management Console。

> **Note**
>
> 只要您尚未將 IAM Identity Center 的執行個體部署到選擇加入區域 (預設為停用) 的組織，不論部署日期為何，成員帳戶AWS 區域 就可以建立帳戶執行個體。在選擇加入中部署的 IAM 身分中心的任何組織執行個體都 AWS 區域 會阻止建立帳戶執行個體。如需「區域」的資訊，請參閱AWS IAM Identity Center 區域可用性。

啟用組織中的成員帳戶建立帳戶執行個體

1. 開啟 IAM 身分中心主控台。
2. 選擇 [設定]，然後選擇 [管理] 索引標籤。
3. 在「IAM 身分中心的帳戶執行個體」區段中，選擇「啟用 IAM 身分中心的帳戶執行個體」。
4. 在 [啟用 IAM 身分中心的帳戶執行個體] 對話方塊中，選擇 [啟用]，確認您要允許組織中的成員帳戶建立帳戶執行個體。

> **Important**
>
> 為成員帳戶啟用 IAM 身分中心的帳戶執行個體是一次性操作。這意味著此操作無法反轉。啟用後，您可以透過建立服務控制策略 (SCP) 來限制帳戶執行個體的建立。如需指示，請參閱使用服務控制原則控制帳戶執行個體建立。

使用服務控制策略控制帳戶實例的創建

使用者可以建立 IAM 身分中心執行個體繫結至單 AWS 帳戶一 (稱為 IAM 身分中心帳戶執行個體) 的執行個體。您可以使用服務控制策略 (SCP) 控制帳戶執行個體的建立。

1. 開啟 IAM 身分中心主控台。
2. 在 [儀表板] 的 [中央管理] 區段中，選擇 [防止帳戶執行個體] 按鈕。
3. 在 [附加 SCP 以防止建立新帳戶執行個體] 對話方塊中，會為您提供 SCP。複製 SCP 並選擇移至 SCP 儀表板按鈕。系統會將您導向AWS Organizations 主控台以建立 SCP，或將其作為陳述式附加至現有的 SCP。

   服務控制政策是的一項功能 AWS Organizations。如需有關附加 SCP 的指示，請參閱《AWS Organizations 使用者指南》中的〈附加和解除連結服務控制原則〉。

您可以將帳戶執行個體的建立限制為組織 AWS 帳戶 內的特定項目，而不是防止建立帳戶執行個體：

Example ：控制執行個體建立的 SCP

```
{
    "Version": "2012-10-17",
    "Statement" : [
        {
            "Sid": "DenyMemberAccountInstances",
            "Effect": "Deny",
            "Action": "sso:CreateInstance",
            "Resource": "*",
            "Condition": {
                 "StringNotEquals": {
                    "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
                }
            }
```

```
        }
    ]
}
```

建立 IAM 身分中心的帳戶執行個體

組織執行個體是啟用 IAM 身分中心的主要和建議方法。請確定您的使用案例支援建立帳戶執行個體，而且您知道考量事項。

從組織成員帳戶或獨立帳戶建立帳戶執行個體 AWS 帳戶

1. 請執行下列任一項作業，以登入 AWS Management Console。
   - [新增至 AWS (root 使用者)] — 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。在下一頁中，輸入您的密碼。
   - 已在使用 AWS (IAM 登入資料) — 使用具有管理許可的 IAM 登入資料登入。
2. 開啟 IAM 身分中心主控台。
3. 在「啟用 IAM 身分中心」下，選擇「啟用」。
4. 選擇繼續創建帳戶實例，然後選擇繼續。

> **Note**
>
> 如果存在 IAM 身分中心的組織執行個體，請確保您的使用案例需要自己的 IAM 身分中心帳戶執行個體。如果沒有，請選擇 [取消] 並使用組織執行個體。

5. 「選用」。新增您要與此帳戶執行個體建立關聯的標籤。

主控台中的通知表示帳戶執行個體已成功建立，並包含執行個體 ID。您可以在 「設定」摘要中為執行個體命名。

> **Note**
>
> 帳戶執行個體預設為啟用多因素驗證 (MFA)。當使用者的裝置、瀏覽器或位置變更時，系統會提示使用者使用 MFA 登入。作為安全性最佳實務，我們強烈建議您針對員工身分識別使用 MFA。了解 在 IAM 身分中心管理 MFA 裝置。

必須在 IAM Identity Center 主控台中完成管理功能，例如確認身分識別來源、調整多重要素驗證設定以及新增 AWS 受管理的應用程式。

身分驗證

使用者使用其使用者名稱登入 AWS 存取入口網站。當他們這樣做時，IAM 身分中心會根據與使用者電子郵件地址關聯的目錄，將請求重新導向至 IAM 身分中心身分驗證服務。通過驗證後，使用者可以對入口網站中顯示的任何 AWS 帳戶和第三方 software-as-a-service (SaaS) 應用程式進行單一登入存取，而無需額外的登入提示。這表示使用者不再需要針對每天使用的各種指派 AWS 應用程式追蹤多個帳戶認證。

驗證工作階

IAM 身分中心會維護兩種身分驗證工作階段：一種代表使用者登入 IAM 身分中心，另一種代表使用者對 AWS 受管理應用程式的存取權，例如 Amazon SageMaker Studio 或 Amazon 受管的 Grafana。每次使用者登入 IAM 身分中心時，系統就會針對 IAM 身分中心中設定的持續時間建立登入工作階段，最長可達 90 天。如需詳細資訊，請參閱 管理 AWS 存取入口網站和 IAM 身分中心整合應用程式的工作階段持續時間。每次使用者存取應用程式時，就會使用 IAM 身分中心登入工作階段來取得該應用程式的 IAM 身分中心應用程式工作階段。IAM Identity Center 應用程式工作階段具有可重新整理的 1 小時存留期，也就是說，只要從中取得 IAM 身分中心的登入工作階段仍然有效，IAM Identity Center 應用程式工作階段就會每小時自動重新整理一次。當使用者使用 IAM 身分中心存取 AWS Management Console 或 CLI 時，會使用 IAM 身分中心登入工作階段來取得 IAM 工作階段，如對應的 IAM 身分中心權限集中所指定 (更具體地說，IAM 身分中心會在目標帳戶中擔任 IAM 角色，該角色由 IAM 身分中心管理)。

當您在 IAM 身分中心停用或刪除使用者時，該使用者將立即無法登入以建立新的 IAM 身分中心登入工作階段。IAM Identity Center 登入工作階段會快取一小時，這表示當您在使用中的 IAM 身分中心登入工作階段期間停用或刪除使用者時，其現有的 IAM 身分中心登入工作階段最多可持續一小時，具體取決於上次重新整理登入工作階段的時間。在此期間，使用者可以啟動新的 IAM 身分中心應用程式和 IAM 角色工作階段。

IAM 身分中心登入工作階段到期後，使用者將無法再啟動新的 IAM 身分中心應用程式或 IAM 角色工作階段。不過，IAM Identity Center 應用程式工作階段最多可快取一個小時，如此使用者可能會在 IAM 身分中心登入工作階段過期後保留對應用程式的存取權最多一小時。任何現有的 IAM 角色會話都將根據 IAM 身分中心權限集中設定的持續時間（管理員可配置，最多 12 小時）繼續進行。

下表總結了這些行為：

使用者體驗/系統行為	使用者停用/刪除後的時間
使用者無法再登入 IAM 身分中心；使用者無法取得新的 IAM 身分中心登入工作階段	無 (立即生效)
使用者無法再透過 IAM 身分中心啟動新的應用程式或 IAM 角色工作階段	最多 1 小時
使用者無法再存取任何應用程式 (所有應用程式工作階段皆終止)	最多 2 小時 (IAM 身分中心登入工作階段到期最多 1 小時，加上 IAM 身分中心應用程式工作階段到期最多 1 小時)
使用者無法再 AWS 帳戶 透過 IAM 身分中心存取任何內容	最多 13 小時 (IAM 身分中心登入工作階段到期最多 1 小時，以及每個權限集的 IAM 身分中心工作階段持續時間設定，管理員設定的 IAM 角色工作階段到期最多 12 小時)

如需工作階段的詳細資訊，請參閱設定工作階段期。

管理員工身分

AWS Identity and Access Management(IAM) 可協助您安全地管理身分識別以及對AWS服務和資源的存取。身為 IAM 服務，AWS IAM Identity Center您可以AWS一次建立或連接員工身分識別，並集中管理對多個應用程式AWS 帳戶和應用程式的存取權。

對於 IAM 身分中心客戶，您集中管理多個AWS 帳戶或應用程式存取的方式並沒有變更。對於 IAM 身分中心的新客戶，您可以彈性地設定 IAM 身分中心，使其與身分識別中心同時執行，或使用 IAM AWS 帳戶 取代單一存取管理。

主題

使用案例

以下是說明如何使用 IAM 身分中心來滿足不同業務需求的使用案例。

主題

啟用應用程式的單一登入存取權 (AWS應用程式管理員角色)

如果您是管理 Amazon SageMaker 或之類的應用程式管理員AWS IoT SiteWise，且必須向使用者提供單一登入存取權，則此使用案AWS 受管理應用例提供指導。

在開始之前，請考慮下列事項：

- 是否要在的單獨組織中建立測試或生產環境AWS Organizations？
- 您的組織是否已啟用 IAM 身分中心？ 您是否擁有在的管理帳戶中啟用 IAM 身分中心的許可AWS Organizations？

檢閱下列指引，根據您的業務需求決定後續步驟。

在獨立配置我的AWS應用程序 AWS 帳戶

如果您必須提供AWS應用程式的單一登入存取權，並且知道您的 IT 部門尚未使用 IAM 身分中心，您可能需要建立獨立功能AWS 帳戶才能開始使用。根據預設，當您建立自己的組織時AWS 帳戶，您將擁有建立和管理自己AWS組織所需的權限。若要啟用 IAM 身分中心，您必須具有AWS 帳戶根使用者許可。

IAM 身分識別中心AWS Organizations可以在某些AWS應用程式的設定期間自動啟用 (例如，Amazon 受管 Grafana)。如果您的AWS應用程式未提供啟用這些服務的選項，您必須先設定AWS Organizations和 IAM 身分中心，才能提供應用程式的單一登入存取權。

我的組織中未設定 IAM 身分中心

在您身為應用程式管理員的角色中，視您的許可而定，您可能無法啟用 IAM 身分中心。IAM 身分中心需要AWS Organizations管理帳戶中的特定許可。在此情況下，請聯絡適當的管理員，在 Organizations 管理帳戶中啟用 IAM 身分中心。

如果您有足夠的許可來啟用 IAM 身分中心，請先執行此操作，然後繼續進行應用程式設定。如需詳細資訊，請參閱開始使用 IAM 身分中心的常見任務。

我的組織目前已設定 IAM 身分中心

在這個案例中，您可以繼續部署AWS應用程式，而不採取任何進一步的動作。

> **Note**
>
> 如果您的組織在 2019 年 11 月 25 日之前在管理帳戶中啟用 IAM 身分中心，您還必須在管理帳戶中啟用AWS受管理應用程式，並可選擇在成員帳戶中啟用受管理應用程式。如果您僅在管理帳戶中啟用它們，則可以稍後在成員帳戶中啟用它們。若要啟用這些應用程式，請在 IAM Identity Center 主控台的 [AWS受管應用程式] 區段的 [設定] 頁面中選擇 [啟用存取 如需詳細資訊，請參閱設定 IAM 身分中心以共用身分資訊 。

啟用對您的 Amazon EC2 Windows 執行個體的單一登入存取

如果您是管理身分中心目錄 (IAM 身分中心的預設身分識別來源) 或受支援的外部身分識別供應商 (IdP) 中的使用者的應用程式管理員，則可以啟用對 Amazon EC2 Windows 執行個體的單一登入存取權，而且必須從AWS叢集管理員主控台提供 IAM 身分中心存取您的 Amazon EC2 Windows 桌面。

透過此組態，您可以使用現有的公司登入資料安全地存取 Amazon EC2 Windows 執行個體。您不需要共享管理員憑據，多次訪問憑據或配置遠程訪問客戶端軟件。您可以跨多個大規模集中授予和撤銷 Amazon EC2 Windows 執行個體的存取權AWS 帳戶。例如，如果您將員工從 IAM 身分中心整合的身分識別來源中移除，他們就會自動失去所有AWS資源的存取權，包括 Amazon EC2 Windows 執行個體。

如需詳細資訊，請參閱如何使用 IAM 身分中心啟用對 Amazon EC2 Windows 執行個體的安全無縫單一登入。

如需如何設定 IAM 身分中心以啟用此功能的示範，請參閱使用 IAM 身分中心啟用對 Amazon EC2 Windows 的單一登入。

使用者、群組和佈建

在 IAM 身分中心與使用者和群組合作時，請牢記下列考量事項。

用戶名和電子郵件地址的唯一

IAM 身分中心中的使用者必須具備唯一識別身分。IAM 身分中心會實作使用者名稱，該名稱是您使用者的主要識別碼。雖然大多數人將使用者名稱設定為等於使用者的電子郵件地址，但 IAM 身分中心和 SAML 2.0 標準並不需要這樣做。不過，許多 SAML 2.0 型應用程式會使用電子郵件地址做為使用者的唯一識別碼。這些應用程式會從 SAML 2.0 身分識別提供者在驗證期間傳送的宣告中取得此資訊。此類應用程序取決於每個用戶的電子郵件地址的唯一性。基於這個原因，IAM 身分中心允許您指定電子郵件地址以外的其他內容進行使用者登入。IAM 身分中心要求使用者的所有使用者名稱和電子郵件地址都是非空值且唯一的。

群組

群組是您定義的使用者的邏輯組合。您可以建立群組，並將使用者新增至群組。IAM 身分中心不支援將群組新增至群組 (巢狀群組)。將存取權指派給AWS 帳戶和應用程式時，群組非常有用。您可以將權限授予群組，而不是個別指派每個使用者。稍後，當您從群組中新增或移除使用者時，使用者會動態取得或失去指派給群組之帳戶和應用程式的存取權。

使用者和群組佈建

佈建是指讓使用者和群組資訊可供 IAM Identity Center 和AWS受管理的應用程式或客戶管理的應用程式使用的程序。您可以直接在 IAM 身分中心建立使用者和群組，或與 Active Directory 或外部身分識別提供者中擁有的使用者和群組合作。IAM 身分中心必須了解使用者和群組AWS 帳戶，才能使用 IAM

身分中心指派使用者和群組存取權限。同樣地，AWS受管應用程式和客戶受管應用程式也可以與 IAM Identity Center 感知的使用者和群組一起使用。

IAM 身分中心的佈建會根據您使用的身分識別來源而有所不同。如需詳細資訊，請參閱 管理身分識別來源。

管理身分識別來源

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。設定身分識別來源後，您可以查詢使用者或群組，以授與他們對AWS 帳戶應用程式的單一登入存取權，或同時授與兩者。

在中，每個組織只能有一個身分識別來源AWS Organizations。您可以選擇下列其中一項作為身分識別來源：

- 身分識別中心目錄 — 當您第一次啟用 IAM 身分中心時，系統會自動將身分識別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您AWS 帳戶和應用程式。
- Active Directory — 如果您想要繼續使用目錄或中的自我管理AWS Managed Microsoft AD目錄來管理使用AWS Directory Service者，請選擇此選項。Active Directory (AD)
- 外部身分識別提供者 — 如果您要管理外部身分識別提供者 (IdP) 中的使用者，例如Okta或Microsoft Entra ID，請選擇此選項。

> **Note**
>
> IAM 身分識別中心不支援以 Samba4 為基礎的 Simple AD 做為身分識別來源。

主題

變更身分識別來源的考量

雖然您可以隨時變更身分識別來源，但建議您考慮此變更可能會對您目前的部署造成什麼影響。

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 中的管理使用者) 都將失去對其 AWS 帳戶 和應用程式的單一登入存取權。

在您變更 IAM 身分中心的身分識別來源之前，請先檢閱下列考量事項，然後再繼續操作。如果您想繼續變更身分識別來源，請參閱以變更身分識別來源取得更多資訊。

在 IAM 身份中心和活動目錄之間切換

如果您已經在 Active Directory 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目錄。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，請先執行此動作。

如果您已經在預設 Identity Center 目錄中管理使用者和群組，請考慮下列事項：

- 已移除指派並刪除使用者和群組 — 將您的身分識別來源變更為 Active Directory 會從身分識別中心目錄中刪除您的使用者和群組。此變更也會移除您的指派。在此情況下，變更為 Active Directory 之後，您必須將使用者和群組從 Active Directory 同步處理到識別中心目錄中，然後重新套用其指派。

  如果您選擇不使用 Active Directory，則必須在身分識別中心目錄中建立使用者和群組，然後進行指派。
- 刪除身分時不會刪除指派 — 刪除身分識別中心目錄中的身分時，對應的指派也會在 IAM 身分中心中刪除。不過，在 Active Directory 中，當身分識別遭到刪除 (無論是在使用中目錄或已同步的身分識別中)，對應的指派都不會刪除。
- 沒有 API 的輸出同步處理 — 如果您使用 Active Directory 做為身分識別來源，建議您謹慎使用建立、更新和刪除 API。IAM 身分中心不支援輸出同步，因此您的身分識別來源不會隨著您使用這些 API 對使用者或群組所做的變更而自動更新。
- 存取入口網站 URL 將會變更 — 變更身分識別中心和 Active Directory 之間的身分識別來源也會變更 AWS 存取入口網站的 URL。

如需 IAM 身分中心如何佈建使用者和群組的相關資訊，請參閱Connect 至目Microsoft AD錄。

從 IAM 身分中心變更為外部 IdP

如果您將身分識別來源從 IAM 身分中心變更為外部身分識別提供者 (IdP)，請考慮下列事項：

- 指派和成員資格可以使用正確的宣告 — 只要新的 IdP 傳送正確的宣告 (例如 SAML NameID)，您的使用者指派、群組指派和群組成員資格將繼續運作。這些宣告必須與 IAM 身分中心中的使用者名稱和群組相符。
- 沒有輸出同步 — IAM 身分中心不支援輸出同步，因此您的外部 IdP 不會隨著您在 IAM 身分中心所做的使用者和群組所做的變更而自動更新。
- SCIM 佈建 — 如果您使用 SCIM 佈建，身分提供者中的使用者和群組所做的變更只會在您的身分提供者傳送這些變更至 IAM 身分中心後反映在 IAM 身分中心。請參閱 使用自動佈建的考量。
- 復原 — 您可以隨時將身分識別來源還原為使用 IAM 身分中心。請參閱 從外部 IdP 變更為 IAM 身分中心。

如需 IAM 身分中心如何佈建使用者和群組的相關資訊，請參閱Connect 至外部身分識別提供者。

從外部 IdP 變更為 IAM 身分中心

如果您將身分識別來源從外部身分提供者 (IdP) 變更為 IAM 身分中心，請考慮下列事項：

- IAM 身分中心會保留您的所有指派。
- 強制重設密碼 — 在 IAM 身分中心擁有密碼的使用者可以使用舊密碼繼續登入。對於位於外部 IdP 且不在 IAM 身分中心的使用者，系統管理員必須強制重設密碼。

如需 IAM 身分中心如何佈建使用者和群組的相關資訊，請參閱在 IAM 身分中心管理身分識別。

從一個外部 IdP 變更為另一個外部 IdP

如果您已使用外部 IdP 做為 IAM 身分中心的身分來源，而且您變更為不同的外部 IdP，請考慮下列事項：

- 指派和成員資格使用正確的宣告 — IAM 身分中心會保留您的所有指派。只要新的 IdP 傳送正確的宣告 (例如 SAML NameID)，使用者指派、群組指派和群組成員資格就會繼續運作。

  當您的使用者透過新的外部 IdP 進行驗證時，這些宣告必須與 IAM 身分中心的使用者名稱相符。
- SCIM 佈建 — 如果您使用 SCIM 佈建至 IAM 身分中心，建議您檢閱本指南中的 IDP 特定資訊和 IdP 提供的文件，以確保啟用 SCIM 時，新的提供者能夠正確匹配使用者和群組。

如需 IAM 身分中心如何佈建使用者和群組的相關資訊，請參閱Connect 至外部身分識別提供者。

在使用中目錄與外部 IdP 之間變更

如果您將身分識別來源從外部 IdP 變更為作用中目錄，或從作用中目錄變更為外部 IdP，請考慮下列事項：

- 刪除使用者、群組和指派 — 所有使用者、群組和指派都會從 IAM 身分中心刪除。在外部 IdP 或作用中目錄中，不會影響任何使用者或群組資訊。
- 佈建使用者 — 如果您變更為外部 IdP，則必須設定 IAM 身分中心來佈建使用者。或者，您必須先手動佈建外部 IdP 的使用者和群組，然後才能設定指派。
- 建立指派和群組 — 如果您變更為 Active Directory，您必須使用 Active Directory 中目錄中的使用者和群組來建立指派。

如需 IAM 身分中心如何佈建使用者和群組的相關資訊，請參閱Connect 至目Microsoft AD錄。

變更身分識別來源

下列程序說明如何從 IAM 身分識別中心提供的目錄 (預設身分識別中心目錄) 變更為 Active Directory 或外部身分識別提供者，或相反地變更。繼續前，請檢閱中的資訊變更身分識別來源的考量。視您目前的部署而定，此變更可能會移除您在 IAM 身分中心設定的任何使用者和群組指派。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 帳戶和應用程式。

若要變更您的身分識別來源

1. 開啟IAM Identity Center 主控台。
2. 選擇 Settings (設定)。
3. 在「」設定頁面上，選擇身分識別來源標籤。選擇動作，然後選擇變更身分識別來源。
4. 下選擇身分識別來源下，選取您要變更的來源，然後選擇下一頁。

   如果您要變更為使用中目錄，請從下一頁的功能表中選擇可用的目錄。

   > **Important**
   >
   > 將身分識別來源變更為 Active Directory 或從中移除身分識別中心目錄中的使用者和群組。此變更也會移除您在 IAM 身分中心中設定的任何指派。

   如果您要切換至外部身分識別提供者，建議您遵循中的步驟如何連線至外部身分識別提供者。

5. 閱讀免責聲明並準備好繼續後，請輸入接受。
6. 選擇變更身分識別來源。如果您要將身分識別來源變更為 Active Directory，請繼續進行下一個步驟。
7. 將您的身分識別來源變更為使用中目錄會帶您前往設定頁面。在「」設定頁面上，執行下列任何一項操作：
   - 選擇啟動引導設定。如需如何完成引導設定程序的詳細資訊，請參閱引導式設定。
   - 在身分識別來源區段中，選擇動作，然後選擇管理同步設定您的同步範圍，要同步的使用者和群組清單。

管理所有身分識別來源類型的登入和屬性使用

IAM Identity Center 提供下列功能，可讓管理員控制 AWS 存取入口網站的使用情況、為存取入口網站和應用程式中的使用者設定工作階段持續時間，以及使用屬性進行存取控制。 AWS 這些功能可搭配 Identity Center 目錄或外部身分識別提供者做為您的身分識別來源使用

> **Note**
>
> 如果您使用 Active Directory 做為 IAM 身分識別中心的身分識別來源，則不支援工作階段管理。

主題

- 管理 AWS 存取入口網站和 IAM 身分中心整合應用程式的工作階段持續時間
- 設定 AWS 存取入口網站和 IAM 身分中心整合應用程式的工作階段持續時間
- 刪除 AWS 存取入口網站和 AWS 整合式應用程式的工作
- 支援的使用者和群組屬性

管理 AWS 存取入口網站和 IAM 身分中心整合應用程式的工作階段持續時間

IAM 身分中心管理員可以針對與 IAM 身分中心整合的兩個應用程式設定工作階段持續時間 AWS 存取入口網站。工作階段持續時間組態決定使用者需要多久重新驗證。IAM 身分中心管理員可以結束使用中 AWS 存取入口網站工作階段，這樣做也可以結束整合應用程式的工作階段。

如需詳細資訊，請參閱 設定 AWS 存取入口網站和 IAM 身分中心整合應用程式的工作階段持續時間。如需如何管理和使用者工作階段的詳細資訊，請參閱刪除 AWS 存取入口網站和 AWS 整合式應用程式的工作。

> **Note**
>
> 修改 AWS 存取入口網站工作階段持續時間和結束 AWS 存取入口網站工作階段不會影響您在權限集中定義的 AWS 管理主控台工作階段持續時間。

設定 AWS 存取入口網站和 IAM 身分中心整合應用程式的工作階段持續時間

AWS 存取入口網站 與 IAM Identity Center 整合式應用程式的身份驗證工作階段持續時間是指使用者無需重新驗證即可登入的最長時間長度。預設的工作階段持續時間為 8 小時。IAM 身分中心管理員可以指定不同的持續時間，從最少 15 分鐘到最長 90 天。如需驗證工作階段持續時間和使用者行為的詳細資訊，請參閱 身分驗證

下列主題提供設定 AWS 存取入口網站和 IAM Identity Center 整合應用程式工作階段持續時間的相關資訊。

主題

- 先決條件和考量事項
- 如何設定工作階段持續時間

先決條件和考量事項

以下是為 AWS 存取入口網站和 IAM Identity Center 整合式應用程式設定工作階段持續時間的先決條件和考量事項。

外部身分提供者

IAM 身分中心使用 SAML 宣告中的`SessionNotOnOrAfter`屬性來協助判斷工作階段的有效期限。

- 如果未`SessionNotOnOrAfter`在 SAML 宣告中傳遞， AWS 存取入口網站工作階段的持續時間不會受到外部 IdP 工作階段持續時間的影響。例如，如果您的 IdP 工作階段持續時間為 24 小時，而您在 IAM 身分中心設定 18 小時的工作階段持續時間，則您的使用者必須在 18 小時後在 AWS 存取入口網站中重新驗證。
- 如果`SessionNotOnOrAfter`在 SAML 宣告中傳遞，工作階段持續時間值會設定為較短的 AWS 存取入口網站工作階段持續時間和 SAML IdP 工作階段持續時間。如果您在 IAM 身分中心設定 72 小

時的工作階段持續時間，且 IdP 的工作階段持續時間為 18 小時，則您的使用者將可以存取 IdP 中定義的 18 小時內的 AWS 資源。

- 如果 IdP 的工作階段持續時間長於 IAM 身分中心中設定的工作階段，您的使用者將能夠根據他們與您的 IdP 仍然有效的登入工作階段，啟動新的 IAM 身分中心工作階段，而無需重新輸入其登入資料。

> **Note**
>
> 如果您使用 Active Directory 做為 IAM 身分識別中心的身分識別來源，則不支援工作階段管理。

AWS CLI 和 SDK 工作階段

如果您使用 AWS 軟體開發套件 (SDK) 或其他開 AWS 發工具以程式設計方式存取 AWS 服務，則必須符合下列先決條件，才能設定 AWS 存取入口網站和 IAM Identity Center 整合應用程式的工作階段持續時間。 AWS Command Line Interface

- 您必須在 IAM 身分中心主控台中設定 AWS 存取入口網站工作階段持續時間。
- 您必須在共用設定檔中定義單一登入設定的設 AWS 定檔。此設定檔是用來連線到 AWS 存取入口網站。我們建議您使用 SSO 權杖提供者組態。使用此配置，您的 AWS SDK 或工具可以自動檢索刷新的身份驗證令牌。如需詳細資訊，請參閱 AWS SDK 和工具參考指南中的 SSO 權杖提供者設定。
- 使用者必須執行支援工作階段管理的 AWS CLI 或 SDK 版本。

支援工作階段管理的最低版本 AWS CLI

以下是支援工作階段管理的最低版本。 AWS CLI

- AWS CLI 第 2 2 版或更新版本
- AWS CLI 第 1 版本 1.27.10 或更新版本

如需如何安裝或更新最新 AWS CLI 版本的相關資訊，請參閱安裝或更新最新版本的 AWS CLI.

如果您的使用者正在執行 AWS CLI，如果您在 IAM Identity Center 工作階段設定為到期之前重新整理權限集，且工作階段持續時間設定為 20 小時，而權限集的持續時間設定為 12 小時， AWS CLI 工作階段最多會執行 20 小時加上 12 小時，總共 32 小時。如需 IAM 身分中心 CLI 的詳細資訊，請參閱AWS CLI 命令參考。

支援 IAM 身分中心工作階段管理的 SDK 最低版本

以下是支援 IAM 身分中心工作階段管理的 SDK 最低版本。

SDK	最低版本
Python	1.26.10
PHP	3.245.0
Ruby	aws-sdk-core 3.167.0
Java V2	AWS 適用於 Java 第 2 版的開發套件 (2.18.13)
去 V2	整個開發套件：發行版本 -2022-11 和特定的圍棋模塊：憑證/版本 1.13.0，配置
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

如何設定工作階段持續時間

使用下列程序來設定 AWS 存取入口網站和 IAM 身分中心整合應用程式的工作階段持續時間。

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上，選擇 [驗證] 索引標籤。
4. 在 [驗證] 下，選擇 [工作階段設定] 旁邊的 [設定 設定工作階段設定對話方塊隨即出現。
5. 在 [設定工作階段設定] 對話方塊中，選取下拉式箭頭，選擇使用者的工作階段持續時間上限 (以分鐘、小時和天為單位)。選擇工作階段的長度，然後選擇 [儲存]。您返回 「設定」 頁面。

刪除 AWS 存取入口網站和 AWS 整合式應用程式的工作

使用下列程序來檢視和刪除 IAM 身分中心使用者的作用中工作階段。

若要刪除 AWS 存取入口網站和 IAM 身分中心整合應用程式的使用中工作階段

1. 開啟 IAM 身分中心主控台。
2. 選擇 Users (使用者)。
3. 在 [使用者] 頁面上，選擇您要管理其工作階段之使用者的使用者名稱。這將帶您進入包含用戶信息的頁面。
4. 在使用者的頁面上，選擇作用中工作階段索引標籤。作用中階段作業旁的括號內的數字表示此使用者目前作用中工作階段的數目。
5. 選取您要刪除的工作階段旁邊的核取方塊，然後選擇 [刪除工作階段]。會出現一個對話方塊，確認您正在刪除此使用者的作用中工作階段。閱讀對話方塊中的資訊，如果您要繼續，請選擇 [刪除工作階段]。
6. 您會返回使用者的頁面。會出現一個綠色的閃爍列，表示已順利刪除選取的工作階段。

如需撤銷驗證工作階段行為的詳細資訊，請參閱驗證工作階。

支援的使用者和群組屬性

屬性是可協助您定義和識別個別使用者或群組物件的資訊name，例如email、或members。IAM Identity Center 支援最常用的屬性，無論這些屬性是在使用者建立期間手動輸入，還是使用同步引擎自動佈建 (例如跨網域身分識別管理 (SCIM) 規格的系統中定義的。如需有關此規格的詳細資訊，請參閱 https://tools.ietf.org/html/rfc7642。如需手動和自動佈建的詳細資訊，請參閱使用者來自外部 IdP 時進行佈建。

由於 IAM 身分中心支援 SCIM 進行自動佈建使用案例，因此身分識別中心目錄支援 SCIM 規格中列出的所有相同使用者和群組屬性，但有一些例外情況。下列各節說明 IAM 身分中心不支援哪些屬性。

使用者物件

IAM 身分中心身分存放區支援 SCIM 使用者結構描述 (https://tools.ietf.org/html/rfc7643#section-8.3) 中的所有屬性，但下列項目除外：

- password
- ims
- photos
- entitlements
- x509Certificates

支援使用者的所有子屬性，下列項目除外：

- `'display'`任何多值屬性的子屬性 (例如，`emails`或) `phoneNumbers`
- `'version'`屬性的子屬性 `'meta'`

群組物件

支援 SCIM 群組結構描述 (https://tools.ietf.org/html/rfc7643#section-8.4) 中的所有屬性。

支援群組的所有子屬性，下列項目除外：

- `'display'`任何多值屬性的子屬性 (例如，成員)。

在 IAM 身分中心管理身分識別

IAM 身分中心為您的使用者和群組提供下列功能：

- 建立您的使用者與群組。
- 新增使用者做為各群組的成員。
- 為您的 AWS 帳戶 和應用程式指派具有所需存取層級的群組。

若要管理 IAM 身分中心存放區中的使用者和群組，請 AWS 支援身分識別中心動作中列出的 API 操作。

使用者位於 IAM 身分中心時進行佈建

當您直接在 IAM 身分中心建立使用者和群組時，系統會自動進行佈建。這些身分可立即用於進行指派，以及供應用程式使用。如需詳細資訊，請參閱 使用者和群組佈建。

變更身分識別來源

如果您偏好管理中的使用者 AWS Managed Microsoft AD，可以隨時停止使用身分識別中心目錄，而是使用將 IAM 身分中心連線到 Microsoft AD 中的目錄 AWS Directory Service。如需詳細資訊，請參閱的考量在 IAM 身份中心和活動目錄之間切換。

如果您偏好管理外部身分識別提供者 (IdP) 中的使用者，可以將 IAM 身分中心連線到 IdP 並啟用自動佈建。如需詳細資訊，請參閱的考量從 IAM 身分中心變更為外部 IdP。

主題

新增使用者

您在身分識別中心目錄中建立的使用者和群組只能在 IAM 身分中心使用。使用下列程序，使用 IAM 身分中心主控台將使用者新增至您的身分中心目錄。或者，您可以呼叫 AWS API 作業CreateUser來新增使用者。

若要新增使用者

1. 開啟 IAM 身分中心主控台。
2. 選擇 Users (使用者)。
3. 選擇 [新增使用者] 並提供下列必要資訊：

    a. 使用者名稱 — 需要此使用者名稱才能登入 AWS 存取入口網站，之後無法變更。必須介於 1 到 100 個字元之間。

    b. 密碼 — 您可以傳送包含密碼設定指示的電子郵件 (此為預設選項)，或產生一次性密碼。如果您要建立系統管理使用者並選擇傳送電子郵件，請務必指定可存取的電子郵件地址。

        i. 傳送附有密碼設定指示的電子郵件給此使用者。— 此選項會自動向使用者傳送一封來自 Amazon Web Services 的電子郵件，其中包含「邀請加入」 AWS IAM Identity Center (AWS 單一登入的後續任務)。電子郵件會代表貴公司邀請使用者存取 IAM 身分中心 AWS 存取入口網站。

> **Note**
>
> 在某些區域，IAM 身分中心會使用其他區域的 Amazon 簡易電子郵件服務傳送電子郵件給使用者 AWS 區域。如需如何傳送電子郵件的詳細資訊，請參閱跨區域通話。
>
> IAM 身分中心服務傳送的所有電子郵件都會來自地址no-reply@signin.aws.com或no-reply@login.awsapps.com。我們建議您設定電子郵件系統，使其接受來自這些寄件者電子郵件地址的電子郵件，並且不會將其視為垃圾郵件或垃圾郵件處理。

ii. 產生可與此使用者共用的一次性密碼。— 此選項為您提供 AWS 存取入口網站 URL 和密碼詳細資訊，您可以從您的電子郵件地址手動傳送給使用者。

c. 電子郵件地址 — 電子郵件地址必須是唯一的。

d. 確認電郵地址

e. 名字 — 您必須在此輸入名稱，自動佈建才能運作。如需詳細資訊，請參閱 自動佈建。

f. 姓氏 — 您必須在此輸入名稱，自動佈建才能運作。

g. 顯示名稱

> **Note**
>
> (選擇性) 如果適用，您可以指定其他屬性的值，例如使用者的 Microsoft 365 不可變 ID，以協助提供使用者對特定商務應用程式的單一登入存取權。

4. 選擇下一步。
5. 如果適用，請選取一或多個要新增使用者的群組，然後選擇 [下一步]。
6. 複查您在「步驟 1：指定使用者詳細資訊」和「步驟 2：新增使用者至群組-選用」中指定的資訊。按任一步驟選擇 「編輯」 以進行任何更改。確認兩個步驟都指定了正確的資訊之後，請選擇 [新增使用者]。

新增群組

使用下列程序，使用 IAM 身分中心主控台將群組新增至您的身分識別中心目錄。或者，您也可以呼叫 AWS API 作業CreateGroup來新增群組。

新增群組

1. 開啟 IAM 身分中心主控台。
2. 選擇 Groups (群組)。
3. 選擇 Create group (建立群組)。
4. 輸入「群組」名稱與「摘要」-選擇性。描述應提供有關已指派或將要指派給群組的權限的詳細資訊。在 [新增使用者至群組-選用] 底下，找出您要新增為成員的使用者。接著選取每個使用者旁的核取方塊。
5. 選擇 Create group (建立群組)。

將此群組新增至您的身分識別中心目錄後，您可以將單一登入存取權指派給此群組。如需詳細資訊，請參閱 指派使用者存取權給 AWS 帳戶。

將使用者新增至群組

請遵循下列程序，將使用者新增為先前使用 IAM 身分中心主控台在身分識別中心目錄中建立的群組成員。或者，您可以呼叫 AWS API 作業，CreateGroupMembership將使用者新增為群組的成員。

新增使用者做為群組的成員

1. 開啟 IAM 身分中心主控台。
2. 選擇 Groups (群組)。
3. 選擇您要更新的群組名稱。
4. 在群組詳細資料頁面的 [此群組中的使用者] 下，選擇 [新增使用者至群組]。
5. 在 [將使用者新增至群組] 頁面的 [其他使用者] 底下，找出您要新增為成員的使用者。然後，選取它們旁邊的核取方塊。
6. 選擇 Add users (新增使用者)。

刪除 IAM 身分中心中的群組

當您刪除 IAM Identity Center 目錄中的群組時，它會移除屬於此群組成員之所有使用者的存取權 AWS 帳戶 和應用程式。刪除群組後，就無法復原。使用下列程序，使用 IAM 身分中心主控台刪除身分中心目錄中的群組。

刪除 IAM 身分中心中的群組

> **Important**
>
> 此頁面上的說明適用於AWS IAM Identity Center。它們不適用於 AWS Identity and Access Management(IAM)。IAM 身分中心使用者、群組和使用者登入資料與 IAM 使用者、群組和 IAM 使用者登入資料不同。如果您正在尋找有關在 IAM 中刪除群組的說明，請參閱使用者指南中的刪除 IAM AWS Identity and Access Management 使用者群組。

1. 開啟 IAM 身分中心主控台。
2. 選擇 Groups (群組)。
3. 刪除群組的方法有兩種：
   - 在「群組」頁面上，您可以選取要刪除的多個群組。選取您要刪除的群組名稱，然後選擇 [刪除群組]。
   - 選擇您要刪除的群組名稱。在群組詳細資訊頁面上，選擇 [刪除群組]。
4. 系統可能會要求您確認刪除群組的意圖。
   - 如果您一次刪除多個群組，請在 [刪除群組] 對話方塊**Delete**中輸入以確認您的意圖。
   - 如果您刪除包含使用者的單一群組，請在 [刪除群組] 對話方塊中輸入要刪除的群組名稱來確認您的目的。
5. 選擇 Delete group (刪除群組)。如果您選取了多個要刪除的群組，請選擇刪除 # 群組。

刪除 IAM 身分中心中的使用者

當您刪除 IAM 身分中心目錄中的使用者時，會移除其對應用程式 AWS 帳戶 和應用程式的存取權限。刪除使用者之後，就無法復原。使用下列程序，使用 IAM 身分中心主控台刪除身分中心目錄中的使用者。

> **Note**
>
> 當您在 IAM Identity Center 中停用使用者存取權或刪除使用者時，該使用者將立即無法登入 AWS 存取入口網站，且無法建立新的登入工作階段。如需詳細資訊，請參閱 驗證工作階。

刪除 IAM 身分中心中的使用者

> **Important**
>
> 此頁面上的說明適用於AWS IAM Identity Center。它們不適用於 AWS Identity and Access Management(IAM)。IAM 身分中心使用者、群組和使用者登入資料與 IAM 使用者、群組和 IAM 使用者登入資料不同。如果您正在尋找有關在 IAM 中刪除使用者的說明，請參閱使用者指南中的刪除 IAM AWS Identity and Access Management 使用者。

1. 開啟 IAM 身分中心主控台。
2. 選擇 Users (使用者)。
3. 刪除使用者的方法有兩種：
   - 在 [使用者] 頁面上，您可以選取多個要刪除的使用者。選取您要刪除的使用者名稱，然後選擇 [刪除使用者]。
   - 選擇您要刪除的用戶名。在使用者詳細資訊頁面上，選擇刪除使用者。
4. 如果您一次刪除多個使用者，請在 [刪除使用者] 對話方塊**Delete**中輸入以確認您的意圖。
5. 選擇刪除使用者。如果您選取了多個要刪除的使用者，請選擇刪除 # 個使用者。

在 IAM 身分中心停用使用者存取權

當您停用 IAM Identity Center 目錄中的使用者存取權時，您無法編輯使用者詳細資料、重設密碼、將使用者新增至群組或檢視其群組成員資格。使用下列程序，使用 IAM 身分中心主控台停用身分中心目錄中的使用者存取權限。

> **Note**
>
> 當您在 IAM Identity Center 中停用使用者存取權或刪除使用者時，該使用者將立即無法登入 AWS 存取入口網站，且無法建立新的登入工作階段。如需詳細資訊，請參閱 驗證工作階。

在 IAM 身分中心停用使用者存取權

1. 開啟 IAM 身分中心主控台。

> **Important**
>
> 此頁面上的說明適用於AWS IAM Identity Center。它們不適用於 AWS Identity and Access Management(IAM)。IAM 身分中心使用者、群組和使用者登入資料與 IAM 使用者、群組和 IAM 使用者登入資料不同。如果您正在尋找關於在 IAM 中停用使用者的指示，請參閱使用AWS Identity and Access Management 者指南中的管理 IAM 使用者。

2. 選擇 Users (使用者)。
3. 選取您要停用其存取權的使用者名稱。
4. 在您要停用其存取權的使用者名稱下方，在 [一般資訊] 區段中，選擇 [停用使用者存取]。
5. 在 [停用使用者存取權] 對話方塊中，選擇 [停用使用者存取

編輯使用者屬性

使用下列程序，使用 IAM 身分中心主控台編輯身分中心目錄中使用者的屬性。或者，您可以呼叫 AWS API 作業UpdateUser來更新使用者屬性。

在 IAM 身分中編輯使用者屬性

1. 開啟 IAM 身分中心主控台。
2. 選擇 Users (使用者)。
3. 選擇您要編輯的使用者。
4. 在 [使用者設定檔] 頁面的 [設定檔詳細資料] 旁，選擇 [編輯]
5. 在 [編輯設定檔詳細資料] 頁面上，視需要更新屬性。然後，選擇 Save changes (儲存變更)。

> **Note**
>
> (選用) 您可以修改其他屬性，例如員工編號和 Office 365 不可變 ID，以協助將 IAM 身分識別中心中的使用者身分與使用者需要使用的特定商務應用程式對應。

> **Note**
>
> 「電子郵件地址」屬性是可編輯的欄位，而且您提供的值必須是唯一的。

重設使用者的 IAM 身分中心使用者密碼

此程序適用於需要為 IAM 身分中心目錄中的使用者重設密碼的管理員。您將使用 IAM 身分中心主控台來重設密碼。

身分識別提供者和使用者類型的注

- Microsoft使用中目錄或外部提供者 — 如果您要將身分識別中心連線到 Microsoft Active Directory 或外部提供者，則必須從 Active Directory 或外部提供者內部完成使用者密碼重設。這表示無法從 IAM 身分中心主控台重設這些使用者的密碼。
- IAM 身分中心目錄中的使用者 — 如果您是 IAM 身分中心使用者，則可以重設自己的 IAM 身分中心密碼，請參閱重設 IAM 身分中心使用者密碼。

重設 IAM 身分中心最終使用者的密碼

> **Important**
>
> 此頁面上的說明適用於AWS IAM Identity Center。它們不適用於 AWS Identity and Access Management(IAM)。IAM 身分中心使用者、群組和使用者登入資料與 IAM 使用者、群組和 IAM 使用者登入資料不同。如果您正在尋找有關變更 IAM 使用者密碼的指示，請參閱《使用AWS Identity and Access Management 者指南》中的「管理 IAM 使用者的密碼」。

1. 開啟 IAM 身分中心主控台。
2. 選擇 Users (使用者)。
3. 選取您要重設密碼之使用者的使用者名稱。
4. 在使用者詳細資訊頁面上，選擇 [重設密碼]。
5. 在 [重設密碼] 對話方塊中，選取下列其中一個選項，然後選擇 [重設密碼]：

   a. 傳送電子郵件給使用者，其中包含重設密碼的指示 — 此選項會自動向使用者傳送一封來自 Amazon Web Services 的電子郵件，引導使用者逐步瞭解如何重設密碼。

      > **Warning**
      >
      > 安全性最佳作法是在選取此選項之前，確認此使用者的電子郵件地址是否正確。如果將此密碼重設電子郵件傳送到錯誤或設定錯誤的電子郵件地址，惡意收件者可能會利用此密碼重設電子郵件來取得您 AWS 環境的未經授權存取。

b. 產生一次性密碼並與使用者共用密碼 — 此選項提供您可以從電子郵件地址手動傳送給使用者的密碼詳細資訊。

為從 API 創建的用戶發送電子郵件 OTP

當您使用 CreateUserAPI 作業建立使用者時，他們沒有密碼。您可以通過選擇在使用 API 創建時向用戶發送電子郵件一次性密碼（OTP）來更改此設置。用戶首次嘗試登錄時會收到電子郵件 OTP。收到電子郵件 OTP 後，當用戶登錄時，他們必須設置新密碼。如果您未啟用此設定，則必須產生 OTP，並與您使用 CreateUserAPI 建立的使用者共用 OTP。

向使用 CreateUserAPI 建立的使用者傳送電子郵件 OTP

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上，選擇 [驗證] 索引標籤。
4. 在 [標準驗證] 區段中，選擇 [設定]。
5. 會出現一個對話方塊。勾選「傳送電子郵件 OTP」旁邊的方塊。然後選擇 Save (儲存)。狀態會從「停用」更新為「已啟用」。

在 IAM 身分中心管理身分時的密碼要求

> **Note**
>
> 這些需求僅適用於在身分識別中心目錄中建立的使用者。如果您已設定 IAM Identity Center 以外的身分識別來源進行身分驗證 (例如Active Directory或外部身分提供者)，則會在這些系統 (而非 IAM Identity Center) 中定義和強制執行使用者的密碼政策。如果您的身分識別來源是 AWS Managed Microsoft AD，請參閱管理密碼策略以 AWS Managed Microsoft AD取得詳細資訊。

當您使用 IAM 身分識別中心做為身分識別來源時，使用者必須遵守下列密碼要求，才能設定或變更其密碼：

- 密碼區分大小寫。
- 密碼長度必須介於 8 到 64 個字元之間。
- 密碼必須包含以下四種類別中的至少一個字元：

- 小寫字母 (a-z)
- 大寫字母 (A-Z)
- 數字 (0-9)
- 非英數字元 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

- 最後三個密碼不能重複使用。
- 無法使用透過從第三方洩露的資料集公開已知的密碼。

Connect 至目Microsoft AD錄

使用時 AWS IAM Identity Center，您可以使用連線作用中目錄 (AD) 中的自我管理目錄或中 AWS Managed Microsoft AD 的 AWS Directory Service目錄。此 Microsoft AD 目錄定義了系統管理員在使用 IAM 身分中心主控台指派單一登入存取權時可從中提取的身分集區。將公司目錄連線至 IAM 身分中心後，您就可以授與 AD 使用者或群組存取應用 AWS 帳戶程式或兩者的存取權。

AWS Directory Service 幫助您設置和運行託管在 AWS 雲中的獨立 AWS Managed Microsoft AD 目錄。您還可以使用 AWS Directory Service 將 AWS 資源與現有的自我管理 AD 連接起來。若 AWS Directory Service 要設定為使用自我管理 AD，您必須先設定信任關係，才能將驗證延伸至雲端。

IAM 身分中心會使用提供的連線， AWS Directory Service 對來源 AD 執行個體執行傳遞驗證。當您用 AWS Managed Microsoft AD 作身分識別來源時，IAM 身分中心可以與來自透過 AD 信 AWS Managed Microsoft AD 任連線之任何網域的使用者搭配使用。如果您想要在四個或更多網域中尋找使用者，使用者在執行 IAM Identity Center 登入時，必須使用該`DOMAIN\user`語法做為其使用者名稱。

> **備註**
>
> - 作為先決步驟，請確定您的 AD Connector 或目錄 AWS Directory Service 位 AWS Managed Microsoft AD 於您的 AWS Organizations 管理帳戶內。如需詳細資訊，請參閱 在 IAM 身分中心確認您的身分來源。
> - IAM 身分識別中心不支援以 SAMBA 4 為基礎的 Simple AD 做為連線目錄。

使用作用中目錄的考量

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：

- 如果您使用的是 AWS Managed Microsoft AD，您必須在設定 AWS Managed Microsoft AD 目錄的相同 AWS 區域 位置啟用 IAM 身分中心。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。此外，請注意， AWS 存取入口網站使用與您的目錄相同的存取 URL。

- 使用位於管理帳戶中的活動目錄：

  您必須在中設定現有的 AD Connector 或 AWS Managed Microsoft AD 目錄 AWS Directory Service，而且必須位於您的 AWS Organizations 管理帳戶中。您一次只能連線一個 AD Connector 目錄或一個目錄。 AWS Managed Microsoft AD 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：

  - 將目錄 Connect AWS Managed Microsoft AD 到 IAM 身分中心
  - Connect 作用中目錄中的自我管理目錄連線至 IAM 身分識別中心
- 使用駐留在委託管理員帳戶中的活動目錄：

  如果您計劃啟用 IAM 身分中心委派管理員，並使用 Active Directory 做為您的 IAM 身分中心身分識別來源，則可以使用現有的 AD Connector 或 AWS Managed Microsoft AD 目錄設定在委派管理員帳戶中的 AWS 目錄。

  如果您決定將 IAM 身分中心身分識別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。

Connect 活動目錄並指定用戶

如果您已經在使用 Active Directory，下列主題將協助您準備將目錄連線到 IAM 身分識別中心。

您可以使用 IAM 身分識別中心來連線 Active Directory 中的目錄或自我管理目錄。 AWS Managed Microsoft AD 如果您打算連線 Active AWS Managed Microsoft AD Directory 中的目錄或自我管理的目錄，請確定您的 Active Directory 組態符合中在 IAM 身分中心確認您的身分來源的先決條件。

> **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。如果您計劃在 Active AWS Managed Microsoft AD Directory 中連線目錄或自我管理的目錄，但並未搭配使用 RADIUS MFA AWS Directory Service，請在 IAM 身分中心啟用 MFA。

AWS Managed Microsoft AD

1. 檢閱中的指引Connect 至目Microsoft AD錄。

2. 請遵循 將目錄 Connect AWS Managed Microsoft AD 到 IAM 身分中心 中的步驟。
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。

活動目錄中的自我管理目錄

1. 檢閱中的指引Connect 至目Microsoft AD錄。
2. 請遵循 Connect 作用中目錄中的自我管理目錄連線至 IAM 身分識別中心 中的步驟。
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。

外部 IdP

1. 檢閱中的指引Connect 至外部身分識別提供者。
2. 請遵循 如何連線至外部身分識別提供者 中的步驟。
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. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上選擇 [身分識別來源] 索引標籤，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] 索引標籤，然後選擇 [新增使用者和群組]。
5. 在 [使用者] 索引標籤的 [使用者] 下，輸入確切的使用者名稱並選擇 [新增]
6. 在新增的使用者和群組下，執行下列操作：

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. 選擇提交。

7. 在 [管理同步] 頁面中，您指定的使用者會出現在 [同步範圍內的使用者] 清單中。

8. 在導覽窗格中，選擇使用者 。

9. 在 [使用者] 頁面上，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。如需詳細資訊，請參閱 建立許可集合。

當使用者來自作用中目錄時佈建

IAM 身分識別中心會使用提供的連線， AWS Directory Service 將使用者、群組和成員資格資訊從 Active Directory 中的來源目錄同步至 IAM 身分識別中心身分存放區。沒有密碼資訊會同步至 IAM 身分識別中心，因為使用者身分驗證是直接從 Active Directory 中的來源目錄進行的。應用程式會使用此識別資料來促進應用程式內查閱、授權和協同作業案例，而不會將 LDAP 活動傳回 Active Directory 中的來源目錄。

如需上述佈建的詳細資訊，請參閱使用者和群組佈建。

主題

- 將目錄 Connect AWS Managed Microsoft AD 到 IAM 身分中心
- Connect 作用中目錄中的自我管理目錄連線至 IAM 身分識別中心
- AWS Managed Microsoft AD 目錄的屬性對應
- 從作用中目錄佈建使用者和群組

將目錄 Connect AWS Managed Microsoft AD 到 IAM 身分中心

使用下列程序將由其管理 AWS Managed Microsoft AD 的目錄連線 AWS Directory Service 到 IAM 身分中心。

若要連線 AWS Managed Microsoft AD 至 IAM 身分中心

1. 開啟 IAM 身分中心主控台。

> **Note**
>
> 在進行下一個步驟之前，請確定 IAM 身分中心主控台使用 AWS Managed Microsoft AD 目錄所在的其中一個區域。

2. 選擇設定。
3. 在 [設定] 頁面上，選擇 [識別來源] 索引標籤，然後選擇 [動作] > [變更身分識別來源]
4. 在 [選擇身分識別來源] 下，選取 [使用中的目錄]，然後選擇 [
5. 在 [Connect 使用中的目錄] 下， AWS Managed Microsoft AD 從清單中選擇一個目錄，然後選擇 [下一步]。
6. 在 [確認變更] 下，檢閱資訊，並在準備就緒時輸入 AC CEPT，然後選擇 [變更身分識別來源]

> **Important**
>
> 若要將 Active Directory 中的使用者指定為 IAM 身分中心的系統管理使用者，您必須先將要從 Active Directory 授與管理權限的使用者同步到 IAM 身分中心。若要啟用，請依照「將管理使用者同步至 IAM 身分中心」中的步驟進行。

Connect 作用中目錄中的自我管理目錄連線至 IAM 身分識別中心

Active Directory (AD) 中自我管理目錄中的使用者也可以在存取入口網站中擁有單一登入存 AWS 取權 AWS 帳戶 和應用程式。若要設定這些使用者的單一登入存取權，您可以執行下列其中一項作業：

- 建立雙向信任關係 — 在 AD 中建立雙向信任關係與自我管理目錄時，AD 中自我管理目錄中的使用者可以使用其公司認證登入各種 AWS 服務和商務應用程式。 AWS Managed Microsoft AD 單向信任不適用於 IAM 身分中心。

  AWS IAM Identity Center 需要雙向信任，以便它具有從您的網域讀取使用者和群組資訊的權限，以同步處理使用者和群組中繼資料。IAM 身分中心會在指派權限集或應用程式的存取權時使用此中繼資料。應用程式也會使用使用者和群組中繼資料進行協同作業，例如與其他使用者或群組共用儀表板時。從 AWS Directory Service Microsoft 活動目錄到您的域的信任允許 IAM 身份中心信任您的域進行身份驗證。相反方向的信任會授 AWS 予讀取使用者和群組中繼資料的權限。

  如需有關設定雙向信任的詳細資訊，請參閱《AWS Directory Service 管理指南》中的建立信任關係的時機。

- 建立 AD 連接器 — AD Connector 是一種目錄閘道，可將目錄要求重新導向至自我管理的 AD，而不會在雲端中快取任何資訊。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的 Connect 至目錄。

> **Note**
>
> 如果您要將 IAM 身分中心連線至 AD Connector 目錄，則 future 任何使用者密碼重設都必須在 AD 內完成。這表示使用者將無法從 AWS 存取入口網站重設其密碼。
> 如果您使用 AD 連接器將 Active Directory 網域服務連線至 IAM 身分識別中心，則 IAM 身分中心只能存取 AD Connector 所附加之單一網域的使用者和群組。如果您需要支援多個網域或樹系，請使 AWS Directory Service 用 Microsoft 作用中目錄。

> **Note**
>
> IAM 身分識別中心不適用於以 Samba4 為基礎的 Simple AD 目錄。

AWS Managed Microsoft AD 目錄的屬性對應

屬性對應用於將 IAM 身分中心中存在的屬性類型與 AWS Managed Microsoft AD 目錄中的類似屬性對應。IAM 身分識別中心會從您的 Microsoft AD 目錄擷取使用者屬性，並將其對應至 IAM 身分識別中心使用者屬性。這些 IAM 身分中心使用者屬性對應也可用於為您的應用程式產生 SAML 2.0 宣告。每個應用程式都會決定成功單一登入所需的 SAML 2.0 屬性清單。

IAM 身分中心在應用程式設定頁面上的 [屬性對應] 索引標籤下，為您預先填入一組屬性。IAM 身分中心會使用這些使用者屬性來填入傳送至應用程式的 SAML 宣告 (作為 SAML 屬性)。系統接下來從您的 Microsoft AD 目錄擷取這些使用者屬性。如需詳細資訊，請參閱 將應用程式中的屬性對應至 IAM 身分中心屬性。

IAM 身分中心也會在目錄設定頁面的「屬性對應」區段下為您管理一組屬性。如需詳細資訊，請參閱 將 IAM 身分中心中的屬性對應至 AWS Managed Microsoft AD 目錄中的屬性。

支援的目錄屬性

下表列出所有支援且可對應至 IAM 身分中心使用者屬性的 AWS Managed Microsoft AD 目錄屬性。

Microsoft AD 目錄中受支援的屬性
${dir:email}
${dir:displayname}
${dir:distinguishedName}
${dir:firstname}
${dir:guid}
${dir:initials}
${dir:lastname}
${dir:proxyAddresses}
${dir:proxyAddresses:smtp}
${dir:proxyAddresses:SMTP}
${dir:windowsUpn}

您可以指定任何支援 Microsoft AD 目錄屬性的組合，以對應至 IAM 身分識別中心中的單一可變屬性。例如，您可以在 IAM 身分中心欄的「使用者」屬性下選擇屬性。subject然後將其映射到${dir:displayname}${dir:lastname}${dir:firstname }或任何單個支持的屬性或任何支持屬性的任意組合。如需 IAM 身分中心中使用者屬性的預設對應清單，請參閱預設對映。

> **Warning**
>
> 某些 IAM 身分中心屬性無法修改，因為它們是不可變的，並且預設會對應至特定的 Microsoft AD 目錄屬性。
> 例如，「使用者名稱」是 IAM 身分中心的必要屬性。如果您將「使用者名稱」對應至具有空值的 AD 目錄屬性，IAM 身分中心會將該windowsUpn值視為「使用者名稱」的預設值。如果您想要從目前的對應變更「使用者名稱」的屬性對應，請在進行變更之前，確認與「使用者名稱」相依性的 IAM Identity Center 流程將繼續如預期般運作。

如果您使用ListUsers或 ListGroupsAPI 動作或list-users和 list-groups AWS CLI 命令來指派應用程式的使用者 AWS 帳戶 和群組存取權，則必須將的值指定AttributeValue為 FQDN。此值的格式必須如下：user@example.com。在下列範例中AttributeValue，設定為janedoe@example.com。

```
aws identitystore list-users --identity-store-id d-12345a678b --filters
 AttributePath=UserName,AttributeValue=janedoe@example.com
```

支援的 IAM 身分中心屬性

下表列出所有支援且可對應至 AWS Managed Microsoft AD 目錄中使用者屬性的 IAM 身分中心屬性。設定應用程式屬性對應後，您可以使用這些相同的 IAM 身分中心屬性來對應至該應用程式使用的實際屬性。

IAM 身分中心支援的屬性
${user:AD_GUID}
${user:email}
${user:familyName}
${user:givenName}
${user:middleName}
${user:name}
${user:preferredUsername}
${user:subject}

支援的外部身分識別提供

下表列出所有受支援的外部身分識別提供者 (IdP) 屬性，這些屬性可對應至您存取控制的屬性在 IAM 身分中心設定時可使用的屬性。使用 SAML 宣告時，您可以使用 IdP 支援的任何屬性。

IdP 中支援的屬性
${path:userName}

IdP 中支援的屬性
${path:name.familyName}
${path:name.givenName}
${path:displayName}
${path:nickName}
${path:emails[primary eq true].value}
${path:addresses[type eq "work"].streetAddress}
${path:addresses[type eq "work"].locality}
${path:addresses[type eq "work"].region}
${path:addresses[type eq "work"].postalCode}
${path:addresses[type eq "work"].country}
${path:addresses[type eq "work"].formatted}
${path:phoneNumbers[type eq "work"].value}
${path:userType}
${path:title}
${path:locale}
${path:timezone}
${path:enterprise.employeeNumber}
${path:enterprise.costCenter}
${path:enterprise.organization}
${path:enterprise.division}

IdP 中支援的屬性
`${path:enterprise.department}`
`${path:enterprise.manager.value}`

預設對映

下表列出 IAM Identity Center 中使用者屬性與 AWS Managed Microsoft AD 目錄中使用者屬性的預設對應。IAM 身分中心僅支援 IAM 身分中心欄中「使用者」屬性中的屬性清單。

> **Note**
>
> 如果在啟用可設定的 AD 同步時，在 IAM 身分中心中沒有任何使用者和群組的指派，則會使用下表中的預設對應。如需有關如何自訂這些對映的資訊，請參閱設定同步的屬性對應。

IAM 身分中心中的使用者屬性	對應至 Microsoft AD 目錄中的這個屬性
`AD_GUID`	`${dir:guid}`
`email` *	`${dir:windowsUpn}`
`familyName`	`${dir:lastname}`
`givenName`	`${dir:firstname}`
`middleName`	`${dir:initials}`
`name`	`${dir:displayname}`
`preferredUsername`	`${dir:displayname}`
`subject`	`${dir:windowsUpn}`

* IAM 身分中心中的電子郵件屬性在目錄中必須是唯一的。否則，JIT 登入程序可能會失敗。

您可以根據您的需求變更預設對應，或將更多屬性新增至 SAML 2.0 宣告。例如，假設您的應用程式需要 S `User.Email` AML 2.0 屬性中的使用者電子郵件。此外，假設電子郵件地址儲存在 Microsoft AD

目錄中的windowsUpn屬性中。若要達成此對應，您必須在 IAM 身分中心主控台的下列兩個位置進行變更：

1. 在 Directory (目錄) 頁面的 Attribute mappings (屬性對應) 區段下，您需要將使用者屬性 **email** 對應至 **${dir:windowsUpn}** 屬性 (位於 Maps to this attribute in your directory (對應至您目錄中的這個屬性) 欄)。
2. 在 [應用程式] 頁面上，從表格中選擇應用程式。選擇「屬性對應」頁籤。然後將User.Email屬性對應至**${user:email}**屬性 (在「對應至此字串值」或「IAM 身分中心」欄中的使用者屬性中)。

請注意，您必須以 $ {dir:**AttributeName**} 格式提供每個目錄屬性。例如，Microsoft AD 目錄中的 firstname 屬性要變為 ${dir:firstname}。請務必為每個目錄屬性指派實際值。在 ${dir: 之後缺少值的屬性將造成使用者登入問題。

將 IAM 身分中心中的屬性對應至 AWS Managed Microsoft AD 目錄中的屬性

您可以使用下列程序來指定 IAM 身分中心中的使用者屬性應如何對應至 Microsoft AD 目錄中對應的屬性。

將 IAM 身分中心中的屬性對應至目錄中的屬性

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上，選擇 [存取控制的屬性] 索引標籤，然後選擇 [管理屬性]。
4. 在 [管理存取控制屬性] 頁面上，在 IAM Identity Center 中尋找您要對應的屬性，然後在文字方塊中輸入值。例如，您可能想要將 IAM 身分識別中心使用者屬性對應**email**至 Microsoft AD 目錄屬性**${dir:windowsUpn}**。
5. 選擇儲存變更。

從作用中目錄佈建使用者和群組

IAM 身分識別中心提供下列兩種方式，從 Active Directory 佈建使用者和群組。

- IAM 身分識別中心可設定的作用中目錄 (AD) 同步 (建議使用) — 使用此同步方法，您可以執行下列動作：
  - 在 Microsoft Active Directory 中明確定義自動同步處理至身分識別中心的使用者和群組，藉此控制資料界限。您可以新增使用者和群組，或移除使用者和群組，以隨時變更同步範圍。

  - 指派同步處理的使用者和群組對應用程式的單一登入存取權 AWS 帳戶或存取 應用程式可以是 AWS 管理應用程式或客戶管理的應用程式
  - 視需要暫停並繼續同步來控制同步處理程序。這有助於您調節生產系統上的負載。
- 身分識別中心 AD 同步 — 透過這種同步方法，您可以使用 IAM 身分中心，將 Active Directory 中的使用者和群組存取權指派給 AWS 帳戶和應用程式。所有具有指派的身分都會自動同步至 IAM 身分中心。

IAM 身分識別中心可設定 AD 同步

IAM 身分識別中心可設定的使用中目錄 (AD) 同步功能可讓您明確設定 Microsoft Active Directory 中的身分識別，這些身分會自動同步至身分識別中心，並控制同步處理程序。

下列主題提供的資訊可讓您設定及管理可設定的 AD 同步處理。

主題

- 先決條件和考量事項
- 可設定 AD 同步的運作方式
- 設定和管理您的同步範圍

先決條件和考量事項

使用可設定的 AD 同步之前，請注意下列先決條件和考量事項：

- 在作用中目錄中指定要同步的使用者和群組

  您必須先在 Active Directory 中指定要同步的使用者和群組，然後將其同步至 AWS 帳戶 IAM 身分中心，才能使用 IAM 身分中心指派新使用者和群組存取受管理應用程式或客戶受管應用程式，以及存取權管理應用程式。 AWS
  - AD 同步 — 當您使用 IAM Identity Center 主控台或相關的指派 API 動作為新使用者和群組指派時，IAM Identity Center 會直接搜尋指定的使用者或群組、完成指派，然後定期將使用者或群組中繼資料同步至 IAM 身分中心。
  - 可設定的 AD 同步：IAM 身分中心不會直接搜尋使用者和群組的網域控制站。您必須先指定要同步的使用者和群組清單。您可以透過下列其中一種方式設定此清單 (也稱為同步範圍)，具體取決於您是否有已同步至 IAM Identity Center 的使用者和群組，或者您有新的使用者和群組是透過可設定的 AD 同步進行第一次同步。

  - 現有使用者和群組：如果您的使用者和群組已同步至 IAM Identity Center，則可設定 AD 同步中的同步範圍會預先填入這些使用者和群組的清單。若要指派新使用者或群組，您必須特別將使用者或群組新增至同步範圍。如需詳細資訊，請參閱 將使用者和群組新增至同步範圍。
  - 新使用者和群組：如果您想要指派應用程式的新使用者 AWS 帳戶 和群組存取權限，則必須指定要在可設定 AD 同步中新增至同步範圍的使用者和群組，然後才能使用 IAM Identity Center 進行指派。如需詳細資訊，請參閱 將使用者和群組新增至同步範圍。

- 在作用中目錄中指定巢狀群組

  屬於其他群組成員的群組稱為巢狀群組 (或子群組)。當您指派給 Active Directory 中包含巢狀群組的群組時，套用指派的方式取決於您使用 AD 同步還是可設定的 AD 同步。

  - AD 同步 — 當您指派給 Active Directory 中包含巢狀群組的群組時，只有群組的直屬成員可以存取該帳戶。例如，如果您將存取權指派給群組 A，而群組 B 是群組 A 的成員，則只有群組 A 的直屬成員可以存取該帳戶。群組 B 的成員不會繼承存取權。
  - 可設定的 AD 同步 — 使用可設定的 AD 同步，將指派給 Active Directory 中包含巢狀群組的群組，可能會增加具有應用程式存取權限 AWS 帳戶 或存取應用程式的使用者範圍。在此情況下，指派會套用至所有使用者，包括巢狀群組中的使用者。例如，如果您將存取權指派給群組 A，而群組 B 是群組 A 的成員，則群組 B 的成員也會繼承此存取權。
- 更新自動工作流

  如果您擁有使用 IAM 身分中心身分存放區 API 動作和 IAM 身分中心指派 API 動作的自動化工作流程，將新使用者和群組存取權指派給帳戶和應用程式，並將其同步至 IAM 身分中心，則必須在 2022 年 4 月 15 日之前調整這些工作流程，以便透過可設定的 AD 同步功能如預期運作。可設定的 AD 同步會變更使用者和群組指派和佈建的執行順序，以及執行查詢的方式。

  - AD 同步 — 指派程序會先進行。您可以將應用程式的存取權指派給使用者 AWS 帳戶 和群組。為使用者和群組指派存取權後，系統會自動佈建這些使用者和群組 (同步至 IAM 身分中心)。如果您有自動化工作流程，這表示當您將新使用者新增至 Active Directory 時，自動化工作流程可以使用身分識別存放區 `ListUser` API 動作來查詢使用者的 Active Directory，然後使用 IAM 身分識別中心指派 API 動作來指派使用者存取權。由於使用者具有指派，因此該使用者會自動佈建到 IAM 身分中心。
  - 可配置的 AD 同步 — 佈建首先進行，不會自動執行。相反地，您必須先將使用者和群組新增至同步範圍，將使用者和群組明確新增至識別身分存放區。如需自動化可設定 AD 同步之同步設定的建議步驟的詳細資訊，請參閱自動執行可設定 AD 同步的同步設定。

可設定 AD 同步的運作方式

IAM 身分中心會使用下列程序，重新整理身分識別存放區中以 AD 為基礎的身分識別資料。

建立

將 Active Directory 中的自我管理目錄或由 IAM 身分識別中心管理的 AWS Managed Microsoft AD 目錄連線 AWS Directory Service 到身分識別中心後，您可以明確設定要同步至 IAM 身分中心身分識別存放區的 Active Directory 使用者和群組。您選擇的身分會每三個小時左右同步至 IAM 身分中心身分存放區。視目錄大小而定，同步處理程序可能會花費較長的時間。

身為其他群組 (稱為巢狀群組或子群組) 成員的群組也會寫入識別身分存放區。當您指派給 Active Directory 中包含巢狀群組的群組時，套用指派的方式取決於您使用 AD 同步還是可設定的 AD 同步。如需詳細資訊，請參閱 Making assignments to nested groups in Active Directory。

您只能在新使用者或群組同步至 IAM 身分識別中心身分存放區後，將存取權指派給新使用者或群組。

更新

IAM 身分識別中心身分識別存放區中的身分識別資料會定期讀取 Active Directory 中的來源目錄中的資料，以保持最新狀態。身分識別中心預設會在同步週期內每小時同步處理 Active Directory 中的資料。根據您使用中目錄的大小，資料可能需要 30 分鐘到 2 小時才能同步到 IAM 身分中心。

在 IAM 身分識別中心建立或更新位於同步範圍內的使用者和群組物件及其成員資格，以對應至 Active Directory 中來源目錄中的對應物件。對於使用者屬性，在 IAM 身分中心中，僅更新 IAM 身分中心主控台 [存取控制屬性] 區段中列出的屬性子集。您在 Active Directory 中進行的任何屬性更新可能需要一個同步週期，才能反映在 IAM 身分識別中心。

您也可以更新同步至 IAM 身分識別中心身分存放區的使用者和群組子集。您可以選擇將新使用者或群組新增至此子集，或將其移除。您新增的任何身分識別會在下次排定的同步處理時同步處理。您從子集移除的身分識別將停止在 IAM 身分中心身分存放區中更新。任何未同步處理超過 28 天的使用者都會在 IAM 身分中心身分識別存放區中停用。對應的使用者物件將在下一個同步週期期間在 IAM Identity Center 身分存放區中自動停用，除非這些使用者物件屬於另一個仍屬於同步範圍的群組。

刪除

從 Active Directory 中的來源目錄中刪除對應的使用者或群組物件時，會從 IAM 身分識別中心身分存放區中刪除使用者和群組。或者，您可以使用 IAM 身分中心主控台，從 IAM 身分中心身分存放區明確刪除使用者物件。如果您使用 IAM 身分中心主控台，還必須從同步範圍中移除使用者，以確保他們不會在下一個同步週期中重新同步回 IAM 身分中心。

您也可以隨時暫停並重新啟動同步處理。如果您暫停同步處理超過 28 天，則會停用所有使用者。

設定和管理您的同步範圍

您可以使用下列其中一種方式設定同步範圍：

- 引導式設定：如果您是第一次將使用者和群組從 Active Directory 同步到 IAM 身分中心，請依照中的步驟設引導式設定定同步範圍。完成引導式設定之後，您可以隨時依照本節中的其他程序修改同步範圍。
- 如果您已經有同步至 IAM 身分中心的使用者和群組，或者您不想遵循指導式設定，請選擇 [管理同步]。略過指導式設定程序，並視需要遵循本節中的其他程序，以設定及管理同步範圍。

程序

- 引導式設定
- 將使用者和群組新增至同步範圍
- 從同步範圍移除使用者和群組
- 暫停並繼續同步
- 設定同步的屬性對應
- 自動執行可設定 AD 同步的同步設定

引導式設定

1. 開啟 IAM 身分中心主控台。

   > **Note**
   >
   > 在進行下一個步驟之前，請確定 IAM 身分中心主控台正 AWS 區域 在使用您 AWS Managed Microsoft AD 目錄所在的其中一個位置。

2. 選擇設定。
3. 在頁面頂端的通知訊息中，選擇 [開始引導式設定]。
4. 在步驟 1 — 選用：設定屬性對應中，檢閱預設使用者和群組屬性對應。如果不需要變更，請選擇「下一步」。如果需要變更，請進行變更，然後選擇 [儲存變更]。
5. 在步驟 2 — 選用：設定同步範圍中，選擇 [使用者] 索引標籤。然後，輸入您要新增至同步範圍之使用者的確切使用者名稱，然後選擇 [新增]。接下來，選擇組標籤。輸入您要新增至同步範圍之群

組的確切群組名稱，然後選擇 [新增]。然後選擇下一步。如果您想稍後將使用者和群組新增至同步範圍，請不要進行變更，然後選擇 [下一步]。

6. 在步驟 3：檢閱並儲存組態中，在步驟 2：同步範圍中的步驟 1：屬性對應以及您的使用者和群組中確認您的屬性對應。選擇 Save configuration (儲存組態)。這會帶您前往「管理同步」頁面。

將使用者和群組新增至同步範圍

新增使用者

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上選擇 [身分識別來源] 索引標籤，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] 索引標籤，然後選擇 [新增使用者和群組]。
5. 在 [使用者] 索引標籤的 [使用者] 下，輸入確切的使用者名稱並選擇 [新增]
6. 在 [新增的使用者和群組] 底下，檢閱您要新增的使用者。
7. 選擇提交。
8. 在導覽窗格中，選擇使用者 。
9. 在 [使用者] 頁面上，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。

若要新增群組

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上選擇 [身分識別來源] 索引標籤，選擇 [動作]，然後選擇 [管理同步]。
4. 在 [管理同步] 頁面上，選擇 [群組] 索引標籤，然後選擇 [新增使用者和群組]。
5. 選擇 Groups (群組) 標籤。在 [群組] 下，輸入確切的群組名稱並選擇 [新增]。
6. 在 [新增的使用者和群組] 底下，檢閱您要新增的群組。
7. 選擇提交。
8. 在導覽窗格中，選擇 Groups (AS 安全群組)。
9. 在 [群組] 頁面上，您指定的群組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群組清單。

從同步範圍移除使用者和群組

如需從同步範圍移除使用者和群組時會發生什麼情況的詳細資訊，請參閱可設定 AD 同步的運作方式。

若要移除使用者

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上選擇 [身分識別來源] 索引標籤，選擇 [動作]，然後選擇 [管理同步]。
4. 選擇 Users (使用者) 索引標籤。
5. 在 [同步範圍內的使用者] 底下，選取您要刪除之使用者旁邊的核取方塊。若要刪除所有使用者，請選取使用者名稱旁邊的核取方塊
6. 選擇移除。

若要移除群組

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上選擇 [身分識別來源] 索引標籤，選擇 [動作]，然後選擇 [管理同步]。
4. 選擇 Groups (群組) 標籤。
5. 在同步範圍內的群組下，選取您要刪除之使用者旁邊的核取方塊。若要刪除所有群組，請選取群組名稱旁的核取方塊。
6. 選擇移除。

暫停並繼續同步

暫停同步會暫停所有 future 的同步週期，並防止您對 Active Directory 中使用者和群組所做的任何變更反映在 IAM 身分識別中心。在您恢復同步之後，同步週期會從下一次排程的同步處理中取得這些變更。

若要暫停同步

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上選擇 [身分識別來源] 索引標籤，選擇 [動作]，然後選擇 [管理同步]。
4. 在「管理同步」下，選擇「暫停同步」

繼續同步

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上選擇 [身分識別來源] 索引標籤，選擇 [動作]，然後選擇 [管理同步]。
4. 在「管理同步」下，選擇「繼續同步」

> **Note**
>
> 如果您看到 [暫停同步] 而非 [繼續同步]，表示從 Active Directory 到 IAM 身分中心的同步作業已經繼續進行。

設定同步的屬性對應

如需有關可用屬性的詳細資訊，請參閱AWS Managed Microsoft AD 目錄的屬性對應。

若要將 IAM 身分中心中的屬性對應設定至您的目錄

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上選擇 [身分識別來源] 索引標籤，選擇 [動作]，然後選擇 [管理同步]。
4. 在「管理同步」下選擇「檢視屬性對應」。
5. 在 [使用中目錄使用者屬性] 下，設定 IAM 身分識別中心身分識別存放區屬性和使用中目錄 例如，您可能想要將 IAM 身分識別中心身分識別存放區屬性對應`email`至 Active Directory 使用者目錄屬性`${objectguid}`。

> **Note**
>
> 在 [群組屬性] 下，IAM 身分識別中心身分識別存放區屬性和使用中目錄群組屬性無法變更。

6. 選擇儲存變更。這樣您就會返回「管理同步」頁面。

自動執行可設定 AD 同步的同步設定

為了確保您的自動化工作流程透過可設定的 AD 同步功能如預期般運作，建議您執行下列步驟來自動化同步設定。

自動執行可設定 AD 同步的同步設定

1. 在 Active Directory 中，建立一個家長同步群組，以包含您要同步到 IAM 身分識別中心的所有使用者和群組。例如，您可以將群組命名為 IAM IdentityCenterAllUsersAndGroups。
2. 在 IAM 身分中心中，將家長同步群組新增至可設定的同步清單。IAM 身分中心會同步父系同步群組中包含之所有群組的所有使用者、群組、子群組和成員。
3. 使用 Microsoft 提供的 Active Directory 使用者和群組管理 API 動作，從上層同步群組新增或移除使用者和群組。

IAM 身分識別中心 AD 同步

透過 IAM 身分中心 AD 同步，您可以使用 IAM 身分中心，將 Active Directory 中的使用者和群組指派給受管理應用程式或客戶 AWS 受管應用程式的存取權限。 AWS 帳戶 所有具有指派的身分都會自動同步至 IAM 身分中心。

IAM 身分中心 AD 同步的運作方式

IAM 身分中心會使用下列程序，重新整理身分識別存放區中的 AD 型身分識別資料。

建立

當您使用 AWS 主控台或指派 API 呼叫將使用者 AWS 帳戶 或群組指派給應用程式或應用程式時，有關使用者、群組和成員資格的資訊會定期同步至 IAM Identity Center 身分識別存放區。新增至 IAM 身分中心指派的使用者或群組通常會在兩小時內出現在 AWS 身分識別存放區中。視同步處理的資料量而定，此程序可能需要更長的時間。只有直接指派存取權的使用者和群組，或是指派存取權之群組成員的使用者和群組才會進行同步處理。

身為其他群組 (稱為巢狀群組) 成員的群組也會寫入識別身分存放區。當您指派給 Active Directory 中包含巢狀群組的群組時，套用指派的方式取決於您使用 AD 同步還是可設定的 AD 同步。

- AD 同步 — 當您指派給 Active Directory 中包含巢狀群組的群組時，只有群組的直屬成員可以存取該帳戶。例如，如果您將存取權指派給群組 A，而群組 B 是群組 A 的成員，則只有群組 A 的直屬成員可以存取該帳戶。群組 B 的成員不會繼承存取權。
- 可設定的 AD 同步 — 使用可設定的 AD 同步，將指派給 Active Directory 中包含巢狀群組的群組，可能會增加具有應用程式存取權限 AWS 帳戶 或存取應用程式的使用者範圍。在此情況下，指派會套

用至所有使用者，包括巢狀群組中的使用者。例如，如果您將存取權指派給群組 A，而群組 B 是群組 A 的成員，則群組 B 的成員也會繼承此存取權。

如果使用者在使用者物件首次同步化之前存取 IAM Identity Center，則會使用 just-in-time (JIT) 佈建視需求建立該使用者的身分識別存放區物件。除非直接指派或以群組為基礎的 IAM 身分中心權利，否則由 JIT 佈建建建立的使用者不會進行同步。JIT 提供之使用者的群組成員資格在同步化之後才能使用。

如需如何將存取權指派給使用者的指示 AWS 帳戶，請參閱單一登入存取權 AWS 帳戶。

更新

IAM 身分識別中心身分識別存放區中的身分識別資料會定期讀取 Active Directory 中的來源目錄中的資料，以保持最新狀態。在 Active Directory 中變更的身分識別資料通常會在四小時內出現在 AWS 識別身分存放區中。視同步處理的資料量而定，此程序可能需要更長的時間。

在 IAM 身分中心建立或更新使用者和群組物件及其成員資格，以對應至 Active Directory 中來源目錄中的對應物件。對於使用者屬性，只會在 IAM 身分中心中更新 IAM 身分中心主控台的 [管理存取控制屬性] 區段中列出的屬性子集。此外，使用者屬性也會隨著每個使用者驗證事件更新。

刪除

從 Active Directory 中的來源目錄中刪除對應的使用者或群組物件時，會從 IAM 身分識別中心身分存放區中刪除使用者和群組。

Connect 至外部身分識別提供者

如果您在 Active Directory 中使用自我管理的目錄，或者 AWS Managed Microsoft AD，請參閱Connect 至目Microsoft AD錄。對於其他外部身分識別提供者 (IdPs)，您可 AWS IAM Identity Center 以使用 IdPs 透過安全性宣告標記語言 (SAML) 2.0 標準來驗證身分識別。這可讓您的使用者使用其公司認證登入 AWS 存取入口網站。然後，他們可以導覽至其指派的帳戶、角色和外部託管的應用程式 IdPs。

例如，您可以將外部 IdP (例如Okta或Microsoft Entra ID) 連線至 IAM 身分中心。然後，您的使用者可以使用其現有的Okta或Microsoft Entra ID認證登入 AWS 存取入口網站。若要控制使用者在登入後可執行的動作，您可以在 AWS 組織中的所有帳戶和應用程式中集中指派存取權限給他們。此外，開發人員可以使用現有憑據簡單地登錄 AWS Command Line Interface (AWS CLI)，並從自動短期憑證生成和輪換中受益。

SAML 通訊協定不提供查詢 IdP 以瞭解使用者和群組的方法。因此，您必須將這些使用者和群組佈建到 IAM 身分中心，讓 IAM 身分中心知道這些使用者和群組。

使用者來自外部 IdP 時進行佈建

使用外部 IdP 時，您必須先將所有適用的使用者和群組佈建至 IAM 身分中心，然後才能對應用程式進行 AWS 帳戶 任何指派。為此，您可以自動佈建為您的使用者和群組進行設定，或使用手動佈建。無論您如何佈建使用者，IAM 身分中心都會將命令列介面和應用程式身份驗證重新導向至您的外部 IdP。AWS Management Console然後，IAM 身分中心會根據您在 IAM 身分中心建立的政策授予這些資源的存取權。如需有關佈建的詳細資訊，請參閱使用者和群組佈建。

如何連線至外部身分識別提供者

有可用於支持的 step-by-step 教程 IdPs：

- CyberArk
- Google Workspace
- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- 平身份

對於不同支援的外部，有不同的先決條件、考量和佈建程序 IdPs。下列程序提供與所有外部身分識別提供者搭配使用之程序的一般概觀。

連線至外部身分識別提供者

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上，選擇 [識別來源] 索引標籤，然後選擇 [動作] > [變更身分識別來源]
4. 在選擇身分識別來源下，選取外部身分識別提供者，然後選擇下一步。
5. 在設定外部身分識別提供者下，執行下列操作：

    a. 在「服務提供者中繼資料」下，選擇「下載中繼資料檔案」以下載中繼資料檔案並將其儲存在系統 您的外部身分識別提供者需要 IAM 身分中心 SAML 中繼資料檔案。

    b. 在身分識別提供者中繼資料下，選擇選擇檔案，然後找出您從外部身分識別提供者下載的中繼資料檔案。然後上傳文件。此中繼資料檔案包含必要的公用 x509 憑證，用於信任從 IdP 傳送的訊息。

c. 選擇下一步。

> **Important**
>
> 將您的來源變更為或從 Active Directory 移除所有現有的使用者和群組指派。成功變更來源之後，您必須手動重新套用指派。

6. 閱讀免責聲明並準備繼續之後，請輸入 AC CEPT。
7. 選擇 [變更識別來源]。狀態訊息會通知您已成功變更身分識別來源。

主題

- 使用 SAML 和 SCIM 身分識別與外部身分識別提供者的聯合
- SCIM 設定檔和 SAML 2.0 實作

使用 SAML 和 SCIM 身分識別與外部身分識別提供者的聯合

IAM 身分中心針對聯合身分實作下列標準式通訊協定：

- 用於使用者驗證的 SAML 2.0
- 用於佈建的 SCIM

任何實作這些標準通訊協定的身分識別提供者 (IdP) 都可以與 IAM 身分中心成功互通，並注意下列特殊考量：

- SAML
  - IAM 身分識別中心需要使用 SAML NameID 格式的電子郵件地址 (也就是)。`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
  - 斷言中的 NameID 字段的值必須是 RFC 2822（https://tools.ietf.org/html/rfc2822）兼容添加規範（「」`name@domain.com`）字符串（https://tools.ietf.org/html/rfc2822#section-3.4.1）。
  - 中繼資料檔案不能超過 75000 個字元。
  - 中繼資料必須包含實體 ID、X509 憑證，並 SingleSignOnService作為登入網址的一部分。
  - 不支援加密金鑰。

- SCIM

- IAM 身分識別中心 SCIM 的實作是以 SCIM RFC 7642 (https://tools.ietf.org/html/rfc7642)、7643 (https://tools.ietf.org/html/rfc7643) 和 7644 (完整) 為基礎，以及 2020 年 3 月 FastFed 基本 SCIM 設定檔 1.0 (完整) 草案中列出的互通性要求。 https://tools.ietf.org/html/rfc7644 https://openid.net/specs/fastfed-scim-1_0-02.html#rfc.section.4 這些文件與 IAM 身分識別中心目前實作之間的任何差異，請參閱 IAM 身分中心 SCIM 實作開發人員指南的支援 API 作業一節。

IdPs 不支持不符合上述標準和注意事項的內容。請聯絡您的 IdP，以取得有關其產品符合這些標準和考量的問題或說明。

如果您在將 IdP 連線到 IAM 身分中心時遇到任何問題，建議您檢查：

- AWS CloudTrail 通過對事件名稱 ExternalIdP 進行過濾記錄 DirectoryLogin
- IDP 特定的記錄檔和/或偵錯記錄檔
- IAM 身分中心問題疑難排解

> **Note**
>
> 有些 IdPs (例如中的) 會以專為 IAM 身分中心建置的「應用程式」或「連接器」形式入門教學課程，為 IAM 身分中心提供簡化的組態體驗。如果您的 IdP 提供此選項，建議您使用它，請謹慎選擇專為 IAM 身分中心建置的項目。其他名為「AWS」、「同AWS 盟」或類似的一般「AWS」名稱的項目可能會使用其他同盟方法和/或端點，而且可能無法如預期般運作 IAM 身分中心。

SCIM 設定檔和 SAML 2.0 實作

SCIM 和 SAML 都是設定 IAM 身分中心的重要考量因素。

SAML 2.0 實作

IAM 身分中心支援使用 SAML (安全性宣告標記語言) 2.0 聯合身分識別。這可讓 IAM 身分中心驗證來自外部身分識別提供者的身分識別 (IdPs)。SAML 2.0 是用於安全交換 SAML 判斷提示的開放標準。SAML 2.0 會在 SAML 授權單位 (稱為身分識別提供者或 IdP) 和 SAML 取用者 (稱為服務提供者或 SP) 之間傳遞使用者的相關資訊。IAM 身分中心服務會使用此資訊來提供聯合單一登入。單一登入可讓使用者根據現有的身分識別提供者認證存取 AWS 帳戶 和設定的應用程式。

IAM 身分中心將 SAML IdP 功能新增至您的 IAM 身分中心存放區或外部身分識別提供者。 AWS Managed Microsoft AD然後，使用者可以單一登入支援 SAML 的服務，包括 AWS Management Console 和第三方應用程式，例如Microsoft 365Concur、和Salesforce。

然而，SAML 通訊協定並未提供查詢 IdP 以瞭解使用者和群組的方法。因此，您必須將這些使用者和群組佈建到 IAM 身分中心，讓 IAM 身分中心知道這些使用者和群組。

SCIM 設定檔

IAM 身分識別中心為跨網域身分識別管理 (SCIM) 2.0 版標準的系統提供支援。SCIM 可讓您的 IAM 身分中心身分與 IdP 中的身分識別保持同步。這包括您的 IdP 和 IAM 身分中心之間使用者的任何佈建、更新和取消佈建。

如需如何實作 SCIM 的詳細資訊，請參閱自動佈建。如需 IAM 身分中心 SCIM 實作的其他詳細資訊，請參閱 IAM 身分中心 SCIM 實作開發人員指南。

主題

- 自動佈建
- 手動佈建
- 管理 SAML 2.0 憑證

自動佈建

IAM 身分中心支援使用跨網域身分識別管理系統 (SCIM) 2.0 通訊協定，將身分提供者 (IdP) 的使用者和群組資訊自動佈建 (同步) 至 IAM 身分中心。設定 SCIM 同步時，您可以建立身分識別提供者 (IdP) 使用者屬性與 IAM 身分中心中具名屬性的對應。這會導致 IAM 身分中心和 IdP 之間的預期屬性相符。您可以使用適用於 IAM 身分中心的 SCIM 端點以及在 IAM 身分中心建立的承載權杖，在 IdP 中設定此連線。

主題

- 使用自動佈建的考量
- 如何監控訪問令牌到期
- 如何啟用自動佈建
- 如何停用自動佈建
- 如何生成新的訪問令牌
- 如何刪除訪問令牌

- 如何旋轉訪問令牌

使用自動佈建的考量

在開始部署 SCIM 之前，我們建議您先檢閱下列有關如何與 IAM 身分中心搭配使用的重要考量事項。有關其他佈建考量，請參閱入門教學課程適用於 IdP 的內容。

- 如果您要佈建主要電子郵件地址，則此屬性值對於每個使用者都必須是唯一的。在某些情況下 IdPs，主要電子郵件地址可能不是真實的電子郵件地址。例如，它可能是只看起來像電子郵件的通用主要名稱 (UPN)。這些電子郵件地址 IdPs 可能包含使用者真實電子郵件地址的次要或「其他」電子郵件地址。您必須在 IdP 中設定 SCIM，以將非空唯一電子郵件地址對應至 IAM 身分中心主要電子郵件地址屬性。而且您必須將使用者非 Null 唯一登入識別碼對應至 IAM 身分中心使用者名稱屬性。檢查您的 IdP 是否具有單一值，即登入識別碼和使用者的電子郵件名稱。如果是這樣，您可以將該 IdP 欄位對應至 IAM 身分中心主要電子郵件和 IAM 身分中心使用者名稱。
- 若要使用 SCIM 同步處理，每個使用者都必須指定「名字」、「姓氏」、「使用者名稱」和「顯示名稱」值。如果使用者遺漏這些值中的任何一個，將不會佈建該使用者。
- 如果您需要使用協力廠商應用程式，您首先需要將輸出 SAML 主旨屬性對應至使用者名稱屬性。如果協力廠商應用程式需要可傳遞的電子郵件地址，您必須將電子郵件屬性提供給 IdP。
- SCIM 佈建和更新間隔由您的身分識別提供者控制。身分供應商將這些變更傳送至 IAM 身分中心後，身分供應商對使用者和群組的變更才會反映在 IAM 身分中心。如需使用者和群組更新頻率的詳細資訊，請洽詢您的身分提供者。
- 目前，多值屬性 (例如指定使用者的多個電子郵件或電話號碼) 未使用 SCIM 佈建。嘗試使用 SCIM 將多值屬性同步至 IAM 身分中心將會失敗。若要避免失敗，請確定每個屬性只傳遞一個值。如果您的使用者具有多值屬性，請移除或修改 IdP 中 SCIM 中的重複屬性對應，以連線至 IAM 身分中心。
- 確認 IdP 上的 `externalId` SCIM 對應與唯一、永遠存在且最不可能為使用者變更的值相對應。例如，您的 IdP 可能會提供保證`objectId`或其他識別碼，這些識別碼不受使用者屬性變更 (例如名稱和電子郵件) 的影響。如果是這樣，您可以將該值對應至 SCIM `externalId` 欄位。如此可確保您的使用者在需要變更其名稱或電子郵件時，不會遺失 AWS 權利、指派或權限。
- 尚未指派給應用程式或 AWS 帳戶 無法佈建至 IAM 身分中心的使用者。若要同步使用者和群組，請確定這些使用者和群組已指派給應用程式或代表您 IdP 與 IAM 身分中心連線的其他設定。
- 使用者取消佈建行為由身分識別提供者管理，並可能因其實作而有所不同。如需取消佈建的詳細資訊，請洽詢您的身分識別提供者。

如需 IAM 身分中心 SCIM 實作的詳細資訊，請參閱 IAM 身分識別中心 SCIM 實作開發人員指南。

如何監控訪問令牌到期

SCIM 存取權杖的有效期為一年。當您的 SCIM 存取權杖設定為 90 天或更短時間到期時，請在 IAM 身分中心主控台和 AWS Health 儀表板 AWS 傳送提醒給您，以協助您輪換權杖。藉由在 SCIM 存取權杖到期前輪換，您可以持續保護自動佈建使用者和群組資訊的安全性。如果 SCIM 存取權杖到期，您的身分供應商將使用者和群組資訊同步處理到 IAM 身分中心會停止，因此自動佈建無法再進行更新或建立和刪除資訊。中斷自動佈建可能會增加安全風險，並影響您對服務的存取。

身分中心主控台提醒會持續存在，直到您輪換 SCIM 存取權杖並刪除任何未使用或過期的存取權杖為止。 AWS Health 儀表板事件每週更新 90 至 60 天，每週兩次，從 60 到 30 天，每週三次，從 30 到 15 天，以及從每天 15 天更新，直到 SCIM 存取權杖到期為止。

如何啟用自動佈建

使用下列程序，使用 SCIM 通訊協定啟用從 IdP 到 IAM 身分中心的使用者和群組自動佈建。

> **Note**
>
> 在開始此程序之前，我們建議您先檢閱適用於 IdP 的佈建考量。如需詳細資訊，請參入門教學課程閱 IdP 的。

在 IAM 身分中心啟用自動佈建

1. 完成必要條件後，請開啟 IAM 身分中心主控台。
2. 在左側導覽窗格中選擇 [設定]。
3. 在 [設定] 頁面上，找出 [自動佈建資訊] 方塊，然後選擇 [啟用]。這會立即在 IAM 身分中心啟用自動佈建，並顯示必要的 SCIM 端點和存取權杖資訊。
4. 在「輸入自動佈建」對話方塊中，複製下列選項的每個值。稍後在 IdP 中配置佈建時，您將需要貼上這些內容。
   a. SCIM 端點
   b. 訪問令牌
5. 選擇關閉。

完成此程序後，您必須在 IdP 中設定自動佈建。如需詳細資訊，請參入門教學課程閱 IdP 的。

如何停用自動佈建

使用下列程序在 IAM 身分中心主控台中停用自動佈建。

> **Important**
>
> 您必須先刪除存取權杖，然後才能啟動此程序。如需詳細資訊，請參閱 如何刪除訪問令牌。

在 IAM 身分中心主控台中停用自動佈建

1. 在 IAM 身分中心主控台中，選擇左側導覽窗格中的 [設定]。
2. 在 [設定] 頁面上，選擇 [識別來源] 索引標籤，然後選擇 [動作] > [管理佈建]。
3. 在 [自動佈建] 頁面上，選擇 [停用]。
4. 在 [停用自動佈建] 對話方塊中，檢閱資訊，輸入 DISABLE，然後選擇 [停用自動佈建]。

如何生成新的訪問令牌

使用下列程序在 IAM 身分中心主控台中產生新的存取權杖。

> **Note**
>
> 此程序需要您先前已啟用自動佈建。如需詳細資訊，請參閱 如何啟用自動佈建。

若要產生新的存取權杖

1. 在 IAM 身分中心主控台中，選擇左側導覽窗格中的 [設定]。
2. 在 [設定] 頁面上，選擇 [識別來源] 索引標籤，然後選擇 [動作] > [管理佈建]。
3. 在 [自動佈建] 頁面的 [存取權杖] 下，選擇 [產生權杖]。
4. 在 [產生新的存取權杖] 對話方塊中，複製新的存取權杖並將其儲存在安全的位置。
5. 選擇關閉。

如何刪除訪問令牌

使用下列程序刪除 IAM 身分中心主控台中的現有存取權杖。

若要刪除現有的存取權杖

1. 在 IAM 身分中心主控台中，選擇左側導覽窗格中的 [設定]。
2. 在 [設定] 頁面上，選擇 [識別來源] 索引標籤，然後選擇 [動作] > [管理佈建]。
3. 在 [自動佈建] 頁面的 [存取權杖] 下，選取要刪除的存取權杖，然後選擇 [刪除]。
4. 在 [刪除存取權杖] 對話方塊中，檢閱資訊、輸入 DELETE，然後選擇 [刪除存取權杖]。

如何旋轉訪問令牌

IAM 身分中心目錄一次最多支援兩個存取權杖。要在任何輪替之前生成其他訪問令牌，請刪除任何過期或未使用的訪問令牌。

如果您的 SCIM 存取權杖即將到期，您可以使用下列程序輪替 IAM 身分中心主控台中的現有存取權杖。

若要旋轉存取權杖

1. 在 IAM 身分中心主控台中，選擇左側導覽窗格中的 [設定]。
2. 在 [設定] 頁面上，選擇 [識別來源] 索引標籤，然後選擇 [動作] > [管理佈建]。
3. 在 [自動佈建] 頁面上的 [存取權杖] 下，記下您要輪換的權杖 ID。
4. 依照中的步如何生成新的訪問令牌驟建立新權杖。如果您已經創建了 SCIM 訪問令牌的最大數量，則首先需要刪除其中一個現有令牌。
5. 前往身分提供者的網站，設定用於 SCIM 佈建的新存取權杖，然後使用新的 SCIM 存取權杖測試與 IAM 身分中心的連線。確認使用新 Token 的佈建成功運作後，請繼續執行此程序的下一個步驟。
6. 按照中的步驟如何刪除訪問令牌刪除您之前提到的舊訪問令牌。您也可以使用權杖的建立日期作為要移除哪個權杖的提示。

手動佈建

有些 IdPs 不具備跨網域身分識別管理 (SCIM) 的系統支援，或具有不相容的 SCIM 實作。在這些情況下，您可以透過 IAM 身分中心主控台手動佈建使用者。將使用者新增至 IAM 身分中心時，請務必將使用者名稱設定為與 IdP 中的使用者名稱相同。您至少必須擁有唯一的電子郵件地址和使用者名稱。如需詳細資訊，請參閱 用戶名和電子郵件地址的唯一。

您也必須在 IAM 身分中心手動管理所有群組。若要這麼做，您可以建立群組並使用 IAM 身分中心主控台新增群組。這些群組不需要與 IdP 中存在的內容相符。如需詳細資訊，請參閱 群組。

管理 SAML 2.0 憑證

IAM 身分中心使用憑證在 IAM 身分中心與您的外部身分提供者 (IdP) 之間設定 SAML 信任關係。在 IAM 身分中心新增外部 IdP 時，您還必須從外部 IdP 取得至少一個公用 SAML 2.0 X.509 憑證。該憑證通常會在建立信任期間在 IdP SAML 中繼資料交換期間自動安裝。

身為 IAM 身分中心管理員，您偶爾需要以較新的 IdP 憑證取代較舊的憑證。例如，當憑證的到期日臨近時，您可能需要取代 IdP 憑證。以較新的憑證取代舊憑證的程序稱為憑證輪替。

主題

旋轉 SAML 2.0 憑證

您可能需要定期匯入憑證，以輪替身分提供者所發行的無效或過期憑證。這有助於防止驗證中斷或停機。所有匯入的憑證都會自動啟用。只有在確定憑證不再與相關的身分識別提供者搭配使用之後，才應刪除憑證。

您還應該考慮某些證書 IdPs 可能不支持多個證書。在這種情況下，使用這些證書輪換證書的行為 IdPs 可能意味著您的用戶臨時服務中斷。當具有該 IdP 的信任已成功重新建立時，就會還原服務。如果可能，請在非繁忙時間仔細規劃此操作。

> **Note**
>
> 作為安全性最佳做法，在任何現有 SAML 憑證遭到入侵或處理不當的跡象時，您應立即移除並輪換憑證。

輪換 IAM 身分中心憑證是一個包含下列各項的多步驟程序：

- 從 IdP 取得新憑證
- 將新憑證匯入 IAM 身分中心
- 在 IdP 中啟動新憑證
- 刪除較舊的憑證

請使用下列所有程序來完成憑證輪替程序，同時避免任何驗證停機時間。

步驟 1：從 IdP 取得新憑證

前往 IdP 網站並下載他們的 SAML 2.0 憑證。請確定以 PEM 編碼格式下載憑證檔案。大多數提供者都允許您在 IdP 中建立多個 SAML 2.0 憑證。這些可能會被標記為已停用或非作用中。

步驟 2：將新憑證匯入 IAM 身分中心

使用下列程序，使用 IAM 身分中心主控台匯入新憑證。

1. 在 IAM 身分中心主控台中，選擇 [設定]。
2. 在 [設定] 頁面上，選擇 [識別來源] 索引標籤，然後選擇 [動作] > [管理驗證]。
3. 在「管理 SAML 2.0 憑證」頁面上，選擇「匯入憑證」。
4. 在「匯入 SAML 2.0 憑證」對話方塊中，選擇「選擇檔案」，瀏覽至您的憑證檔案並加以選取，然後選擇「匯入憑證」。

此時，IAM 身分中心將信任從您匯入的兩個憑證簽署的所有內送 SAML 訊息。

步驟 3：在 IdP 中啟用新憑證

返回 IdP 網站，並將先前建立的新憑證標示為主要或作用中憑證。此時 IdP 簽署的所有 SAML 訊息都應該使用新憑證。

步驟 4：刪除舊證書

請使用下列程序來完成 IdP 的憑證輪替程序。必須至少列出一個有效的憑證，且無法移除。

> **Note**
>
> 請確定您的身分提供者不再使用此憑證簽署 SAML 回應，然後再刪除它。

1. 在「管理 SAML 2.0 憑證」頁面上，選擇您要刪除的憑證。選擇刪除。
2. 在 [刪除 SAML 2.0 憑證] 對話方塊中，輸**DELETE**入確認，然後選擇 [刪除]。
3. 返回 IdP 的網站並執行必要步驟以移除較舊的非作用中憑證。

憑證到期狀態指示器

在「管理 SAML 2.0 憑證」頁面上，您可能會注意到狀態指示器圖示有彩色。這些圖示會出現在清單中每個憑證旁邊的 [到期日] 欄中。以下說明 IAM 身分中心用來決定每個憑證顯示哪個圖示的條件。

- 紅色 — 表示憑證目前已過期。
- 黃色 — 表示憑證將在 90 天內到期。
- 綠色 — 表示憑證目前有效，且至少有效期為 90 天。

若要檢查憑證的目前狀態

1. 在 IAM 身分中心主控台中，選擇 [設定]。
2. 在 [設定] 頁面上，選擇 [識別來源] 索引標籤，然後選擇 [動作] > [管理驗證]。
3. 在「管理 SAML 2.0 驗證」頁面的「管理 SAML 2.0 憑證」下，檢閱清單中的憑證狀態，如「到期日」欄中所指示。

使用 AWS 存取入口網站

AWS 存取入口網站提供您 (使用者) 對所有 AWS 帳戶 和最常用的雲端應用程式 (例如 Office 365、Concur、Salesforce 等) 的單一登入存取權。只要在入口網站中選擇 AWS 帳戶 或應用程式圖示，即可快速啟動多個應用程式。存 AWS 取入口網站中出現應用程式圖示，表示貴公司的管理員已授予您存取這些 AWS 帳戶 或應用程式的存取權。這也表示您可以從存取入口網站存取所有這些帳戶或應用程式，而無需額外的登入提示。 AWS

在下列情況下，請聯絡您的管理員以要求其他存取權限：

- 您看不到需要存取的 AWS 帳戶 或應用程式。
- 您對特定帳戶或應用程序的訪問權限不是您所期望的。

主題

- 接受加入 IAM 身分中心的邀請
- 登入 AWS 存取入口網站
- 重設 IAM 身分中心使用者密碼
- 取得 AWS CLI 或 AWS SDK 的 IAM 身分中心使用者登入資料
- 建立 AWS Management Console 目的地的捷徑連結
- 為 MFA 註冊裝置
- 自訂 AWS 存取入口網站 URL

接受加入 IAM 身分中心的邀請

如果這是您第一次登入 AWS 存取入口網站，請查看您的電子郵件，以取得如何啟用使用者憑證的指示。

若要啟用您的使用者認證

1. 根據您從公司收到的電子郵件，選擇下列其中一種方法來啟用您的使用者認證，以便您可以開始使用 AWS 存取入口網站。

   a. 如果您收到含有加入 AWS IAM 身分中心邀請主旨的電子郵件 (AWS 單一登入的繼任者)，請開啟電子郵件，然後選擇 [接受邀請]。在 [新使用者註冊] 頁面上，輸入並確認密碼，然後選擇 [設定新密碼]。每次登入入口網站時，您都會使用該密碼。

   b. 如果您收到來自公司 IT 支援或 IT 管理員的電子郵件，請依照他們提供的指示啟用您的使用者認證。

2. 在您提供新密碼來啟用使用者認證之後， AWS 存取入口網站會自動將您登入。如果沒有發生這種情況，您可以使用下一節中提供的說明手動登入 AWS 存取入口網站。

登入 AWS 存取入口網站

此時，系統管理員應該已經為您提供 AWS 存取入口網站的特定登入 URL。擁有此 URL 後，您可以繼續登入入口網站。如需詳細資訊，請參閱登入 AWS 存取入口網站。

> **Note**
>
> 登入後， AWS 存取入口網站工作階段的預設持續時間為 8 小時。請注意，管理員可以變更此工作階段的持續時間。

信任的裝置

當您從登入頁面選擇 [這是受信任的裝置] 選項時，IAM Identity Center 會將該裝置的所有 future 登入都視為已授權。這表示，只要您使用的是受信任的裝置，IAM 身分中心就不會顯示輸入 MFA 代碼的選項。但是，也有一些例外情況，包括從新的瀏覽器登錄或當您的設備獲得了未知的 IP 地址時。

存取入口網站的登 AWS 入秘訣

以下是一些可協助您管理 AWS 存取入口網站體驗的提示。

- 有時候，您可能需要登出並重新登入 AWS 存取入口網站。這對於存取管理員最近指派給您的新應用程式，可能是必要步驟。不過，這不是必要的，因為所有新應用程式每小時都會重新整理。
- 當您登入 AWS 存取入口網站時，您可以選擇應用程式的圖示，開啟入口網站中列出的任何應用程式。使用完應用程式後，您可以關閉應用程式或登出 AWS 存取入口網站。關閉應用程式只會登出該應用程式。您從 AWS 存取入口網站開啟的任何其他應用程式會保持開啟並執行。
- 您必須先登出存取入口網站，才能以其他使用者身分登 AWS 入。從入口網站登出會從瀏覽器工作階段完全移除您的登入資料。
- 登入 AWS 存取入口網站後，您可以切換到角色。切換角色會暫時拋開原始使用者權限，而是提供指派給該角色的權限。 如需詳細資訊，請參閱切換到角色 (主控台)。

登出 AWS 存取入口網站

從入口網站登出時，您的登入資料會從瀏覽器工作階段中完全移除。如需詳細資訊，請參閱AWS 登入指南中的登出 AWS 存取入口網站。

若要登出 AWS 存取入口網站

- 在 AWS 存取入口網站中，從導覽列選擇 [登出]。

> **Note**
>
> 如果您想要以其他使用者身分登入，您必須先登出 AWS 存取入口網站。

重設 IAM 身分中心使用者密碼

AWS 存取入口網站可讓 IAM 身分中心使用者透過入口網站存取其所有指派 AWS 帳戶和雲端應用程式的單一登入存取權。 AWS 存取入口網站與管理 AWS 資源的服務主控台集合不同。AWS Management Console

使用此程序來重設存 AWS 取入口網站的 IAM 身分中心使用者密碼。進一步瞭解使用者指南中的AWS 登入 使用者類型。

考量事項

您 AWS 存取入口網站的重設密碼功能僅適用於使用 Identity Center 目錄或AWS Managed Microsoft AD作為其身分識別來源的 Identity Center 執行個體的使用者。如果您的使用者已連線至外部身分識別提供者或 AD Connector，則必須透過外部身分識別提供者或連線使用者密碼重設Active Directory。

- 如果您的身分識別來源是 IAM 身分中心目錄，請參閱在 IAM 身分中心管理身分時的密碼要求。
- 如果您的身分識別來源是 AWS Managed Microsoft AD，請參閱中重設密碼時的密碼需求 AWS Managed Microsoft AD。

若要重設存 AWS 取入口網站的密碼

1. 開啟網頁瀏覽器，然後前往 AWS 存取入口網站的登入頁面。

   如果您沒有 AWS 存取入口網站 URL，請檢查您的電子郵件。您應該已收到加入 AWS IAM 身分中心的邀請，其中包含 AWS 存取入口網站的特定登入 URL。或者，您的管理員可能已直接向您提供一次性密碼和 AWS 存取入口網站 URL。如果找不到此資訊，請要求您的管理員傳送給您。

   如需有關登入 AWS 存取入口網站的詳細資訊，請參閱AWS 登入 使用者指南中的登入 AWS 存取入口網站。
2. 輸入您的使用者名稱，然後選擇下一步。
3. 在「密碼」下，選擇「忘記密碼」

   驗證您的用戶名並輸入所提供圖像的字符以確認您不是機器人。然後選擇下一步。如果您無法輸入字元，您可能需要停用廣告封鎖軟體。
4. 會出現一則訊息，確認已傳送重設密碼電子郵件。選擇繼續。
5. 您將收到一封電子郵件，其中no-reply@signin.aws包含要求重設密碼的主題。在電子郵件中，選擇「重設密碼」。
6. 在 [重設密碼] 頁面上，確認您的使用者名稱、指定 AWS 存取入口網站的新密碼，然後選擇 [設定新密碼]。
7. 您將收到一封電子郵件no-reply@signin.aws，主題行密碼已更新。

> **Note**
>
> 管理員可以傳送電子郵件給您，其中包含重設密碼的指示，或產生一次性密碼並與您分享密碼，以重設密碼。如果您是系統管理員，請參閱重設使用者的 IAM 身分中心使用者密碼。

取得 AWS CLI 或 AWS SDK 的 IAM 身分中心使用者登入資料

您可以使用 AWS Command Line Interface 或 AWS 軟體開發套件 (SDK) 搭配 IAM 身分中心的使用者登入資料，以程式設計方式存取 AWS 服務。本主題說明如何在 IAM 身分中心取得使用者的臨時登入資料。

AWS 存取入口網站為 IAM 身分中心使用者提供對其 AWS 帳戶 和雲端應用程式的單一登入存取權。以 IAM 身分中心使用者身分登入 AWS 存取入口網站後，您可以取得臨時登入資料。然後，您可以使用 AWS CLI 或 AWS SDK 中的登入資料 (也稱為 IAM 身分中心使用者登入資料) 來存取. AWS 帳戶

如果您使用 AWS CLI 以程式設計方式存取 AWS 服務，則可以使用本主題中的程序啟動 AWS CLI. 若要取得有關的資訊 AWS CLI，請參閱《AWS Command Line Interface 使用指南》。

如果您使用 AWS SDK 以程式設計方式存取 AWS 服務，請遵循本主題中的程序，也會直接為 AWS SDK 建立驗證。如需 AWS SDK 的相關資訊，請參閱 AWS SDK 和工具參考指南。

> **Note**
>
> IAM 身分中心的使用者與 IAM 使用者不同。IAM 使用者會獲得資源的長期登入 AWS 資料。IAM 身分中心的使用者會被授與臨時登入資料。我們建議您使用臨時登入資料作為存取您的安全性最佳作法， AWS 帳戶 因為這些認證是在您每次登入時產生的。

必要條件

若要取得 IAM 身分中心使用者的臨時登入資料，您需要下列項目：

- IAM 身分中心使用者 — 您將以此使用者身分登入 AWS 存取入口網站。您或您的管理員可能會建立此使用者。如需如何啟用 IAM 身分中心和建立 IAM 身分中心使用者的相關資訊，請參閱開始使用 IAM 身分中心的常見任務。
- 使用者存取權 AWS 帳戶— 若要授與 IAM 身分中心使用者擷取其臨時登入資料的權限，您或管理員必須將 IAM 身分中心使用者指派給權限集。權限集會儲存在 IAM 身分中心，並定義 IAM 身分中心使用者擁有的存取層級 AWS 帳戶。如果管理員為您建立 IAM 身分中心使用者，請要求他們為您新增此存取權。如需詳細資訊，請參閱 指派使用者存取權給 AWS 帳戶。
- AWS CLI install — 若要使用臨時認證，您必須安裝 AWS CLI. 如需相關指示，請參閱《AWS CLI 使用者指南》中的安裝或更新 AWS CLI的最新版本。

考量事項

在完成為 IAM 身分中心使用者取得臨時登入資料的步驟之前，請記住以下考量事項：

- IAM 身分中心會建立 IAM 角色 — 當您將 IAM 身分中心中的使用者指派給權限集時，IAM 身分中心會從權限集建立對應的 IAM 角色。由權限集建立的 IAM 角色與以下列方式建立 AWS Identity and Access Management 的 IAM 角色不同：
  - IAM 身分中心擁有並保護由權限集建立的角色。只有 IAM 身分中心可以修改這些角色。
  - 只有 IAM 身分中心的使用者可以擔任與其指派的權限集相對應的角色。您無法將權限集存取權指派給 IAM 使用者、IAM 聯合身分使用者或服務帳戶。
  - 您無法修改這些角色的角色信任政策，以允許存取 IAM 身分中心以外的主體。

  如需如何取得在 IAM 中建立之角色的臨時登入資料的詳細資訊，請參閱使用AWS Identity and Access Management 者指南 AWS CLI中的〈使用臨時安全登入資料〉。
- 您可以設定權限集的工作階段持續時間 — 登入 AWS 存取入口網站後，您的 IAM Identity Center 使用者所指派的權限集會顯示為可用角色。IAM 身分中心會為此角色建立個別的工作階段。此工作階段可以從 1 到 12 小時，具體取決於為權限集配置的工作階段持續時間。預設的工作階段持續時間為一小時。如需詳細資訊，請參閱 設定工作階段期。

取得並重新整理暫時認證

您可以自動或手動取得和重新整理 IAM 身分中心使用者的臨時登入資料。

主題

- 自動認證重新整理 (建議)
- 手動認證重新整

自動認證重新整理 (建議)

自動認證刷新使用 Open ID Connect（OIDC）設備代碼授權標準。使用此方法，您可以使用中的`aws configure sso`命令直接起始存取 AWS CLI。您可以使用此命令自動存取與您為任何指派的任何權限集相關聯的任何角色 AWS 帳戶。

若要存取為 IAM 身分中心使用者建立的角色，請執行`aws configure sso`命令，然後 AWS CLI 從瀏覽器視窗授權。只要您擁有作用中的 AWS 存取入口網站工作階段，就會 AWS CLI 自動擷取暫時認證並自動重新整理認證。

如需詳細資訊，請參閱AWS Command Line Interface 使用《使用指南》*aws configure sso wizard*中的〈設定您的設定檔〉。

取得自動重新整理的臨時登入資料

1. 使用管理員提供的特定登入 URL 登入 AWS 存取入口網站。如果您已建立 IAM 身分中心使用者，則會 AWS 傳送包含您登入 URL 的電子郵件邀請。如需詳細資訊，請參閱登入使用者指南中的 AWS 登入 AWS 存取入口網站。
2. 在 [帳戶] 索引標籤中，找出您要 AWS 帳戶 從中擷取認證的。當您選擇帳戶時，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。

   > **Note**
   >
   > 如果您沒有看到任何AWS 帳戶列出的內容，表示您可能尚未指派給該帳戶的權限集。在此情況下，請聯絡您的系統管理員，並要求他們為您新增此存取權。如需詳細資訊，請參閱 指派使用者存取權給 AWS 帳戶。

3. 在帳戶名稱下方，您的 IAM 身分中心使用者所指派的權限集會顯示為可用角色。例如，如果您的 IAM 身分中心使用者被指派給該帳戶的PowerUserAccess權限集，則該角色會在 AWS 存取入口網站中顯示為PowerUserAccess。
4. 根據您在角色名稱旁邊的選項，選擇 [存取鍵] 或選擇 [命令列] 或 [程式設計存取]。
5. 在「取得認證」對話方塊中，選擇 macOS 和 Linux、Windows PowerShell，或視您安裝的作業系統而定 AWS CLI。
6. 在 AWS IAM 身分中心登入資料 (建議) 下，會顯示`SSO Region`您的`SSO Start URL`和。若要同時設定已啟用 IAM 身分中心的設定檔和您`sso-session`的 AWS CLI. 若要完成此組態，請依照使用者指南中的〈配置您的設定檔〉`aws configure sso wizard`中的AWS Command Line Interface 指示進行。

請 AWS CLI 視需要繼續使用， AWS 帳戶 直到憑證過期為止。

手動認證重新整

您可以使用手動認證重新整理方法，取得與特定權限集相關聯之角色的臨時認證 AWS 帳戶。若要這麼做，請複製並貼上暫時認證所需的命令。使用此方法時，您必須手動重新整理暫時認證。

您可以執行 AWS CLI 命令，直到您的臨時認證過期為止。

若要取得您手動重新整理的認證

1. 使用管理員提供的特定登入 URL 登入 AWS 存取入口網站。如果您已建立 IAM 身分中心使用者，則會 AWS 傳送包含您登入 URL 的電子郵件邀請。如需詳細資訊，請參閱登入使用者指南中的 AWS 登入 AWS 存取入口網站。
2. 在 [帳戶] 索引標籤中，找出您要擷取存取登入資料的 AWS 帳戶 來源，並將其展開以顯示 IAM 角色名稱 (例如管理員)。根據 IAM 角色名稱旁邊的選項，選擇 [存取金鑰] 或選擇 [命令列] 或 [程式設計存取]。

   > **Note**
   >
   > 如果您沒有看到任何AWS 帳戶列出的內容，表示您可能尚未指派給該帳戶的權限集。在此情況下，請聯絡您的系統管理員，並要求他們為您新增此存取權。如需詳細資訊，請參閱 指派使用者存取權給 AWS 帳戶。

3. 在「取得認證」對話方塊中，選擇 MacOS 和 Linux PowerShell、Windows，或視您安裝的作業系統而定 AWS CLI。
4. 選擇下列任一選項：

   - 選項 1：設定 AWS 環境變數

     選擇此選項可覆寫所有身份證明設定，包括`credentials`檔案和`config`檔案中的任何設定。若要取得更多資訊，請參閱《使用指南》 AWS CLI中的〈要配置的環境變數AWS CLI〉。

     要使用此選項，請將命令複製到剪貼板，將命令粘貼到 AWS CLI 終端機窗口中，然後按 Enter 鍵以設置所需的環境變量。

   - 選項 2：將配置文件添加到您的 AWS 憑據文件

     選擇此選項可使用不同的證明資料集執行命令。

     若要使用此選項，請將指令複製到剪貼簿，然後將指令貼到共用 AWS `credentials`檔案中，以設定新的具名設定檔。如需詳細資訊，請參閱 AWS SDK 和工具參考指南中的共用設定和認證檔案。若要使用此認證，請在指 AWS CLI 令中指定`--profile`選項。這會影響使用相同認證檔案的所有環境。

   - 選項 3：在 AWS 服務客戶端中使用個別值

     選擇此選項可從 AWS 服務用戶端存取 AWS 資源。如需詳細資訊，請參閱建置在其上的工具 AWS。

若要使用此選項，請將值複製到剪貼簿，將值貼到程式碼中，然後將它們指派給 SDK 適當的變數。如需詳細資訊，請參閱特定 SDK API 的說明文件。

建立 AWS Management Console 目的地的捷徑連結

在 AWS 存取入口網站中建立的捷徑連結，可將 IAM Identity Center 使用者帶到中的特定目的地 AWS Management Console、具有特定權限集和特定權限集的特定目的地 AWS 帳戶。

捷徑連結為你和你的協作者節省時間。您不必透過多個頁面 (包括 AWS 存取入口網站) 在 AWS Management Console (例如 Amazon S3 儲存貯體執行個體頁面) 中導覽至所需的目標 URL，而是使用捷徑連結自動前往相同的目的地。

捷徑連結目的地選項

捷徑連結有三個目的地選項，這裡依優先順序列出：

- (選擇性) 捷徑連結中 AWS Management Console 指定的任何目的地 URL。例如，Amazon S3 儲存貯體執行個體頁面。
- (選擇性) 針對相關權限集的管理員設定的轉送狀態 URL。若要取得有關設定轉送狀態的更多資訊，請參閱設定繼電器狀態。
- AWS Management Console 家。如果您未指定預設目的地。

> **Note**
>
> 只有在您透過 IAM 身分中心進行驗證，並為 AWS 帳戶和目的地 URL 指派必要的權限集時，自動導覽至目的地才會成功。

AWS 存取入口網站包含「建立」捷徑按鈕，可協助您建立可共享的捷徑連結。如果您打算指定目的地 URL (上一個清單中的第一個選項)，您可以將 URL 複製到剪貼簿來共用。

在 AWS 存取入口網站中建立捷徑連結

1. 登入 AWS 存取入口網站後，選擇 [帳戶] 索引標籤，然後選擇 [建立捷徑] 按鈕。
2. 在對話方塊中：

a. 選擇使 AWS 帳戶 用帳戶 ID 或帳戶名稱。當您輸入時，下拉式功能表會顯示您可以存取的相符帳戶 ID 和名稱。您只能選擇一個您有權訪問的帳戶。

b. 選擇性地從下拉式清單中選擇 IAM 角色。這些是為所選帳戶指派給您的權限集。如果您忽略選擇角色，則在使用捷徑連結時，系統會提示使用者為所選帳號選取指定給他們的角色。

> **Note**
>
> 您無法透過捷徑連結授予新存取權。捷徑連結僅適用於已指派給使用者的權限集。如果使用者沒有為帳戶和目的地 URL 指派必要的權限集，就會拒絕他們存取。

c. 選擇性地輸入 AWS 存取入口網站目的地 URL。如果您省略輸入 URL，使用捷徑連結時會根據之前提到的捷徑連結目的地選項自動確定目的地。

d. 您的捷徑連結會根據您的輸入，在對話方塊的底部產生。選擇「複製 URL」按鈕。您現在可以使用複製的捷徑連結建立書籤，或是與擁有相同權限集相同帳戶或其他足夠權限集存取相同帳戶的共同作業人員分享。

使用 URL 編碼構建安全 AWS Management Console 快捷鏈接

URL 的所有參數值 (包括帳戶 ID、權限集名稱和目的地 URL) 都必須經過 URL 編碼。

捷徑連結會以下列路徑擴充 AWS 存取入口網站 URL：

```
/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

傳統 AWS 分區中的完整 URL 遵循以下模式：

```
https://[your_subdomain].awsapps.com/start/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

以下是使用`S3FullAccess`權限集登入使用者`123456789012`的捷徑連結範例，並將其導向 S3 主控台首頁：

- `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) `https://start.us-gov-west-1.us-gov-home.awsapps.com/directory/example/#/console?`

```
account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F
%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome
```

為 MFA 註冊裝置

在 AWS 存取入口網站中使用下列程序，為您的新裝置註冊多重要素驗證 (MFA)。

> **Note**
>
> 我們建議您先將適當的驗證器應用程式下載到您的裝置上，然後再開始執行此程序中的步驟。如需可用於 MFA 裝置的應用程式清單，請參閱虛擬驗證器應用程式。

註冊您的裝置以便與 MFA 搭配使用

1. 登入您的 AWS 存取入口網站。如需詳細資訊，請參閱 登入 AWS 存取入口網站。
2. 在頁面右上角附近，選擇 MFA 裝置。
3. 在 [多重要素驗證 (MFA) 裝置] 頁面上，選擇 [註冊裝置]。

   > **Note**
   >
   > 如果「註冊 MFA 裝置」選項呈現灰色，請聯絡您的管理員以取得註冊裝置的協助。

4. 在 [註冊 MFA 裝置] 頁面上，選取下列其中一種 MFA 裝置類型，然後依照指示進行：

   - 驗證器應用程式
     1. 在 [設定驗證器應用程式] 頁面上，您可能會注意到新 MFA 裝置的設定資訊，包括 QR 碼圖形。該圖形表示了在不支持 QR 碼的設備上可用於手動輸入的密鑰。
     2. 使用實體 MFA 裝置，執行下列動作：
        a. 開啟相容的 MFA 驗證器應用程式。如需可與 MFA 裝置搭配使用的已測試應用程式清單，請參閱虛擬驗證器應用程式。如果 MFA 應用程式支援多個帳戶 (多個 MFA 裝置)，請選擇建立新帳戶 (新的 MFA 裝置) 的選項。
        b. 確定 MFA 應用程式是否支援 QR 碼，然後在「設定驗證器應用程式」頁面上執行下列其中一項操作：
           i. 選擇 [顯示 QR 碼]，然後使用應用程式掃描 QR 碼。例如，您可以選擇相機圖示或選擇類似於「掃描程式碼」的選項。然後使用設備的相機掃描代碼。

ii. 選擇顯示密鑰，然後將該密鑰輸入到您的 MFA 應用程序中。

> **Important**
>
> 當您為 IAM 身分中心設定 MFA 裝置時，建議您將 QR 碼或私密金鑰的複本儲存在安全的地方。如果您遺失手機或必須重新安裝 MFA 驗證器應用程式，這可能會有所幫助。如果其中一種情況發生，您可以快速重新配置應用程序以使用相同的 MFA 配置。

3. 在 [設定驗證器應用程式] 頁面的 [驗證器代碼] 下，輸入目前顯示在實體 MFA 裝置上的一次性密碼。

> **Important**
>
> 產生代碼之後立即提交您的請求。如果您產生程式碼，然後等待太長時間才能提交要求，MFA 裝置已成功與您的使用者建立關聯，但 MFA 裝置不同步。會發生這種情況是因為定時式的一次性密碼 (TOTP) 在過了一小段時間後就會過期。如果發生這種情況，您可以再次同步設備。

4. 選擇 Assign MFA (指派 MFA)。MFA 裝置現在可以開始產生一次性密碼，現在可以與 AWS.

- 安全金鑰或內建驗證器

1. 在 [註冊使用者的安全金鑰] 頁面上，依照瀏覽器或平台提供的指示進行。

> **Note**
>
> 使用體驗會因瀏覽器或平台而有所不同。成功註冊裝置後，您可以將易記的顯示名稱與新註冊的裝置建立關聯。若要變更名稱，請選擇 [重新命名]，輸入新名稱，然後選擇 [儲存]。

自訂 AWS 存取入口網站 URL

根據預設，您可以 AWS 使用以下格式的 URL 存取入口網站：`d-xxxxxxxxxx.awsapps.com/start`。您可以按照以下方式自定義 URL：`your_subdomain.awsapps.com/start`

> **Important**
>
> 如果您變更 AWS 存取入口網站 URL，稍後將無法編輯。

若要自訂您的網址

1. 請在以下位置開啟 AWS IAM Identity Center 主控台。 https://console.aws.amazon.com/singlesignon/
2. 在 IAM 身分中心主控台中，選擇導覽窗格中的 [儀表板]，然後找到 [設定摘要] 區段。
3. 選擇 AWS 存取入口網站 URL 下方的「自訂」按鈕。

   > **Note**
   >
   > 如果沒有顯示 [自訂] 按鈕，表示 AWS 存取入口網站已經自訂。自訂 AWS 存取入口網站 URL 是無法復原的一次性作業。

4. 輸入您想要的子網域名稱，然後選擇 [儲存]。

您現在可以使用自訂 URL 透過 AWS 存取入口網站登入 AWS 主控台。

身分識別中心使用者的多因素驗證

多重驗證 (MFA) 提供了一種簡單而安全的方式，在使用者名稱和密碼的預設驗證機制之上增加額外的保護層。

當系統管理員啟用 MFA 時，使用者必須以兩個因素登入AWS存取入口網站：

- 他們的使用者名稱和密碼。這是用戶知道的第一個因素。
- 代碼，安全密鑰或生物識別技術。這是第二個因素，是用戶擁有（擁有）或（生物特徵識別）的東西。第二個因素可能是從他們的流動裝置產生的驗證碼，連接到他們的電腦的保安密鑰，或用戶的生物識別掃描。

除非成功完成有效的 MFA 挑戰，否則這些多重因素通過防止未經授權訪問您的AWS資源來提供更高的安全性。

每個用戶最多可以註冊兩個虛擬身份驗證器應用程序，這些應用程序是安裝在您的移動設備或平板電腦上的一次性密碼驗證器，以及六個 FIDO 驗證器（包括內置身份驗證器和安全密鑰），總共八個 MFA 設備。進一步了解 IAM 身分中心可用的 MFA 類型。

> **Important**
>
> 我們強烈建議您啟用 MFA，做為安全性最佳作法。

主題

IAM 身分中心可用的 MFA 類型

多重要素驗證 (MFA) 是一種簡單而有效的機制，可增強使用者的安全性。用戶的第一個因素-他們的密碼-是他們記住的秘密，也被稱為知識因素。其他因素可能是擁有因素（您擁有的東西，例如安全密鑰）或固有因素（您所屬的東西，例如生物識別掃描）。強烈建議您設定 MFA，為您的帳戶增加額外的安全層。

IAM 身分中心 MFA 支援下列裝置類型。以瀏覽器為基礎的主控台存取以及搭配 IAM 身分中心使用 AWS CLI v2 都支援所有 MFA 類型。

- FIDO2 驗證器，包括內建驗證器和安全金鑰
- 虛擬驗證器應用程式
- 通過連接您自己的MFA 半徑實施 AWS Managed Microsoft AD

一個用戶最多可以有八個 MFA 設備，其中包括最多兩個虛擬身份驗證器應用程序和六個 FIDO 身份驗證器，並在一個帳戶中註冊。您也可以設定 MFA 啟用設定，以便在使用者每次登入時都要求 MFA，或啟用每次登入時不需要 MFA 的受信任裝置。如需如何為使用者設定 MFA 類型的詳細資訊，請參閱選擇 MFA 類型和設定 MFA 裝置強制。

FIDO2 驗證器

FIDO2 是一個包含 CTAP2 的標準，WebAuthn並且基於公鑰加密技術。FIDO 憑據具有網絡釣魚功能，因為它們對於創建憑據的網站而言是唯一的，例如。AWS

AWS支援 FIDO 驗證器的兩種最常見的外形規格：內建驗證器和安全金鑰。有關最常見 FIDO 驗證器類型的更多信息，請參見下文。

主題

- 內建驗證器
- 安全金鑰
- 密碼管理員、金鑰提供者和其他 FIDO 驗證器

內建驗證器

許多現代計算機和移動電話都內置了身份驗證器，例如 Macbook 上的觸摸 ID 或與 Windows 幫助兼容的相機。如果您的設備具有與 FIDO 兼容的內置身份驗證器，則可以將指紋，臉部或設備 PIN 碼用作第二個因素。

安全金鑰

安全金鑰是與 FIDO 相容的外部硬體驗證器，您可以透過 USB、BLE 或 NFC 購買並連接裝置。當系統提示您輸入 MFA 時，您只需使用按鍵的感應器完成一個手勢即可。安全密鑰的一些示例包括 YubiKeys 和 Feitian 密鑰，最常見的安全密鑰創建了綁定設備的 FIDO 憑據。如需所有 FIDO 認證安全金鑰的清單，請參閱 FIDO 認證產品。

密碼管理員、金鑰提供者和其他 FIDO 驗證器

多個第三方提供商支持移動應用程序中的 FIDO 身份驗證，如密碼管理器中的功能，具有 FIDO 模式的智能卡以及其他外形規格。這些與 FIDO 相容的裝置可與 IAM 身分中心搭配使用，但我們建議您先測試 FIDO 驗證器，然後再為 MFA 啟用此選項。

> **Note**
>
> 某些 FIDO 驗證器可以建立稱為密碼的可探索 FIDO 認證。密碼金鑰可能會繫結至建立密碼的裝置，也可能是同步纜線並備份到雲端。例如，您可以在支持的 Macbook 上使用蘋果觸摸 ID 註冊密鑰，然後通過在登錄時按照屏幕上的提示使用谷歌瀏覽器與 iCloud 中的密鑰從 Windows 筆記本電腦登錄到網站。如需有關哪些裝置 Support 同步纜線金鑰以及作業系統和瀏覽器之間目前金鑰互通性的詳細資訊，請參閱 passkeys.dev 的裝置支援，FIDO 聯盟和全球資訊網聯盟 (W3C) 維護的資源。

虛擬驗證器應用程式

身份驗證器應用程序基本上是基於一次性密碼（OTP）的第三方身份驗證器。您可以使用安裝在行動裝置或平板電腦上的驗證器應用程式做為授權的 MFA 裝置。協力廠商驗證器應用程式必須符合 RFC 6238，RFC 6238 是標準型一次性密碼 (TOTP) 演算法，能夠產生六位數驗證碼。

當系統提示輸入 MFA 時，使用者必須在顯示的輸入方塊中輸入驗證器應用程式的有效代碼。每個指派給使用者的 MFA 裝置都必須是唯一的。任何指定使用者都可以註冊兩個驗證器應用程式。

測試驗證器應用程式

任何符合 TOTP 標準的應用程式都可以與 IAM 身分中心 MFA 搭配使用。下表列出了可供選擇的知名第三方身份驗證器應用程序。

作業系統	測試驗證器應用程式
Android	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

MFA 半徑

遠端驗證撥入使用者服務 (RADIUS) 是業界標準的用戶端-伺服器通訊協定，提供驗證、授權和帳戶管理，讓使用者能夠連線到網路服務。 AWS Directory Service包含 RADIUS 用戶端，可連接至您實作 MFA 解決方案的 RADIUS 伺服器。如需詳細資訊，請參閱為 AWS Managed Microsoft AD.

您可以在 IAM 身分識別中心中使用 RADIUS MFA 或 MFA 來登入使用者入口網站，但不能同時使用兩者。在您想要AWS原生雙因素驗證以存取入口網站時，IAM 身分識別中心中的 MFA 是 RADIUS MFA 的替代方案。

當您在 IAM 身分中心啟用 MFA 時，您的使用者需要 MFA 裝置才能登入AWS存取入口網站。如果您之前曾使用 RADIUS MFA，則在 IAM 身分中心啟用 MFA 可有效地覆寫登入存取入口網站的使用者的 RADIUS MFA。AWS但是，當使用者登入所有其他可使用的應用程式 (例如 Amazon WorkDocs) 時 AWS Directory Service，RADIUS MFA 仍會持續挑戰他們。

如果您的 MFA 在 IAM 身分中心主控台上已停用，且您已將 RADIUS MFA 設定為AWS Directory Service，RADIUS MFA 會管理AWS存取入口網站登入。這表示如果停用 MFA，IAM 身分識別中心會退回 RADIUS MFA 組態。

設定 MFA

下列主題提供在 IAM 身分中心設定 MFA 裝置的指示。

主題

在 IAM 身分中心啟用 MFA 之前的考量

啟用 MFA 之前，請考慮下列事項：

- 建議使用者為所有已啟用的 MFA 類型註冊多個備份驗證器。此做法可防止 MFA 裝置損壞或放錯位置時遺失存取權。
- 如果您的使用者必須登入AWS存取入口網站才能存取其電子郵件，請勿選擇要求他們提供透過電子郵件傳送的一次性密碼選項。例如，您的使用者可能會在AWS存取入口網站Microsoft 365中使用來讀取他們的電子郵件。在此情況下，使用者將無法擷取驗證碼，也無法登入AWS存取入口網站。如需詳細資訊，請參閱設定 MFA 裝置強制。
- 如果您已經在使用設定的 RADIUS MFAAWS Directory Service，就不需要在 IAM 身分中心啟用 MFA。身分識別中心中的 MFA 是 IAM 身分識別中心Microsoft Active Directory使用者的 RADIUS MFA 替代方案。如需詳細資訊，請參閱MFA 半徑。
- 當您的身分來源設定為 IAM 身分中心的身分識別存放區或 AD Connector 時，AWS Managed Microsoft AD您可以在 IAM 身分中心使用 MFA 功能。外部身分識別提供者目前不支援 IAM 身分中心中的 MFA。

在 IAM 身分中心啟用 MFA

您可以啟用多因素身份驗證 (MFA)，啟用對AWS存取入口網站、IAM 身分中心整合式應用程式的安全存取。AWS CLI

主題

- 停用 IAM 身分中心目錄的 MFA

提示使用者輸入 MFA

使用下列步驟在 IAM 身分中心主控台中啟用 MFA。在開始之前，我們建議您了解IAM 身分中心可用的 MFA 類型.

> **Note**
>
> 如果您使用外部 IdP，則無法使用多因素身份驗證部分。您的外部 IdP 會管理 MFA 設定，而不是管理這些設定的 IAM 身分中心。

若要啟用 MFA

1. 開啟 IAM 身分中心主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 在 [設定] 頁面上，選擇 [驗證] 索引標籤。
4. 在 [多重要素驗證] 區段中，選擇 [設定]。
5. 在 [設定多重要素驗證] 頁面的 [提示使用者輸入 MFA] 下，根據您的企業需要的安全性層級選擇下列其中一種驗證模式：

   - 僅當他們的登錄上下文更改時（上下文感知）

     在此模式 (預設值) 中，IAM 身分中心為使用者提供在登入期間信任其裝置的選項。在使用者指出要信任裝置之後，IAM Identity Center 會提示使用者輸入 MFA 一次，並分析使用者後續登入的登入內容 (例如裝置、瀏覽器和位置)。對於後續登入，IAM 身分中心會判斷使用者是否使用之前受信任的內容登入。如果使用者的登入內容發生變更，IAM Identity Center 會提示使用者輸入 MFA，以及其電子郵件地址和密碼登入資料。

     此模式為經常從工作場所登入的使用者提供易用性，因此他們不需要在每次登入時完成 MFA。只有在登入內容變更時，系統才會提示他們輸入 MFA。

   - 每次他們登錄（始終在線）

     在此模式中，IAM 身分中心要求擁有已註冊 MFA 裝置的使用者每次登入時都會收到提示。如果您的組織或合規性原則要求使用者每次登入AWS存取入口網站時都必須完成 MFA，則應使用此模式。例如，PCI DSS 強烈建議在每次登入時使用 MFA，以存取支援高風險付款交易的應用程式。

- 從不 (停用)

  在此模式下，所有使用者只能使用其標準使用者名稱和密碼登入。選擇此選項會停用 IAM 身分中心 MFA。

  > **Note**
  >
  > 如果您已經在搭配使用 RADIUS MFAAWS Directory Service，並且想要繼續使用它做為預設 MFA 類型，則可以將驗證模式保持為停用狀態，以便在 IAM 身分中心略過 MFA 功能。從「停用」模式變更為「內容感知」或「永遠開啟」模式，將會覆寫現有的 RADIUS MFA 設定。如需詳細資訊，請參閱MFA 半徑。

6. 選擇 Save changes (儲存變更)。

   相關主題

   - 選擇 MFA 類型
   - 設定 MFA 裝置強制
   - 允許使用者註冊自己的 MFA 裝置

停用 IAM 身分中心目錄的 MFA

當您停用 IAM 身分中心目錄的多重要素驗證 (MFA) 時，它只允許使用者使用其標準使用者名稱和密碼登入。雖然已針對使用者的身分中心目錄停用 MFA，但您無法在其使用者詳細資料中管理 MFA 裝置，且 Identity Center 目錄使用者無法從存取入口網站管理 MFA 裝置。AWS

為您的 IAM 身分中心目錄停用 MFA

> **Important**
>
> 本節中的指示適用於AWS IAM Identity Center。它們不適用於 AWS Identity and Access Management(IAM)。IAM 身分中心使用者、群組和使用者登入資料與 IAM 使用者、群組和 IAM 使用者登入資料不同。如果您正在尋找停用 IAM 使用者 MFA 的相關說明，請參閱使用者指南中的停用 MFA 裝置。AWS Identity and Access Management

1. 開啟 IAM 身分中心主控台。
2. 在左側的導覽窗格中，選擇設定。

3. 在 [設定] 頁面上，選擇 [驗證] 索引標籤。
4. 在 [多重要素驗證] 區段中，選擇 [設定]。
5. 在 [設定多因素驗證] 頁面的 [提示使用者 MFA] 區段中，選擇永不 (停用) 選項按鈕。
6. 選擇儲存變更。

選擇 MFA 類型

在AWS存取入口網站中提示輸入 MFA 時，請使用下列程序選擇使用者可以驗證的裝置類型。

為您的使用者設定 MFA 類型

1. 開啟 IAM 身分中心主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 在 [設定] 頁面上，選擇 [驗證] 索引標籤。
4. 在 [多重要素驗證] 區段中，選擇 [設定]。
5. 在 [設定多因素驗證] 頁面的 [使用者可以使用這些 MFA 類型進行驗證] 下，根據您的業務需求，選擇下列其中一種 MFA 類型。如需詳細資訊，請參閱IAM 身分中心可用的 MFA 類型。
   - FIDO2 驗證器，包括內建驗證器和安全金鑰
   - 虛擬驗證器應用程式
6. 選擇儲存變更。

設定 MFA 裝置強制

使用下列程序來判斷您的使用者在登入AWS存取入口網站時是否必須擁有已註冊的 MFA 裝置。

為您的使用者設定 MFA 裝置強制

1. 開啟 IAM 身分中心主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 在 [設定] 頁面上，選擇 [驗證] 索引標籤。
4. 在 [多重要素驗證] 區段中，選擇 [設定]。
5. 在 [設定多因素驗證] 頁面的 [如果使用者尚未註冊的 MFA 裝置] 下，根據您的業務需求，選擇下列其中一個選項：
   - 要求他們在登入時註冊 MFA 裝置

這是您第一次為 IAM 身分中心設定 MFA 時的預設設定。當您想要求尚未註冊 MFA 裝置的使用者在密碼驗證成功後在登入期間自行註冊裝置時，請使用此選項。這可讓您使用 MFA 保護組織的AWS環境，而不必個別註冊驗證裝置並分發給使用者。在自我註冊期間，您的使用者可以從您先前啟用的IAM 身分中心可用的 MFA 類型可用裝置註冊任何裝置。完成註冊後，使用者可以選擇為新註冊的 MFA 裝置提供一個易記的名稱，然後 IAM Identity Center 會將使用者重新導向至其原始目的地。如果使用者的裝置遺失或遭竊，您只要從其帳戶中移除該裝置，IAM Identity Center 就會要求使用者在下次登入時自行註冊新裝置。

- 要求他們提供以電子郵件發送的一次性密碼以登錄

  如果您想要透過電子郵件傳送驗證碼給使用者，請使用此選項。由於電子郵件未綁定到特定設備，因此此選項不符合行業標準多因素身份驗證的標準。但是它確實提高了安全性，而不是單獨使用密碼。只有在使用者尚未註冊 MFA 裝置時，才會要求電子郵件驗證。如果已啟用內容感知驗證方法，使用者將有機會將收到電子郵件的裝置標示為受信任。之後，他們將不需要在 future 從該設備，瀏覽器和 IP 地址組合登錄時驗證電子郵件代碼。

  > **Note**
  >
  > 如果您使用 Active Directory 做為已啟用 IAM 身分識別中心的身分識別來源，電子郵件地址將永遠以 Active Directory `email` 屬性為基礎。自訂使用中目錄屬性對應不會覆寫此行為。

- 封鎖他們的登入

  如果您想要在每個使用者登入之前強制使用 MFA，請使用「封鎖他們的登入」選項。AWS

  > **Important**
  >
  > 如果您的驗證方法設定為「內容感知」，使用者可能會選取登入頁面上的 [這是受信任的裝置] 核取方塊。在這種情況下，即使您已啟用 [封鎖他們的登入] 設定，系統也不會提示該使用者輸入 MFA。如果您想要提示這些使用者，請將驗證方法變更為 [永遠開啟]。

- 允許他們登入

  使用此選項表示不需要 MFA 裝置，您的使用者才能登入AWS存取入口網站。選擇註冊 MFA 裝置的使用者仍會收到 MFA 的提示。

6. 選擇儲存變更。

允許使用者註冊自己的 MFA 裝置

使用下列程序可讓您的使用者自行註冊自己的 MFA 裝置。

允許使用者註冊自己的 MFA 裝置

1. 開啟 IAM 身分中心主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 在 [設定] 頁面上，選擇 [驗證] 索引標籤。
4. 在 [多重要素驗證] 區段中，選擇 [設定]。
5. 在 [設定多因素驗證] 頁面的 [誰可以管理 MFA 裝置] 下，選擇 [使用者可以新增和管理自己的 MFA 裝置]。
6. 選擇儲存變更。

> **Note**
>
> 為使用者設定自我註冊之後，您可能會想要傳送程序為 MFA 註冊裝置的連結給他們。本主題提供如何設定自己的 MFA 裝置的指示。

在 IAM 身分中心管理 MFA 裝置

下列主題提供在 IAM 身分中心管理 MFA 裝置的指示。

主題

- 註冊 MFA 裝置
- 管理使用者的 MFA 裝置

註冊 MFA 裝置

使用下列程序設定新的 MFA 裝置，以供 IAM 身分中心主控台中的特定使用者存取。您必須擁有對使用者 MFA 裝置的實體存取權，才能註冊它。例如，如果您為將使用智慧型手機上執行的 MFA 裝置的使用者設定 MFA，則需要實際存取智慧型手機才能完成註冊程序。或者，您可以允許使用者設定和管理自己的 MFA 裝置。如需詳細資訊，請參閱允許使用者註冊自己的 MFA 裝置。

若要註冊 MFA 裝置

1. 開啟 IAM 身分中心主控台。
2. 在左側導覽窗格中，選擇 Users (使用者)。在清單中選擇使用者。請勿針對此步驟選取使用者旁邊的核取方塊。
3. 在使用者詳細資料頁面上，選擇 MFA 裝置索引標籤，然後選擇 [註冊 MFA 裝置]。
4. 在 [註冊 MFA 裝置] 頁面上，選取下列其中一種 MFA 裝置類型，然後依照指示進行：

   - 驗證器應用程式

     1. 在 [設定驗證器應用程式] 頁面上，IAM 身分中心會顯示新 MFA 裝置的設定資訊，包括 QR 碼圖形。該圖形是密鑰的表示形式，該密鑰可用於在不支持 QR 碼的設備上手動輸入。
     2. 使用實體 MFA 裝置，執行下列動作：

        a. 開啟相容的 MFA 驗證器應用程式。如需可與 MFA 裝置搭配使用的已測試應用程式清單，請參閱虛擬驗證器應用程式。如果 MFA 應用程式支援多個帳戶 (多個 MFA 裝置)，請選擇建立新帳戶 (新的 MFA 裝置) 的選項。

        b. 確定 MFA 應用程式是否支援 QR 碼，然後在「設定驗證器應用程式」頁面上執行下列其中一項操作：

           i. 選擇 [顯示 QR 碼]，然後使用應用程式掃描 QR 碼。例如，您可以選擇相機圖示或選擇類似於「掃描程式碼」的選項。然後使用設備的相機掃描代碼。

           ii. 選擇顯示秘密金鑰，然後在 MFA 應用程式中輸入該密鑰。

        > **Important**
        >
        > 當您為 IAM 身分中心設定 MFA 裝置時，建議您將 QR 碼或私密金鑰的複本儲存在安全的地方。如果指派的使用者遺失電話或必須重新安裝 MFA 驗證器應用程式，這可能會有所幫助。如果其中一種情況發生，您可以快速重新配置應用程序以使用相同的 MFA 配置。這樣就不需要在 IAM 身分中心為使用者建立新的 MFA 裝置。

     3. 在 [設定驗證器應用程式] 頁面的 [驗證器代碼] 下，輸入目前顯示在實體 MFA 裝置上的一次性密碼。

        > **Important**
        >
        > 產生代碼之後立即提交您的請求。如果您產生程式碼，然後等待太長時間才能提交要求，MFA 裝置就會成功與使用者建立關聯。但是 MFA 設備不同步。會發生這種情況

是因為定時式的一次性密碼 (TOTP) 在過了一小段時間後就會過期。這種情況下，您可以重新同步裝置。

4. 選擇 Assign MFA (指派 MFA)。MFA 裝置現在可以開始產生一次性密碼，現在可以與AWS.

- 安全性金鑰
  1. 在 [註冊使用者的安全金鑰] 頁面上，遵循瀏覽器或平台提供給您的指示。

> **Note**
>
> 這裡的體驗因不同的操作系統和瀏覽器而異，因此請按照您的瀏覽器或平台顯示的說明進行操作。成功註冊使用者的裝置後，您可以選擇將易記的顯示名稱與使用者新註冊的裝置建立關聯。如果您要變更此設定，請選擇 [重新命名]，輸入新名稱，然後選擇 [儲存]。如果您已啟用允許使用者管理自己裝置的選項，使用者將會在AWS存取入口網站中看到此易記名稱。

管理使用者的 MFA 裝置

當您需要重新命名或刪除使用者的 MFA 裝置時，請遵循下列程序。

若要重新命名 MFA 裝置

1. 開啟 IAM 身分中心主控台。
2. 在左側導覽窗格中，選擇 Users (使用者)。在清單中選擇使用者。請勿針對此步驟選取使用者旁邊的核取方塊。
3. 在使用者詳細資料頁面上，選擇 MFA 裝置索引標籤，選取裝置，然後選擇 [重新命名]。
4. 出現提示時，輸入新名稱，然後選擇「重新命名」。

若要刪除 MFA 裝置

1. 開啟 IAM 身分中心主控台。
2. 在左側導覽窗格中，選擇 Users (使用者)。在清單中選擇使用者。
3. 在使用者詳細資料頁面上，選擇 [MFA 裝置] 索引標籤，選取裝置，然後選擇 [刪除]。
4. 若要確認，請輸入 DELETE，然後選擇 [刪除]。

管理存取 AWS 帳戶

AWS IAM Identity Center 與整合 AWS Organizations，可讓您集中管理多個帳戶的權限， AWS 帳戶而無需手動設定每個帳戶。您可以定義權限並將這些權限指派給員工使用者，以控制他們對特定的存取權限 AWS 帳戶。

AWS 帳戶 類型

AWS 帳戶 中有兩種類型 AWS Organizations：

- 管理帳戶- AWS 帳戶 用於創建組織。
- 成員帳戶-屬於組織的其餘部分。 AWS 帳戶

如需有關 AWS 帳戶 類型的詳細資訊，請參閱AWS Organizations 使用指南中的AWS Organizations 術語和概念。

您也可以選擇將成員帳戶註冊為 IAM 身分中心的委派管理員。此帳戶中的使用者可以執行大部分的 IAM 身分中心管理任務。如需詳細資訊，請參閱 委派管理。

對於每個任務和帳戶類型，下表指出帳戶中的使用者是否可以執行 IAM 身分中心管理任務。

IAM 身分識別中心管理工作	成員帳戶	委派管理員帳戶	管理帳戶
讀取使用者或群組 (讀取群組本身和群組的成員資格)	 是	 是	 是
新增、編輯或刪除使用者或群組	 否	 是	 是

IAM 身分識別中心管理工作	成員帳戶	委派管理員帳戶	管理帳戶
啟用或停用使用者存取	 否	 是	 是
啟用、停用或管理內送屬性	 否	 是	 是
變更或管理身分識別來源	 否	 是	 是
建立、編輯或刪除應用程式	 否	 是	 是
設定 MFA	 否	 是	 是
管理未在管理帳戶中佈建的權限集	 否	 是	 是
管理管理帳戶中佈建的權限集	 否	 否	 是

IAM 身分識別中心管理工作	成員帳戶	委派管理員帳戶	管理帳戶
啟用 IAM Identity Center	 否	 否	 是
刪除 IAM 身分中心組態	 否	 否	 是
啟用或停用管理帳戶中的使用者存取	 否	 否	 是
以委派管理員身分註冊或取消註冊成員帳戶	 否	 否	 是

指派 AWS 帳戶 存取權

您可以使用權限集來簡化組織中的使用者和群組指派存取權的方式 AWS 帳戶。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。您可以建立單一權限集，並將其指派給組織 AWS 帳戶 內的多個權限集。您也可以將多個權限集指派給相同的使用者。

如需許可集合的詳細資訊，請參閱建立、管理及刪除權限集。

> **Note**
>
> 您也可以將應用程式的單一登入存取權指派給使用者。如需相關資訊，請參閱管理應用程式的存取。

使用者體驗

AWS 存取入口網站可讓 IAM 身分中心使用者透過入口網站存取其所有指派 AWS 帳戶 和應用程式的單一登入存取權。 AWS 存取入口網站與管理 AWS 資源的服務主控台集合不同。AWS Management Console

當您建立權限集時，您為權限集指定的名稱會以可用角色的形式出現在 AWS 存取入口網站中。使用者登入 AWS 存取入口網站，選擇一個 AWS 帳戶，然後選擇角色。選擇角色之後，他們可以使用 AWS Management Console 或擷取暫時認證以程式設計方式存取 AWS 服務來存取 AWS 服務。

若要開啟 AWS Management Console 或擷取暫時認證以 AWS 程式設計方式存取，使用者必須完成下列步驟：

1. 使用者會開啟瀏覽器視窗，並使用您提供的登入 URL 導覽至 AWS 存取入口網站。
2. 他們使用其目錄認證登入 AWS 存取入口網站。
3. 驗證之後，在 AWS 存取入口網站頁面上，他們選擇 [帳戶] 索引標籤， AWS 帳戶 以顯示他們有權存取的清單。
4. 然後，用戶選擇 AWS 帳戶 他們想要使用的。
5. 在名稱下方 AWS 帳戶，將使用者指派給的任何權限集都會顯示為可用角色。例如，如果您`john_stiles`將使用者指派給`PowerUser`權限集，則該角色會在 AWS 存取入口網站中顯示為`PowerUser/john_stiles`。獲得指派多個許可集合的使用者選擇要使用的 角色。使用者可以選擇要存取的角色 AWS Management Console。
6. 除了角色之外， AWS 存取入口網站使用者還可以選擇 [存取金鑰]，擷取命令列或程式設計存取的臨時認證。

如需可 step-by-step 提供給員工使用者的指引，請參閱使用 AWS 存取入口網站和取得 AWS CLI 或 AWS SDK 的 IAM 身分中心使用者登入資料。

強制執行和限制存取

啟用 IAM 身分中心時，IAM 身分中心會建立服務連結角色。您也可以使用服務控制原則 (SCP)。

委派和強制執行存取

服務連結角色是直接連結至 AWS 服務的 IAM 角色類型。啟用 IAM 身分中心後，IAM 身分中心就可以在組織中的每個 AWS 帳戶 角色中建立服務連結角色。此角色提供預先定義的許可，可讓 IAM Identity

Center 委派和強制執行哪些使用者對您組織中特定的特 AWS 帳戶 定使用者具有單一登入存取權 AWS Organizations。您必須指派一個或多個可存取帳戶的使用者，才能使用此角色。如需詳細資訊，請參閱 服務連結角色 及 針對 IAM 身分中心使用服務連結角色。

限制從成員帳戶存取身分識別存放區

對於 IAM 身分中心使用的身分識別存放區服務，具有成員帳戶存取權限的使用者可以使用需要讀取權限的 API 動作。成員帳戶可以存取 sso-directory 和識別存放區命名空間上的「讀取」動作。如需詳細資訊，請參閱服務授權參考中 AWS 識別身分存放區的 AWS IAM Identity Center 目錄和動作、資源和條件金鑰的動作、資源和條件金鑰。

若要防止成員帳戶中的使用者使用身分識別存放區中的 API 作業，您可以附加服務控制原則 (SCP)。SCP 是一種組織原則，可用來管理組織中的權限。下列範例 SCP 可防止成員帳戶中的使用者存取身分識別存放區中的任何 API 作業。

```
{
    "Sid": "ExplicitlyBlockIdentityStoreAccess",
    "Effect": "Deny",
    "Action": "identitystore:*", "sso-directory:*"],
    "Resource": "*"
}
```

> **Note**
>
> 限制成員帳戶的存取權限可能會損害啟用 IAM 身分中心的應用程式中的功能。

如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策 (SCP)。

委派管理

委派管理為已註冊成員帳戶中的指派使用者提供了一種便利的方式，以執行大部分的 IAM 身分中心管理工作。啟用 IAM 身分中心時， AWS Organizations 依預設會在中的管理帳戶中建立您的 IAM 身分中心執行個體。這原本是以這種方式設計的，讓 IAM 身分中心可以在組織的所有成員帳戶中佈建、取消佈建和更新角色。即使您的 IAM 身分中心執行個體必須始終位於管理帳戶中，您也可以選擇將 IAM 身分中心的管理委派給中的成員帳戶 AWS Organizations，進而擴展從管理帳戶外部管理 IAM 身分中心的能力。

啟用委派管理可提供下列優點：

- 將需要存取管理帳戶的人數減至最少，以協助減輕安全性考量
- 允許選取的管理員將使用者和群組指派給應用程式和組織的成員帳戶

如需 IAM 身分中心如何搭配使用的詳細資訊 AWS Organizations，請參閱管理存取 AWS 帳戶。如需其他資訊，並檢閱示範如何設定委派管理的公司案例，請參閱AWS 安全部落格中的 IAM Identity Center 委派管理入門。

主題

最佳實務

以下是設定委派管理之前，應考量的一些最佳作法。

- 授與管理帳戶最少權限 — 知道管理帳戶是具有高度權限的帳戶，並且為了遵守最低權限的主體，我們強烈建議您將管理帳戶的存取權限制為盡可能少的使用者。委派的系統管理員功能旨在將需要存取管理帳戶的人數降至最低。
- 建立僅在管理帳戶中使用的權限集 — 這可讓您更輕鬆地管理專為存取管理帳戶的使用者量身打造的權限集，並有助於將它們與委派管理員帳戶所管理的權限集區分開來。
- 考慮您的作用中目錄位置 — 如果您計劃使用 Active Directory 做為 IAM 身分中心身分識別來源，請在您已啟用 IAM 身分中心委派系統管理員功能的成員帳戶中找到目錄。如果您決定將 IAM 身分中心身分識別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。
- 僅在管理帳戶中建立使用者指派 — 委派的管理員無法更改管理帳戶中佈建的權限集。不過，委派管理員可以新增、編輯和刪除群組和群組指派。

必要條件

您必須先部署下列環境，才能將帳戶註冊為委派管理員：

- AWS Organizations 除了您的預設管理帳戶之外，還必須啟用並設定至少一個成員帳戶。
- 如果您的身分識別來源設定為使用中目錄，則必須啟用此IAM 身分識別中心可設定 AD 同步功能。

註冊會員帳號

若要設定委派管理，您必須先將組織中的成員帳戶註冊為委派系統管理員。該成員帳戶中具有足夠權限的使用者將擁有 IAM 身分中心的管理存取權。成功註冊成員帳戶以進行委派管理之後，就稱為委派的系統管理員帳戶。若要深入瞭解委派管理員帳戶可執行的工作，請參閱AWS 帳戶 類型。

IAM 身分中心一次僅支援將一個成員帳戶註冊為委派的管理員。您只能在使用管理帳戶的憑據登錄時註冊會員帳戶。

使用下列程序，透過將 AWS 組織中的特定成員帳戶註冊為委派管理員，以授與 IAM Identity Center 的管理存取權。

> **Important**
>
> 此操作會將 IAM 身分中心管理存取權委派給此成員帳戶中的管理員使用者。對此委派管理員帳戶具有足夠權限的所有使用者都可以從該帳戶執行所有 IAM Identity Center 管理任務，但下列情況除外：
>
> - 啟用 IAM 身分識別中心
> - 刪除 IAM 身分中心組態
> - 管理管理帳戶中佈建的權限集
> - 將其他成員帳戶註冊或取消註冊為委派管理員
> - 啟用或停用管理帳戶中的使用者存取
>
> 委派的管理員可以編輯群組成員資格。

註冊會員帳號

1. AWS Management Console 使用您的管理帳戶的認證登入 AWS Organizations。執行 RegisterDelegatedAdministratorAPI 需要管理帳戶認證。
2. 選取啟用 IAM 身分中心的區域，然後開啟 IAM 身分中心主控台。
3. 請選擇 [設定]，然後選取 [管理] 索引標籤。

4. 在 [委派管理員] 區段中，選擇 [註冊帳戶]。
5. 在 [註冊委派的系統管理員] 頁面上，選取 AWS 帳戶 您要註冊的，然後選擇 [註冊帳戶]。

取消註冊成員帳戶

您只能在使用管理帳戶的認證登入時取消註冊成員帳戶。

請遵循下列程序，透過取消註冊 AWS 組織中先前指定為委派管理員的成員帳戶，以移除 IAM Identity Center 的管理存取權。

> **Important**
>
> 取消註冊帳戶時，您可以有效地移除所有管理員使用者從該帳戶管理 IAM 身分中心的功能。因此，他們無法再從此帳戶管理 IAM 身分識別中心身分、存取管理、驗證或應用程式存取。此操作不會影響 IAM Identity Center 中設定的任何許可或指派，因此不會對您的使用者造成任何影響，因為他們將繼續可以 AWS 帳戶 從存取入口網站 AWS 存取其應用程式。

取消註冊會員帳戶

1. AWS Management Console 使用您的管理帳戶的認證登入 AWS Organizations。執行 DeregisterDelegatedAdministratorAPI 需要管理帳戶認證。
2. 選取啟用 IAM 身分中心的區域，然後開啟 IAM 身分中心主控台。
3. 請選擇 [設定]，然後選取 [管理] 索引標籤。
4. 在 [委派管理員] 區段中，選擇 [取消註冊帳戶]。
5. 在 [取消註冊帳戶] 對話方塊中，檢閱安全性隱患，然後輸入成員帳戶的名稱以確認您瞭解。
6. 選擇「取消註冊帳戶」。

檢視哪個成員帳戶已註冊為委派管理員

請使用下列程序，找出您的哪個成員帳戶 AWS Organizations 已設定為 IAM 身分中心的委派管理員。

查看您的註冊會員帳戶

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。

3. 在 [詳細資料] 區段中，在 [委派管理員] 底下找出已註冊的帳戶 您也可以選取「管理」頁籤，然後在「委派管理員」段落下檢視，來尋找此資訊。

臨時高架通道

對您的所有訪問都 AWS 帳戶 涉及某種級別的特權。敏感的作業 (例如，變更高價值資源的組態 (例如，生產環境) 需要特別處理，因為範圍和潛在的影響。暫時提升存取權限 (也稱為 just-in-time 存取) 是要求、核准和追蹤使用權限的一種方式，以便在指定時間內執行特定工作。臨時升級訪問可補充其他形式的訪問控制，例如權限集和多因素身份驗證。

AWS IAM Identity Center 為不同業務和技術環境中的臨時提升訪問管理提供以下選項：

- 供應商管理和支援的解決方案 — AWS 已驗證特定合作夥伴產品的 IAM Identity Center 整合，並根據一組常見的客戶需求評估其功能。選擇最符合您案例的解決方案，並遵循供應商的指引，透過 IAM 身分中心啟用此功能。
- 自我管理和自我支援 — 如果您對 AWS 僅限暫時提升存取權感興趣，而且您可以自行部署、量身打造和維護功能，此選項會提供一個起點。如需詳細資訊，請參閱暫時提升存取管理 (TEAM)。

經過驗證的 AWS 安全合作夥伴，可提升

AWS 安全合作夥伴使用不同的方法來解決一組常見的臨時提升存取需求。我們建議您仔細檢閱每個合作夥伴解決方案，以便選擇最符合您需求和偏好的解決方案，包括您的業務、雲端環境的架構和預算。

> **Note**
>
> 對於災難復原，我們建議您在中斷發生之 AWS Management Console前設定緊急存取。

AWS Identity 已針對 AWS 安全性合作夥伴提供的下列 just-in-time 產品，驗證了與 IAM 身分中心的功能和整合：

- CyberArk Secure Cloud Access— 其中一部分CyberArk Identity Security Platform，此產品提供了對多雲環境的按需 AWS 提升訪問權限。透過與 ITSM 或 ChatOps 工具整合來解決核准。可以記錄所有會話以進行審核和合規。
- Tenable (previously Ermetic)— 該Tenable平台包括為管理操作 AWS 和多雲環境中的 just-in-time特權訪問提供。來自所有雲端環境的工作階段記錄 (包括 AWS CloudTrail 存取記錄) 都可在單一介面中取得，以供分析和稽核使用。該功能與 Slack 和 Microsoft 團隊等企業和開發人員工具集成。

- Okta存取請求 — Okta 身分治理的一部分，可讓您設定 just-in-time 存取請求工作流程，使用Okta身分識別中心外部身分提供者 (IdP) 和 IAM 身分中心權限集。

此清單將更新，以 AWS 驗證其他合作夥伴解決方案的功能，以及這些解決方案與 IAM 身分中心的整合。

> **Note**
>
> 如果您正在使用以資源為基礎的政策，Amazon Elastic Kubernetes Service (Amazon EKS) 或 AWS Key Management Service (AWS KMS)，請在選擇解決方案參考資源政策、Amazon EKS 和中的權限集 AWS KMS之前先查看。 just-in-time

評估 AWS 合作夥伴驗證的臨時提升存取能力

AWS Identity 已驗證CyberArk Secure Cloud Access、Tenable和「存取要求」提供的暫時提升Okta存取功能可滿足下列常見客戶需求：

- 使用者可以針對使用者指定的時段要求存取權限集，指定 AWS 帳戶、權限集、期間和原因。
- 使用者可以接收申請的核准狀態。
- 使用者無法呼叫具有指定範圍的工作階段，除非具有相同範圍的已核准要求，並且在核准的期間叫用工作階段。
- 有一種方法可以指定誰可以核准請求。
- 核准者無法核准自己的請求。
- 核准者有擱置中、已核准和已拒絕請求的清單，可以將其匯出給稽核者。
- 核准者可以核准和拒絕擱置請求。
- 核准者可以新增說明其決定的備註。
- 核准人可以撤銷核准的要求，防止 future 使用提升的存取權。

> **Note**
>
> 如果使用者在撤銷核准的要求時以提升的存取權登入，則在核准撤銷後，其工作階段會保持作用中狀態最多一小時。如需驗證工作階段的資訊，請參閱身分驗證。

- 使用者動作和核准可供稽核。

單一登入存取權 AWS 帳戶

您可以 AWS Organizations 根據一般工作職能，將連線目錄中的使用者指派給組織中的管理帳戶或成員帳戶的權限。或者，您也可依照具體的安全需求，使用合適的自訂許可。例如，您可以授與資料庫管理員廣泛的權限給開發帳戶中的 Amazon RDS，但限制他們在生產帳戶中的許可。IAM 身分中心會自動設定所有必要的使用者許可。 AWS 帳戶

> **Note**
>
> 您可能需要授與使用者或群組在 AWS Organizations 管理帳戶中操作的權限。由於這是一個高度權限的帳戶，因此額外的安全限制要求您必須擁有 IAM FullAccess 政策或同等許可，然後才能進行設定。 AWS 組織中的任何成員帳戶都不需要這些額外的安全性限制。

指派使用者存取權給 AWS 帳戶

使用下列程序將單一登入存取權指派給連線目錄中的使用者和群組，並使用權限集來決定其存取層級。

若要檢查現有的使用者和群組存取權，請參閱檢視使用者和群組指派。

> **Note**
>
> 為了簡化存取許可的管理，我們建議您直接對群組 (而非個別使用者) 指派存取。透過群組，您可以對使用者群組授予或拒絕許可，而不需要為每個使用者套用這些許可。如果使用者移到不同的組織，則只要將該使用者移到不同的群組，即可自動接收新組織所需的許可。

若要將使用者或群組存取權指派給 AWS 帳戶

1. 開啟 IAM 身分中心主控台。

   > **Note**
   >
   > 在進行下一個步驟之前，請確定 IAM 身分中心主控台使用 AWS Managed Microsoft AD 目錄所在的區域。

2. 在功能窗格中的 [多帳戶權限] 下，選擇 AWS 帳戶[。
3. 在此AWS 帳戶頁面上，會出現組織的樹狀檢視清單。選取要指派單一登入存取權 AWS 帳戶 的一或多個旁邊的核取方塊。

> **Note**
>
> 將單一登入存取權指派給使用者和群組時，每個權限集最多可以選取 10 AWS 帳戶 個。若要將 10 個以上的使 AWS 帳戶 用者和群組指派給同一組使用者和群組，請視需要對其他帳戶重複此程序。出現提示時，請選取相同的使用者、群組和權限集。

4. 選擇 [指派使用者或群組]。
5. 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-account-name***" 頁面上，執行下列操作：

   1. 在 [使用者] 索引標籤上，選取要授與單一登入存取權的一或多個使用者。

      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. 在 [群組] 索引標籤上，選取要授與單一登入存取權的一或多個群組。

      若要篩選結果，請開始在搜尋方塊中輸入您要的群組名稱。

   3. 若要顯示您選取的使用者和群組，請選擇 [選取的使用者和群組] 旁邊的橫向三角形。
   4. 確認選取正確的使用者和群組之後，請選擇 [下一步]。
6. 對於步驟 2: 選取權限集，在 [將權限集指派給 "***AWS-account-name***" 頁面上，執行下列動作：

   1. 選取一或多個權限集。如有必要，您可以建立並選取新的權限集。
      - 若要選取一或多個現有權限集，請在 [權限集] 下，選取您要套用至您在上一個步驟中選取之使用者和群組的權限集。
      - 若要建立一或多個新權限集，請選擇 [建立權限集]，然後遵循中的步驟建立許可集合。建立要套用的權限集後，請在 IAM Identity Center 主控台中返回AWS 帳戶並遵循指示進行操作，直到到達「步驟 2：選取權限集」為止。當您執行此步驟時，請選取您建立的新權限集，然後繼續執行此程序的下一個步驟。
   2. 確認選取正確的權限集之後，請選擇 [下一步]。
7. 對於步驟 3：複查並提交，請在「複查並提交指定至」***AWS-###############***作：

   1. 檢閱選取的使用者、群組和權限集。
   2. 確認已選取正確的使用者、群組和權限集之後，請選擇 [提交]。

> **Important**
>
> 使用者和群組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，直到程序順利完成為止。

> **Note**
>
> 您可能需要授與使用者或群組在 AWS Organizations 管理帳戶中操作的權限。由於這是一個高度權限的帳戶，因此額外的安全限制要求您必須擁有 IAM FullAccess 政策或同等許可，然後才能進行設定。 AWS 組織中的任何成員帳戶都不需要這些額外的安全性限制。

移除使用者和群組存取

使用此程序可移除連線目錄中一或多個使 AWS 帳戶 用者和群組的單一登入存取權。

若要移除使用者和群組存取 AWS 帳戶

1. 開啟 IAM 身分中心主控台。
2. 在功能窗格中的 [多帳戶權限] 下，選擇 AWS 帳戶[。
3. 在此AWS 帳戶頁面上，會出現組織的樹狀檢視清單。選取包含您要移除其單一登入存取權之使用者和群組的名稱。 AWS 帳戶
4. 在的 [概觀] 頁面上 AWS 帳戶，在 [已指派的使用者和群組] 下，選取一或多個使用者或群組的名稱，然後選擇 [移除存取權]。
5. 在 [移除存取權] 對話方塊中，確認使用者或群組的名稱正確無誤，然後選擇 [移除存取權]。

撤銷由權限集建立的作用中 IAM 角色工作階段

以下是撤銷 IAM 身分中心使用者的作用中權限集工作階段的一般程序。此程序假設您想要移除已洩露認證的使用者或系統中不良參與者的所有存取權。先決條件是遵循中的指導準備撤銷由權限集建立的作用中 IAM 角色工作階段。我們假設拒絕所有原則存在於服務控制原則 (SCP) 中。

> **Note**
>
> AWS 建議您構建自動化以處理除僅限控制台操作之外的所有步驟。

1. 取得您必須撤銷其存取權之人員的使用者 ID。您可以使用識別身分存放區 API，依使用者的使用者名稱尋找使用者。
2. 更新「拒絕」原則，以從服務控制原則 (SCP) 中的步驟 1 新增使用者識別碼。完成此步驟後，目標使用者將失去存取權，而且無法對策略影響的任何角色採取動作。
3. 移除使用者的所有權限集指派。如果存取權是透過群組成員資格指派，請從所有群組和所有直接權限集指派中移除使用者。此步驟可防止使用者擔任任何其他 IAM 角色。如果使用者擁有使用中 AWS 存取入口網站工作階段，而您停用該使用者，則他們可以繼續擔任新角色，直到您移除其存取權為止。
4. 如果您使用身分識別提供者 (IdP) 或 Microsoft Active Directory 做為身分識別來源，請停用身分識別來源中的使用者。停用使用者可防止建立額外的 AWS 存取入口網站工作階段。使用您的 IdP 或 Microsoft 活動目錄 API 文檔來了解如何自動化此步驟。如果您使用 IAM 身分中心目錄做為身分識別來源，請勿停用使用者存取權。您將在步驟 6 中停用使用者存取權。
5. 在 IAM 身分中心主控台中，尋找使用者並刪除其使用中的工作階段。

   a. 選擇 Users (使用者)。

   b. 選擇您要刪除其作用中階段作業的使用者。

   c. 在使用者的詳細資料頁面上，選擇作用中工作階段索引標籤。

   d. 選取您要刪除的工作階段旁邊的核取方塊，然後選擇刪除工作階段。

   如此可確保使用者的 AWS 存取入口網站工作階段在大約 60 分鐘內停止。瞭解工作階段持續時間。
6. 在 IAM 身分中心主控台中，停用使用者存取權。

   a. 選擇 Users (使用者)。

   b. 選擇您要停用其存取權的使用者。

   c. 在使用者的詳細資訊頁面上，展開 [一般資訊]，然後選擇 [停用使用者存取] 按鈕，以防止使用者進一步登入。
7. 將 [拒絕] 原則保留至少 12 小時。否則，具有有效 IAM 角色工作階段的使用者將會恢復具有 IAM 角色的動作。如果您等待 12 小時，作用中工作階段就會過期，使用者將無法再次存取 IAM 角色。

> **Important**
>
> 如果在停止使用者工作階段之前停用使用者的存取權限 (您未完成步驟 5 就完成了步驟 6)，則無法再透過 IAM Identity Center 主控台停止使用者工作階段。如果您在停止使用者工作階段之前不小心停用使用者存取權，您可以重新啟用使用者、停止其工作階段，然後再次停用其存取權。

如果使用者的密碼遭到入侵，您現在可以變更使用者的認證，並還原其指派。

委派誰可以將單一登入存取權指派給管理帳戶中的使用者和群組

使用 IAM 身分中心主控台將單一登入存取權指派給管理帳戶是一項特權動作。根據預設，只有 AWS 帳戶根使用者 或已附加AWSSSOMasterAccountAdministrator和IAMFullAccess AWS 受管理策略的使用者可以將單一登入存取權指派給管理帳戶。AWSSSOMasterAccountAdministrator和原IAMFullAccess則會管理 AWS Organizations 組織內管理帳戶的單一登入存取權。

使用下列步驟將管理單一登入存取權限委派給目錄中的使用者和群組。

授與管理目錄中使用者和群組的單一登入存取權限

1. 以管理帳戶的根使用者身分或具有管理帳戶管理員權限的其他使用者身分登入 IAM Identity Center 主控台。
2. 依照中的步驟建立許可集合建立權限集，然後執行下列動作：
    1. 在 [建立新權限集] 頁面上，選取 [建立自訂權限集] 核取方塊，然後選擇 [下一步：詳細資料]。
    2. 在 [建立新權限集] 頁面上，指定自訂權限集的名稱，並選擇性地指定描述。必要時，請修改工作階段持續時間並指定轉送狀態 URL。

        > **Note**
        >
        > 對於轉送狀態 URL，您必須指定位於中的 URL AWS Management Console。例如：**`https://console.aws.amazon.com/ec2/`**
        > 如需詳細資訊，請參閱 設定繼電器狀態。

    3. 在 [您想要在權限集中包含哪些原則] 底下？ ，選取 [附加 AWS 受管理的策略] 核取方塊。
    4. 在 IAM 政策清單中，選擇AWSSSOMasterAccountAdministrator和受IAMFullAccess AWS 管政策。這些原則會將權限授與 future 被指派此權限集存取權的任何使用者和群組。

5. 選擇下一步：標籤。
6. 在「新增標籤 (選用)」下，指定「機碼與值」(選用) 的值，然後選擇「下一步：複查」。如需標籤的詳細資訊，請參閱標記 AWS IAM Identity Center 資源。
7. 檢閱您所做的選取，然後選擇 [建立]。

3. 請遵循中的步驟，指派使用者存取權給 AWS 帳戶將適當的使用者和群組指派給您剛建立的權限集。
4. 將下列內容傳達給指派的使用者：當他們登入 AWS 存取入口網站並選擇 [帳戶] 索引標籤時，他們必須選擇適當的角色名稱，以便使用您剛才委派的權限進行驗證。

許可集

權限集是您建立和維護的範本，可定義一或多個 IAM 政策的集合。權限集可簡化組織中使用者和群組的 AWS 帳戶 存取權指派作業。例如，您可以建立資料庫管理員權限集，其中包括管理 AWS RDS、DynamoDB 和 Aurora 服務的原則，並使用該單一權限集為資料庫管理員授與AWS 組織 AWS 帳戶內目標清單的存取權。

IAM 身分中心 AWS 帳戶 透過權限集，將存取權指派給一或多個使用者或群組。指派權限集時，IAM 身分中心會在每個帳戶中建立對應的 IAM 身分中心控制的 IAM 角色，並將權限集中指定的政策附加到這些角色。IAM 身分中心管理角色，並允許您定義的授權使用者擔任該角色，方法是使用 IAM 身分中心使用者入口網站或 AWS CLI。 當您修改權限集時，IAM 身分中心會確保相應地更新對應的 IAM 政策和角色。

您可以將AWS 受管政策、客戶管理的政策、內嵌政策和工作職能的AWS 受管理政策新增至您的權限集。您也可以將 AWS 受管政策或客戶管理的政策指派為權限界限。

若要建立權限集，請參閱建立、管理及刪除權限集。

主題

- 預定義權限
- 自訂權限
- 建立、管理及刪除權限集
- 設定權限集屬性

預定義權限

您可以使用 AWS 受管理的原則建立預先定義的權限集。

當您使用預先定義的權限建立權限集時，您可以從 AWS 受管理的原則清單中選擇一個原則。在可用的原則中，您可以從一般權限原則和 Job 職能原則中進行選擇。

一般權限原則

從 AWS 受管政策清單中選擇，讓您能夠存取整個資源 AWS 帳戶。您可以新增下列其中一個原則：

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

Job 職能政策

從 AWS 受管理的政策清單中選擇，這些策略可讓您存取 AWS 帳戶 可能與組織內工作相關的資源。您可以新增下列其中一個原則：

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

如需可用一般權限原則和工作職能原則的詳細說明，請參閱AWS Identity and Access Management 使用者指南中的工作職能AWS 受管理原則。

如需如何建立權限集的指示，請參閱建立、管理及刪除權限集。

自訂權限

您可以使用自訂許可建立權限集，結合您在 AWS Identity and Access Management (IAM) 中擁有的任何受管政策和客戶受管政策以及內嵌政策。 AWS 您也可以包含權限界限，設定其他原則可以授與您權限集之使用者的最大可能權限。

如需如何建立權限集的指示，請參閱建立、管理及刪除權限集。

您可以附加至權限集的原則類型

主題

內嵌政策

您可以將內嵌原則附加至權限集。內嵌政策是格式化為 IAM 政策的文字區塊，您可以直接新增至權限集。您可以在建立新權限集時貼上政策，或使用 IAM Identity Center 主控台中的政策建立工具產生新的政策。您也可以使用AWS 政策產生器建立 IAM 政策。

當您使用內嵌政策部署權限集時，IAM 身分中心會在您指派權限集的 AWS 帳戶 位置建立 IAM 政策。IAM 身分中心會在您將權限集指派給帳戶時建立政策。然後，該政策會附加到您的使用者假設 AWS 帳戶 的 IAM 角色。

當您建立內嵌政策並指派權限集時，IAM 身分中心會 AWS 帳戶 為您設定中的政策。當您使用建立權限集時客戶受管政策，必須先 AWS 帳戶 自行建立原則，才能指派權限集。

AWS 受管理政策

您可以將AWS 受管理的原則附加至您的權限集。 AWS 受管政策是 AWS 維護的 IAM 政策。相反地，客戶受管政策是您在帳戶中建立和維護的 IAM 政策。 AWS 受管理的政策可解決您的 AWS 帳戶. 您可以將受 AWS 管政策指派為 IAM 身分中心建立之角色的許可，或指派為許可界限。

AWS 維護工作職能的AWS 管理策略，這些策略將工作特定的訪問權限分配給您的 AWS 資源。當您選擇搭配權限集使用預先定義的權限時，您可以新增一個工作函數原則。當您選擇 [自訂] 權限時，您可以新增多個工作功能原則。

您 AWS 帳戶 還包含大量針對特定 AWS 服務 和組合的 AWS 受管 IAM 政策 AWS 服務。當您使用 [自訂] 權限建立權限集時，您可以從許多其他 AWS 受管理的原則中進行選擇，以指派給您的權限集。

AWS 填入每個 AWS 受管理 AWS 帳戶 的策略。若要使用 AWS 受管政策部署權限集，您不需要先在 AWS 帳戶. 當您使用建立權限集時客戶受管政策，必須先 AWS 帳戶 自行建立原則，才能指派權限集。

如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南中的AWS 受管政策。

客戶受管政策

您可以將客戶管理的政策附加至您的權限集。客戶受管政策是您在帳戶中建立和維護的 IAM 政策。相反地，您帳戶中AWS 受管理政策是否 AWS 會維護 IAM 政策。您可以將客戶受管政策指派為 IAM Identity Center 建立之角色的許可，或指派為許可界限。

當您使用客戶受管政策建立權限集時，您必須在每個 IAM Identity Center 為您指派權限集的每個項目 AWS 帳戶 中，建立具有相同名稱和路徑的 IAM 政策。如果您要指定自訂路徑，請務必在每個路徑中指定相同的路徑 AWS 帳戶。如需詳細資訊，請參閱《IAM 使用者指南》中的易記名稱和路徑。IAM 身分中心會將 IAM 政策附加到在您的 AWS 帳戶. 最佳作法是將相同的權限套用至您指派權限集的每個帳戶中的原則。如需詳細資訊，請參閱 在權限集中使用 IAM 政策。

如需詳細資訊，請參閱 IAM 使用者指南中的客戶受管政策。

許可界限

您可以將權限界限附加至權限集。許可界限是 AWS 受管或客戶受管的 IAM 政策，用於設定以身分為基礎的政策可授予 IAM 主體的最大許可。當您套用權限界限時，您的內嵌政策客戶受管政策、和AWS 受管理政策無法授與超出權限界限所授與之權限的任何權限。許可界限不會授予任何許可，而是使 IAM 忽略超出界限的所有許可。

當您建立以客戶受管政策做為許可界限的權限集時，您必須在每個 IAM Identity Center 為您指派權限集的每 AWS 帳戶 個權限集建立具有相同名稱的 IAM 政策。IAM 身分中心會將 IAM 政策做為許可界限附加到在您建立的 IAM 角色 AWS 帳戶 。

如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 實體許可界限。

建立、管理及刪除權限集

權限集定義使用者和群組對的存取層級 AWS 帳戶。權限集會儲存在 IAM 身分中心，並且可以佈建至一或多個 AWS 帳戶。您可以為使用者指派多個許可集合。如需有關權限集及其在 IAM 身分中心使用方式的詳細資訊，請參閱許可集。

建立權限集時，請記住下列考量事項：

- 從預先定義的權限集開始

  使用預先定義的權限集 (使用預先定義的權限)，您可以從可用原則清單中選擇單一 AWS 受管理的原則。每個原則都會授與特定層級的 AWS 服務和資源存取權，或是一般工作職能的權限。如需這些原則的相關資訊，請參閱工作職能的AWS 受管理原則。收集使用情況資料後，您可以將權限集精簡為更具限制性。

- 將管理會話持續時間限制在合理的工作

  當使用者聯合到其 AWS 帳戶 並使用 AWS 管理主控台或 AWS 命令列介面 (AWS CLI) 時，IAM Identity Center 會使用權限集上的工作階段持續時間設定來控制工作階段的持續時間。當使用者工作階段達到工作階段持續時間時，就會登出主控台並要求重新登入。作為安全性最佳作法，建議您不要將工作階段持續時間長度設定超過執行角色所需的長度。依預設，工作階段持續時間的值為一小時。您可以指定 12 小時的最大值。如需詳細資訊，請參閱 設定工作階段期。

- 限制工作人員使用者入口網站

  員工使用者使用入口網站工作階段來選擇角色並存取應用 根據預設，工作階段持續時間上限的值 (決定員工使用者在必須重新驗證之前可登入 AWS 存取入口網站的時間長度) 為八小時。您可以指定 90 天的最大值。如需詳細資訊，請參閱 設定 AWS 存取入口網站和 IAM 身分中心整合應用程式的工作階段持續時間。

- 使用提供最低權限權限的角色

  您建立並指派給使用者的每個權限集，都會在 AWS 存取入口網站中顯示為可用角色。
  當您以該使用者身分登入入口網站時，請選擇與限制最嚴格的權限集合相對應的角色，
  而`AdministratorAccess`不是在帳戶中執行工作。在傳送使用者邀請之前，測試您的權限集，以確認其提供必要的存取權。

> **Note**
>
> 您也可以使用AWS CloudFormation來建立和指派權限集，以及將使用者指派給這些權限集。

主題

建立許可集合

您可以使用此程序來建立使用單一 AWS 受管理原則的預先定義權限集，或使用多達 10 個 AWS 受管理或客戶管理的原則和內嵌原則的自訂權限集。您可以在 IAM 的 Service Quotas 主控台中要求調整最多 10 個政策數目。

您可以在 IAM 身分中心主控台中建立權限集。

建立許可集合

1. 開啟 IAM 身分中心主控台。
2. 在 [多帳戶權限] 下，選擇 [權限集]。
3. 選擇 Create permission set (建立許可集合)。
4. 在 [選取權限集類型] 頁面的 [權限集類型] 下，選取權限集類型。
5. 根據權限集類型，選擇您要用於權限集的一或多個原則：

   - 預先定義權限集

     1. 在 [預先定義權限集的原則] 下，選取清單中的其中一個 IAM Job 功能政策或一般權限政策，然後選擇 [下一步]。如需詳細資訊，請參閱AWS 《AWS Identity and Access Management 使用指南》中的工作職能的AWS 受管理策略和受管理的策略。
     2. 移至步驟 6 以完成 [指定權限集詳細資料] 頁面。

   - 自訂權限集

     1. 選擇下一步。
     2. 在 [指定政策和權限界限] 頁面上，選擇要套用至新權限集的 IAM 政策類型。根據預設，您可以將最多 10 個AWS 受管政策和客戶管理原則的任意組合新增至您的權限集。此配額由 IAM 設定。若要提高政策，請在每個 AWS 帳戶 您要指派權限集的 Service Quotas 主控台中，要求增加附加至 IAM 角色的 IAM 配額受管政策。

        - 展開AWS 受管政策，從 AWS 建置和維護的 IAM 新增政策。如需詳細資訊，請參閱 AWS 受管理政策。

          a. 搜尋並選擇您要在權限集中套用至使用者的AWS 受管理策略。

          b. 如果您要新增其他類型的原則，請選擇其容器並進行選取。選擇所有要套用的策略後，請選擇 [下一步]。移至步驟 6 以完成 [指定權限集詳細資料] 頁面。

        - 展開客戶受管政策，從您建立和維護的 IAM 新增政策。如需詳細資訊，請參閱 客戶受管政策。

          a. 選擇 [附加原則]，然後輸入您要新增至權限集的原則名稱。在您要指派權限集的每個帳戶中，使用您輸入的名稱建立策略。最佳做法是為每個帳戶中的策略指派相同的權限。

          b. 選擇 [附加更多] 以新增其他原則。

          c. 如果您要新增其他類型的原則，請選擇其容器並進行選取。選擇所有要套用的策略後，請選擇 [下一步]。移至步驟 6 以完成 [指定權限集詳細資料] 頁面。

- 展開內嵌政策以新增自訂 JSON 格式的原則文字。內嵌政策與現有 IAM 資源不對應。若要建立內嵌政策，請在提供的表單中輸入自訂原則語言。IAM 身分中心會將政策新增至其在您的成員帳戶中建立的 IAM 資源。如需詳細資訊，請參閱 內嵌政策。

  a. 在互動式編輯器中將所需的動作和資源新增至內嵌政策。可以使用 Add new 語句添加其他語句。

  b. 如果您要新增其他類型的原則，請選擇其容器並進行選取。選擇所有要套用的策略後，請選擇 [下一步]。移至步驟 6 以完成 [指定權限集詳細資料] 頁面。

- 展開許可界限，以新增 AWS 受管或客戶受管 IAM 政策，做為權限集中其他政策可指派的最大許可。如需詳細資訊，請參閱 許可界限。

  a. 選擇 [使用權限界限] 控制權限上限。

  b. 選擇AWS 受管政策，從 IAM 設定AWS建置和維護做為許可界限的政策。選擇客戶受管政策，從您建立和維護的 IAM 設定政策，做為您的許可界限。

  c. 如果您要新增其他類型的原則，請選擇其容器並進行選取。選擇所有要套用的策略後，請選擇 [下一步]。移至步驟 6 以完成 [指定權限集詳細資料] 頁面。

6. 在 [指定權限集詳細資料] 頁面上，執行下列動作：

   1. 在 [權限集名稱] 下，輸入名稱以識別 IAM 身分中心中的此權限集。您為此權限集指定的名稱會以可用角色的形式出現在 AWS 存取入口網站中。使用者登入 AWS 存取入口網站，選擇一個 AWS 帳戶，然後選擇角色。
   2. (選用) 您也可以輸入描述。說明僅會顯示在 IAM 身分中心主控台中，而不會顯示在 AWS 存取入口網站中。
   3. (選擇性) 指定「階段作業持續時間」的值。這個值會決定使用者在主控台將使用者登出工作階段之前可登入的時間長度。如需詳細資訊，請參閱 設定工作階段期。
   4. (選擇性) 指定「轉送」狀態的值。此值用於聯合程序中，用來重新導向帳戶內的使用者。如需詳細資訊，請參閱 設定繼電器狀態。

      > **Note**
      >
      > 轉送狀態 URL 必須位於 AWS Management Console. 例如：
      > **`https://console.aws.amazon.com/ec2/`**

   5. 展開標籤（可選），選擇「新增標籤」，然後指定「機碼和值」的值（可選）。

      如需標籤的相關資訊，請參閱標記 AWS IAM Identity Center 資源。

   6. 選擇下一步。

7. 在 [檢閱並建立] 頁面上，檢閱您所做的選取項目，然後選擇 [建立]。
8. 根據預設，當您建立權限集時，不會佈建權限集 (用於任何 AWS 帳戶)。若要佈建中的權限集 AWS 帳戶，您必須將 IAM Identity Center 存取權指派給帳戶中的使用者和群組，然後將權限集套用至這些使用者和群組。如需詳細資訊，請參閱 單一登入存取權 AWS 帳戶。

委派權限集管理

IAM 身分中心可讓您透過建立參考 IAM 身分中心資源之 Amazon 資源名稱 (ARN) 的 IAM 政策，委派管理帳戶中的許可集和指派。例如，您可以建立策略，讓不同管理員管理指定帳戶中具有特定標籤之權限集的指派。

您可以使用下列其中一種方法來建立這些類型的策略。

- (建議) 在 IAM Identity Center 中建立權限集，每個權限集都有不同的政策，並將權限集指派給不同的使用者或群組。這可讓您管理使用您選擇的 IAM 身分中心身分識別來源登入的使用者的管理許可。
- 在 IAM 中建立自訂政策，然後將其附加到管理員假設的 IAM 角色。如需角色的相關資訊，請參閱 IAM 角色以取得其指派的 IAM 身分中心管理許可。

> **Important**
>
> IAM 身分中心資源 ARN 區分大小寫。

以下顯示參考 IAM 身分中心權限集和帳戶資源類型的適當案例。

資源類型	ARN	上下文鍵
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`
帳戶	`arn:${Partition}:sso:::account/${AccountId}`	不適用

在權限集中使用 IAM 政策

在中建立許可集合，您學習瞭如何將原則 (包括客戶管理的策略和權限界限) 新增至權限集。將客戶受管政策和許可新增至權限集時，IAM 身分中心不會在任何項目中建立政策 AWS 帳戶。您必須在要指派權限集的每個帳戶中預先建立這些原則，並將它們與權限集的名稱和路徑規格相符。將權限集指派給組織 AWS 帳戶 中的一個時，IAM 身分中心會建立 AWS Identity and Access Management (IAM) 角色，並將您的 IAM 政策附加到該角色。

> **Note**
>
> 使用 IAM 政策指派權限集之前，您必須準備好成員帳戶。成員帳戶中 IAM 政策的名稱必須與管理帳戶中的政策名稱區分大小寫。如果您的成員帳戶中不存在該政策，IAM 身分識別中心將無法指派權限集。
> 政策授予的權限不一定要在帳戶之間完全相符。

將 IAM 政策指派給權限集

1. 在您要指派權限集的每個 AWS 帳戶 位置建立 IAM 政策。
2. 將許可指派給 IAM 政策。您可以在不同的帳戶中指派不同的權限。為了獲得一致的體驗，請在每個策略中配置和維護相同的權限。您可以使用自動化資源，例如 AWS CloudFormation StackSets 在每個成員帳戶中建立具有相同名稱和許可的 IAM 政策副本。若要取得有關的更多資訊 CloudFormation StackSets，請參閱使用指南 AWS CloudFormation StackSets中的〈AWS CloudFormation 使用〉。
3. 在管理帳戶中建立權限集，並在客戶受管政策或許可界限下新增 IAM 政策。如需如何建立權限集的詳細資訊，請參閱建立許可集合。
4. 新增任何已準備的內嵌政策、 AWS 受管政策或其他 IAM 政策。
5. 建立並指派您的權限集。

刪除權限集

如果您想要撤銷作用中的權限集工作階段，請參閱撤銷由權限集建立的作用中 IAM 角色工作階段。

您必須先從所有使用 AWS 帳戶 該權限集的使用者中移除權限集，才能從 IAM 身分中心刪除權限集。若要檢查現有的使用者和群組存取權，請參閱檢視使用者和群組指派。

若要移除權限集 AWS 帳戶

1. 開啟 IAM 身分中心主控台。
2. 在「多帳戶權限」下，選擇AWS 帳戶。
3. 在此AWS 帳戶頁面上，會出現組織的樹狀檢視清單。選取您要 AWS 帳戶 從中移除權限集的名稱。
4. 在的 [概觀] 頁面上 AWS 帳戶，選擇 [權限集] 索引標籤。
5. 選取您要移除的權限集旁邊的核取方塊，然後選擇 [移除]。
6. 在 [移除權限集] 對話方塊中，確認已選取正確的權限集，輸入確認**Delete**移除，然後選擇 [移除存取權]。

使用下列程序刪除一或多個權限集，以便組織 AWS 帳戶 中的任何人都無法再使用這些權限集。

> **Note**
>
> 已指派此權限集的所有使用者和群組，無論使 AWS 帳戶 用何種權限集，都將無法再登入。若要檢查現有的使用者和群組存取權，請參閱檢視使用者和群組指派。

若要刪除權限集 AWS 帳戶

1. 開啟 IAM 身分中心主控台。
2. 在 [多帳戶權限] 下，選擇 [權限集]。
3. 選取您要刪除的權限集，然後選擇 [刪除]。
4. 在 [刪除權限集] 對話方塊中，輸入要確認刪除的權限集名稱，然後選擇 [刪除]。名稱區分大小寫。

設定權限集屬性

在 IAM 身分中心，您可以透過設定下列權限集屬性來自訂使用者體驗。

主題

- 設定工作階段期
- 設定繼電器狀態
- 使用拒絕政策撤銷作用中使用者權限

設定工作階段期

對於每個權限集合，您可以指定工作階段持續時間，以控制使用者可登入的時間長度 AWS 帳戶。當指定的持續時間過後，會將使用者 AWS 登出工作階段。

當您建立新的權限集時，工作階段持續時間預設會設定為 1 小時 (以秒為單位)。最短會話持續時間為 1 小時，最多可以設置為 12 小時。IAM 身分中心會針對每個權限集，在每個指派的帳戶中自動建立 IAM 角色，並將這些角色設定為最長 12 小時的工作階段持續時間。

當使用者聯合到其 AWS 帳戶 主控台或使用 AWS Command Line Interface (AWS CLI) 時，IAM Identity Center 會使用權限設定的工作階段持續時間設定來控制工作階段的持續時間。根據預設，IAM 身分中心針對許可集產生的 IAM 角色只能由 IAM 身分中心使用者承擔，這可確保強制執行 IAM 身分中心權限集中指定的工作階段持續時間。

> **Important**
>
> 基於安全最佳實務，建議工作階段持續時間的長度設定勿超過執行其角色所需的時間。

建立權限集之後，您可以更新它以套用新的工作階段持續時間。使用下列程序來修改權限集的工作階段持續時間長度。

設定工作階段持續時間

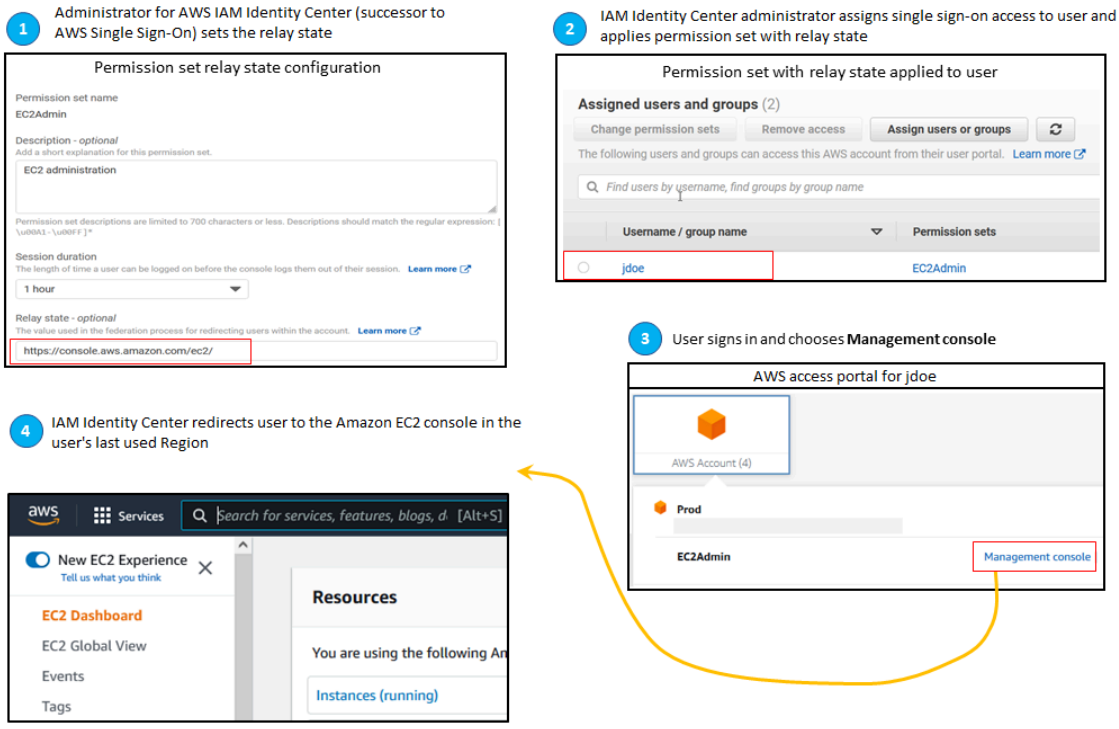
1. 開啟 IAM 身分中心主控台。
2. 在 [多帳戶權限] 下，選擇 [權限集]。
3. 選擇您要變更其工作階段持續時間之權限集的名稱。
4. 在權限集的詳細資料頁面上，選擇 [一般設定] 區段標題右側的 [編輯]。
5. 在 [編輯一般權限集設定] 頁面上，選擇 [工作階段持續時間] 的新值。
6. 如果在任何權限集中佈建 AWS 帳戶，帳戶的名稱會顯示在下方，AWS 帳戶 以便自動重新佈建。更新權限集的工作階段持續時間值之後，會重新佈建所有使用 AWS 帳戶 該權限集的使用者。這表示此設定的新值會套用至所有使 AWS 帳戶 用權限集的使用者。
7. 選擇儲存變更。
8. AWS 帳戶頁面頂端會顯示通知。

    - 如果在一或多個使用權限集中佈建 AWS 帳戶，則通知會確認已成功重新佈建，並將更新的權限集套用至帳戶。 AWS 帳戶

- 如果未在中佈建權限集 AWS 帳戶，則通知會確認權限集的設定已更新。

設定繼電器狀態

根據預設，當使用者登入 AWS 存取入口網站、選擇帳戶，然後選擇從指派的權限集 AWS 建立的角色時，IAM Identity Center 會將使用者的瀏覽器重新導向至 AWS Management Console. 您可以將轉送狀態設定為不同的主控台 URL，以變更此行為。設定轉送狀態可讓您讓使用者快速存取最適合其角色的主控台。例如，您可以將轉送狀態設定為 Amazon EC2 主控台 URL (**`https://console.aws.amazon.com/ec2/`**)，以便在使用者選擇 Amazon EC2 管理員角色時將其重新導向至該主控台。在重新導向至預設 URL 或轉送狀態 URL 期間，IAM Identity Center 會將使用者的瀏覽器路由至使用者上次 AWS 區域 使用的主控台端點。例如，如果使用者結束了歐洲 (斯德哥爾摩) 區域 (eu-north-1) 的最後一個主控台工作階段，則會將使用者重新導向至該區域中的 Amazon EC2 主控台。



若要設定 IAM 身分中心以將使用者重新導向至特定主控台 AWS 區域，請在 URL 中加入區域規格。例如，若要將使用者重新導向至美國東部 (俄亥俄) 區域 (us-east-2) 的 Amazon EC2 主控台，請指定該區域中 Amazon EC2 主控台的 URL ()。**`https://us-east-2.console.aws.amazon.com/ec2/`**如果您在美國西部 (奧勒岡) 區域 (us-west-2) 區域啟用 IAM 身分中心，並且想要將使用者導向至該區域，請指定。**`https://us-west-2.console.aws.amazon.com`**

使用下列程序來設定權限集的轉送狀態 URL。

若要設定轉送狀態

1. 開啟 IAM 身分中心主控台。
2. 在 [多帳戶權限] 下，選擇 [權限集]。
3. 選擇您要為其設定新轉送狀態 URL 的權限集名稱。
4. 在權限集的詳細資料頁面上，選擇 [一般設定] 區段標題右側的 [編輯]。
5. 在 [編輯一般權限集設定] 頁面的 [轉送狀態] 下，輸入任何 AWS 服務的主控台 URL。例如：

   `https://console.aws.amazon.com/ec2/`

   > **Note**
   >
   > 轉送狀態 URL 必須位於 AWS Management Console.

6. 如果在任何權限集中佈建 AWS 帳戶，帳戶的名稱會顯示在下方，AWS 帳戶 以便自動重新佈建。更新權限集的轉送狀態 URL 之後，會重新佈建所有使用 AWS 帳戶 該權限集的使用者。這表示此設定的新值會套用至所有使 AWS 帳戶 用權限集的使用者。
7. 選擇儲存變更。
8. 在「AWS 組織」頁面頂端，會出現一則通知。

   - 如果在一或多個使用權限集中佈建 AWS 帳戶，則通知會確認已成功重新佈建，並將更新的權限集套用至帳戶。 AWS 帳戶
   - 如果未在中佈建權限集 AWS 帳戶，則通知會確認權限集的設定已更新。

> **Note**
>
> 您可以使用 AWS API、 AWS SDK 或 AWS Command Line Interface(AWS CLI) 來自動執行此程序。如需詳細資訊，請參閱：
>
> - IAM 身分中心 API 參考中的`CreatePermissionSet`或`UpdatePermissionSet`動作
> - 《`update-permission-set`指令參考》一`sso-admin`節中的`create-permission-set`或指AWS CLI 令。

使用拒絕政策撤銷作用中使用者權限

當使用者主動使用權限集 AWS 帳戶 時，您可能需要撤銷 IAM 身分中心使用者的存取權限。您可以預先為未指定的使用者實作拒絕政策，以移除他們使用其使用中 IAM 角色工作階段的能力，然後在需要時更新拒絕政策以指定要封鎖其存取權的使用者。本主題說明如何建立拒絕原則，以及如何部署原則的考量事項。

準備撤銷由權限集建立的作用中 IAM 角色工作階段

您可以透過使用服務控制政策套用拒絕特定使用者的所有政策，以防止使用者使用他們正在使用的 IAM 角色採取動作。您也可以防止使用者在變更其密碼之前使用任何權限集，從而移除不良行為者主動濫用竊取的憑證。如果您需要廣泛拒絕存取，並防止使用者重新輸入權限集或存取其他權限集，您也可以移除所有使用者存取、停止使用中存 AWS 取入口網站工作階段，以及停用使用者登入。請參閱撤銷由權限集建立的作用中 IAM 角色工作階段以了解如何將「拒絕」原則與其他動作搭配使用，以取得更廣泛的存取撤銷。

拒絕政策

您可以使用「拒絕」政策，且條件與 IAM Identity Center 身分識別存放區`UserID`中的使用者相符，以防止使用者正在使用的 IAM 角色進一步採取行動。使用此原則可避免對在您部署拒絕原則時可能使用相同權限集的其他使用者造成影響。此原則會使用預留位置使用者 ID *`Add user ID here`*，`"identitystore:userId"`因此您將使用想要撤銷其存取權的使用者 ID 進行更新。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "identitystore:userId": "Add user ID here"
                }
            }
        }
    ]
}
```

儘管您可以使用另一個條件鍵，例如“aws:userId”，但“identitystore:userId”是肯定的，因為它是與一個人相關聯的全局唯一值。在條件“aws:userId”中使用可能會受到從身分來源同步處理使用者屬性的方式影響，並且可能會在使用者的使用者名稱或電子郵件地址變更時進行變更。

從 IAM Identity Center 主控台，您可以瀏覽至使用者、identitystore:userId依名稱搜尋使用者、展開 [一般資訊] 區段，然後複製使用者 ID，以尋找使用者的資訊。在搜索用戶 ID 時，在同一部分中停止用戶訪問門戶會話並禁用其登錄訪問權限也很方便。 AWS 您可以透過查詢身分識別身分存放區 API 來取得使用者的使用者識別碼，以自動化建立「拒絕」策略的程序。

部署拒絕策略

您可以使用無效的預留位置使用者識別碼 (例如*Add user ID here*，使用附加至使用 AWS 帳戶 者可能有權存取的服務控制原則 (SCP) 預先部署拒絕原則。這是推薦的方法，因為它的容易性和速度的影響。當您使用拒絕原則撤銷使用者的存取權時，您將編輯原則，將預留位置使用者 ID 取代為您要撤銷其存取權之人員的使用者 ID。這樣可防止使用者使用您附加 SCP 之每個帳戶中設定的任何權限來採取任何動作。即使使用者使用其使用中 AWS 存取入口網站工作階段來導覽至不同的帳戶並擔任不同的角色，它也會封鎖使用者的動作。在 SCP 完全封鎖使用者的存取權之後，您可以停用其登入、撤銷其指派的能力，以及在需要時停止其 AWS 存取入口網站工作階段。

除了使用 SCP 之外，您也可以將「拒絕」原則包含在權限集的內嵌原則中，以及使用者可以存取的權限集所使用的客戶管理策略中。

如果您必須撤銷多個人員的存取權，您可以在條件區塊中使用值清單，例如：

```
        "Condition": {
                "StringEquals": {
                    "identitystore:userId": [" user1 userId", "user2 userId"...]
                    }
    }
```

> **Important**
>
> 無論您使用哪種方法，您都必須採取任何其他更正措施，並將使用者的使用者 ID 保留在政策中至少 12 小時。在此之後，使用者假設的任何角色都會過期，然後您就可以從拒絕策略中移除其使用者識別碼。

參考資源政策、Amazon EKS 和中的權限集 AWS KMS

將權限集指派給 AWS 帳戶時，IAM 身分中心會建立名稱開頭為的角色AWSReservedSSO_。

角色的完整名稱和 Amazon 資源名稱 (ARN) 使用下列格式：

名稱	ARN
AWSReservedSSO_ *permission-set-name_unique-suffix*	arn:aws:iam:: *aws-account-ID*:role/aws-reserved/sso.amazonaws.com/ *aws-region* /AWSReservedSSO_ *permission-set-name_unique-suffix*

例如，如果您建立的權限集將 AWS 帳戶存取權授與資料庫管理員，則會以下列名稱和 ARN 建立對應的角色：

名稱	ARN
AWSReservedSSO_DatabaseAdministrator_1234567890abcdef	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef

如果您刪除 AWS 帳戶中此權限集的所有指派，IAM 身分中心建立的對應角色也會一併刪除。如果您稍後對相同的權限集進行新指派，IAM Identity Center 會為該權限集建立新角色。新角色的名稱和 ARN 包括不同的唯一尾碼。在這個例子中，唯一的後綴是 abc def0123456789。

名稱	ARN
AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**

新名稱和角色的 ARN 中的尾碼變更將導致參照原始名稱和 ARN 的任何原則變更為原始名稱和 ARN out-of-date，這會中斷使用對應權限集之個人的存取。例如，如果在下列組態中參照原始 ARN，則角色的 ARN 變更將中斷權限集使用者的存取權限：

- 在aws-auth ConfigMap文件 Amazon Elastic Kubernetes Service（Amazon EKS）
- 在以資源為基礎的策略中，用於 AWS Key Management Service （AWS KMS）鍵。此原則也稱為金鑰原則。

雖然您可以為大多數 AWS 服務更新以資源為基礎的政策，以參考與權限集對應的角色的新 ARN，但是您必須具有在 IAM 中為 Amazon EKS 建立的備份角色，以及 ARN 發生變更 AWS KMS 時。對於 Amazon EKS，備份 IAM 角色必須存在於aws-auth ConfigMap. 因為 AWS KMS，它必須存在於您的金鑰原則中。如果您在任一情況下都沒有備份 IAM 角色，則必須聯絡 AWS Support。

避免存取中斷的建議

若要避免因對應於權限集之角色的 ARN 變更而造成存取中斷，建議您執行下列動作。

- 至少維護一個權限集指派。

  在包含您在 Amazon EKS 中參考的角色、中的關鍵政策或其他人以資源aws-auth ConfigMap為基礎的政策的 AWS 帳戶中 AWS KMS維護此指派。 AWS 服務

  例如，如果您建立EKSAccess權限集，並從 AWS 帳戶參考對應的角色 ARN111122223333，則會永久地將系統管理群組指派給該帳戶中設定的權限。由於指派是永久性的，IAM 身分中心不會刪除對應的角色，進而消除重新命名的風險。系統管理群組永遠擁有存取權，而不會有權限提升的風險。
- 對於 Amazon EKS 和 AWS KMS：包括在 IAM 中創建的角色。

  如果您針對 Amazon EKS 叢集中的權限集或 AWS KMS 金鑰金鑰政策參考角色 ARN，建議您至少包含一個在 IAM 中建立的角色。aws-auth ConfigMap角色必須允許您存取 Amazon EKS 叢集或管理 AWS KMS 金鑰政策。權限集必須能夠擔任此角色。如此一來，如果權限集的角色 ARN 變更，您可以更新aws-auth ConfigMap或 AWS KMS 金鑰原則中 ARN 的參照。下一節提供如何為 IAM 中建立的角色建立信任政策的範例。角色只能由AdministratorAccess權限集承擔。

自訂信任原則範例

以下是自訂信任政策的範例，該政策提供可存取 IAM 中建立之角色的AdministratorAccess權限集。此政策的關鍵要素包括：

- 此信任策略的「主體」元素會指定 AWS 帳戶主體。在此政策中，111122223333具有sts:AssumeRole許可的 AWS 帳戶中的主體可以擔任在 IAM 中建立的角色。
- 此信任政策會針對可以承擔在 IAM 中建立Condition element的角色的主體指定其他需求。在此原則中，具有下列角色 ARN 的權限集可以擔任該角色。

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*"
```

> **Note**
>
> Condition元素包括ArnLike條件運算子，並在權限集角色 ARN 的結尾使用萬用字元，而不是唯一的尾碼。這表示即使權限集的角色 ARN 變更，政策也允許權限集承擔在 IAM 中建立的角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
        }
      }
    }
  ]
}
```

在此類政策中包含您在 IAM 中建立的角色，如果意外刪除並重新建立權限集或權限集的所有指派 AWS KMS keys，您可以緊急存取 Amazon EKS 叢集或其他 AWS 資源。

屬性型存取控制

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。您可以使用 IAM 身分中心，使用來自任何 IAM 身分中心身分識別來源的 AWS 帳戶 使用者屬性來管理多個 AWS 資源的存取。在中 AWS，這些屬性稱為標籤。在中使用使用者屬性作為標籤可 AWS 協助您簡化在中建立精細權限的程序， AWS 並確保您的員工只能存取具有相符標籤的 AWS 資源。

例如，您可以將來自兩個不同團隊的開發人員 Bob 和 Sally 指派給 IAM 身分中心中設定的相同權限，然後選取團隊名稱屬性進行存取控制。當 Bob 和 Sally 登入其時 AWS 帳戶，IAM 身分中心 AWS 會在工作階段中傳送其小組名稱屬性，以便 Bob 和 Sally 只有在其團隊名稱屬性與 AWS 專案資源上的小組名稱標籤相符時，才能存取專案資源。如果 Bob 將 future 移至 Sally 的團隊，您只需在公司目錄中更新其團隊名稱屬性，即可修改他的存取權限。當 Bob 下次登入時，他將自動存取其新團隊的專案資源，而不需要在中更新任何權限 AWS。

此方法也有助於減少在 IAM Identity Center 中建立和管理的不同許可數量，因為與相同權限集關聯的使用者現在可以根據其屬性擁有唯一的許可。您可以在 IAM 身分中心權限集和以資源為基礎的政策中使用這些使用者屬性，將 ABAC 實作至 AWS 資源，並簡化大規模的許可管理。

優勢

以下是在 IAM 身分中心使用 ABAC 的其他好處。

- ABAC 需要較少的權限集 — 因為您不需要針對不同的工作職能建立不同的原則，所以建立的權限集就越少。如此可降低您的權限管理複雜度。
- 使用 ABAC，團隊可以快速變更和成長 — 當資源在建立時適當標記資源時，會根據屬性自動授予新資源的權限。
- 搭配 ABAC 使用公司目錄中的員工屬性 — 您可以使用 IAM 身分中心中設定的任何身分來源的現有員工屬性，在中做出存取控制決策。 AWS
- 追蹤誰正在存取資源 — 安全性管理員可以透過檢閱中的使用者屬性 AWS CloudTrail 來追蹤中的使用者活動，輕鬆判斷工作階段的身份 AWS。

如需如何使用 IAM 身分中心主控台設定 ABAC 的相關資訊，請參閱存取控制的屬性。如需如何使用 IAM 身分中心 API 啟用和設定 ABAC 的詳細資訊，請參閱 CreateInstanceAccessControlAttributeConfigurationIAM 身分中心 API 參考指南中的。

主題

- 檢查清單： AWS 使用 IAM 身分中心設定 ABAC

- 存取控制的屬性

檢查清單： AWS 使用 IAM 身分中心設定 ABAC

此檢查清單包含準備 AWS 資源和設定 IAM 身分中心以進行 ABAC 存取所需的組態工作。依序完成此檢查清單中的工作。當參考連結帶您前往某個主題時，請返回本主題，以便您可以繼續執行此檢查清單中的剩餘工作。

步驟	任務	參考資料
1	查看如何在所有 AWS 資源中新增標籤。若要在 IAM 身分中心實作 ABAC，您必須先將標籤新增至您要實作 ABAC 的所有 AWS 資源。	• 標記 AWS 資源
2	檢閱如何在 IAM 身分識別中心中設定身分識別來源，以及身分識別存放區中關聯的使用者身分和屬性。IAM 身分中心可讓您使用任何 ABAC 受支援的 IAM 身分中心身分來源的使用者屬性。 AWS	• 管理身分識別來源
3	根據下列條件，決定您要使用哪些屬性做出存取控制決策， AWS 並將其傳送至 IAM 身分中心。	• 開始使用
	• 如果您使用外部身分識別提供者 (IdP)，請決定要使用從 IdP 傳遞的屬性，還是從 IAM 身分中心選取屬性。	• 使用外部身分識別提供者做為身分識別來源時選擇屬性
	• 如果您選擇讓 IdP 傳送屬性，請將 IdP 設定為在 SAML 宣告中傳輸屬性。請參閱教學課程中有關您特定 IdP 的`Optional`章節。	• 入門教學課程
	• 如果您使用 IdP 做為身分識別來源，並選擇在 IAM 身分中心選取屬性，請研究如何設定 SCIM，以便屬性值來自您的 IdP。如果您無法搭配 IdP 使用 SCIM，請使用 IAM 身分中心主控台使用者頁面新增使用者及其屬性。	• 自動佈建 • 支援的外部身分識別提供
	• 如果您使用 Active Directory 或 IAM 身分中心做為身分識別來源，或者您使用 IdP 並選擇在 IAM 身分中心選取屬性，請檢閱您可以設定的可用屬性。然後立	• 使用 IAM 身分中心做為身分識別來源時選擇屬性

步驟	任務	參考資料
	即跳至步驟 4，開始使用 IAM 身分中心主控台設定 ABAC 屬性。	• 當用 AWS Managed Microsoft AD 作身分識別來源時選擇屬性 • 預設對映
4	使用 IAM 身分中心主控台中的存取控制屬性頁面，選取要用於 ABAC 的屬性。從此頁面，您可以從您在步驟 2 中設定的身分識別來源選取存取控制的屬性。在您的身分及其屬性位於 IAM Identity Center 後，您必須建立鍵值配對 (對應)，這些對應會傳送給您 AWS 帳戶 ，以便在存取控制決策中使用。	• 啟用和設定存取控制的屬性
5	在您的權限集內建立自訂權限原則，並使用存取控制屬性建立 ABAC 規則，讓使用者只能存取具有相符標籤的資源。您在步驟 4 中配置的使用者屬性會作為存取控制決策 AWS 的標籤使用。您可以使用條件參照權限原則中的存取控制屬`aws:PrincipalTag/key` 性。	• 在 IAM 身分中心建立 ABAC 的許可政策
6	在您的各種情況下 AWS 帳戶，將使用者指派給您在步驟 5 中建立的權限集。這樣做可確保當他們聯合到其帳戶並訪問 AWS 資源時，他們只能根據匹配的標籤獲得訪問權限。	• 指派使用者存取權給 AWS 帳戶

完成這些步驟後，聯合到 AWS 帳戶 使用單一登入的使用者將可以根據相符屬性存取其 AWS 資源。

存取控制的屬性

存取控制的屬性是 IAM Identity Center 主控台中的頁面名稱，您可以在其中選取要在政策中使用的使用者屬性來控制資源的存取。您可以 AWS 根據使用者身分識別來源中的現有屬性，將使用者指派給中的工作負載。

例如，假設您要根據部門名稱將存取權指派給 S3 儲存貯體。在 [存取控制屬性] 頁面上，您可以選取 [部門] 使用者屬性，以搭配以屬性為基礎的存取控制 (ABAC) 使用。然後，在 IAM Identity Center 權限集中編寫一個政策，只有在部門屬性與您指派給 S3 儲存貯體的部門標籤相符時，才授與使用者存取權。IAM 身分中心會將使用者的部門屬性傳遞給要存取的帳戶。然後，會根據策略使用屬性來決定存取權限。如需 ABAC 的詳細資訊，請參閱屬性型存取控制。

開始使用

如何開始設定存取控制屬性取決於您使用的身分識別來源。無論您選擇的身分識別來源為何，在選取屬性之後，您都需要建立或編輯權限集原則。這些原則必須將 AWS 資源的存取權授與使用者身分。

使用 IAM 身分中心做為身分識別來源時選擇屬性

將 IAM 身分中心設定為身分識別來源時，首先要新增使用者並設定其屬性。接下來，瀏覽至存取控制的屬性頁面，然後選取您要在策略中使用的屬性。最後，瀏覽至AWS 帳戶頁面以建立或編輯權限集，以使用 ABAC 的屬性。

當用 AWS Managed Microsoft AD 作身分識別來源時選擇屬性

當您將 IAM 身分中心設定 AWS Managed Microsoft AD 為身分識別來源時，首先會將一組屬性從 Active Directory 對應到 IAM 身分識別中心中的使用者屬性。接下來，瀏覽至存取控制的屬性頁面。然後根據從使用中目錄對應的現有 SSO 屬性集，選擇要在 ABAC 組態中使用的屬性。最後，使用權限集中的存取控制屬性來編寫 ABAC 規則，將 AWS 資源的存取權授與使用者身分識別。如需 IAM Identity Center 中使用者屬性與 AWS Managed Microsoft AD 目錄中使用者屬性的預設對應清單，請參閱預設對映。

使用外部身分識別提供者做為身分識別來源時選擇屬性

當您以外部身分識別提供者 (IdP) 作為身分識別來源設定 IAM 身分識別中心時，有兩種方式可以使用 ABAC 的屬性。

- 您可以將 IdP 設定為透過 SAML 宣告傳送屬性。在這種情況下，IAM 身分中心會從 IdP 傳遞屬性名稱和值，以進行政策評估。

  > **Note**
  >
  > 您無法在 [存取控制屬性] 頁面上看到 SAML 宣告中的屬性。您必須事先知道這些屬性，並在編寫原則時將其新增至存取控制規則。如果您決定信任屬性 IdPs 的外部，那麼當使用者聯合到 AWS 帳戶時，這些屬性將一律傳遞給。在相同屬性透過 SAML 和 SCIM 傳送至 IAM 身分中心的案例中，SAML 屬性值在存取控制決策中優先。

- 您可以從 IAM 身分中心主控台的 [存取控制屬性] 頁面設定所使用的屬性。您在此選擇的屬性值會取代來自 IdP 透過宣告的任何相符屬性的值。視您是否使用 SCIM 而定，請考慮下列事項：
  - 如果使用 SCIM，IdP 會自動將屬性值同步到 IAM 身分中心。存取控制所需的其他屬性可能不會出現在 SCIM 屬性清單中。在這種情況下，請考慮與 IdP 中的 IT 管理員合作，以使用必要的前

綴透過 SAML 判斷提示將此類屬性傳送至 IAM 身分中心。`https://aws.amazon.com/SAML/Attributes/AccessControl:`如需如何在 IdP 中針對存取控制設定使用者屬性以透過 SAML 宣告傳送的相關資訊，請參閱 IdP 的入門教學課程。

- 如果您未使用 SCIM，則必須手動新增使用者並設定其屬性，就像使用 IAM 身分中心做為身分識別來源一樣。接下來，瀏覽至存取控制的屬性頁面，然後選擇您要在策略中使用的屬性。

如需 IAM Identity Center 中使用者屬性對外部使用者屬性所支援屬性的完整清單 IdPs，請參閱支援的外部身分識別提供。

若要在 IAM 身分中心開始使用 ABAC，請參閱下列主題。

主題

- 啟用和設定存取控制的屬性
- 在 IAM 身分中心建立 ABAC 的許可政策

啟用和設定存取控制的屬性

若要在所有情況下使用 ABAC，您必須先使用 IAM 身分中心主控台或 IAM 身分中心 API 啟用 ABAC。如果您選擇使用 IAM 身分中心選取屬性，請使用 IAM 身分中心主控台或 IAM 身分中心 API 中的存取控制屬性頁面。如果您使用外部身分識別提供者 (IdP) 做為身分識別來源，並選擇透過 SAML 宣告傳送屬性，則您可以將 IdP 設定為傳遞屬性。如果 SAML 宣告傳遞上述任何屬性，IAM Identity Center 會將屬性值取代為 IAM Identity Center 身分存放區中的值。當使用者聯合到其帳戶時，只有在 IAM 身分中心設定的屬性才會傳送，以便做出存取控制決策。

> **Note**
>
> 您無法從 IAM 身分中心主控台的 [存取控制屬性] 頁面檢視由外部 IdP 設定和傳送的屬性。如果您從外部 IdP 傳遞 SAML 宣告中的存取控制屬性，則這些屬性會直接傳送給使用者聯合 AWS 帳戶 時間。IAM 身分中心無法使用這些屬性進行對應。

啟用存取控制的屬性

使用下列程序，使用 IAM 身分中心主控台啟用存取 (ABAC) 控制功能的屬性。

> **Note**
>
> 如果您擁有現有的權限集，並且計劃在 IAM 身分中心執行個體中啟用 ABAC，則額外的安全限制要求您首先擁有該`iam:UpdateAssumeRolePolicy`政策。如果您的帳戶中沒有建立任何權限集，則不需要這些額外的安全性限制。

啟用存取控制的屬性

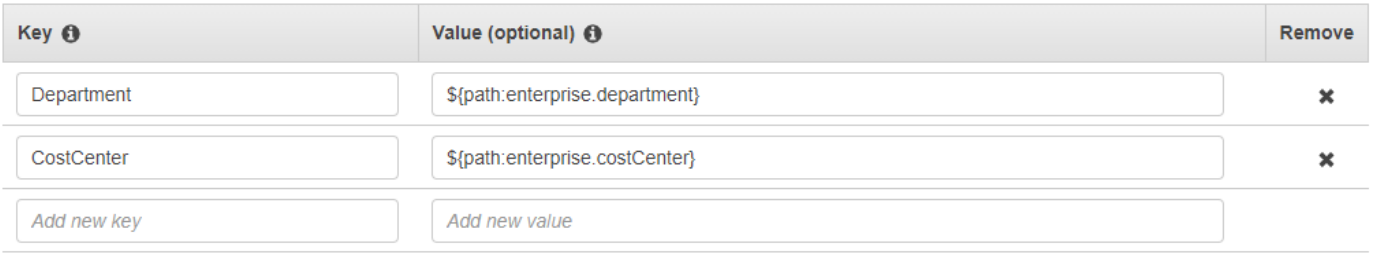
1. 開啟 IAM 身分中心主控台。
2. 選擇設定
3. 在 [設定] 頁面上，找出存取控制資訊的屬性] 方塊，然後選擇 [啟用]。繼續執行下一個程序以進行設定。

選取您的屬性

請使用下列程序來設定 ABAC 組態的屬性。

使用 IAM 身分中心主控台選取屬性

1. 開啟 IAM 身分中心主控台。
2. 選擇設定
3. 在 [設定] 頁面上，選擇 [存取控制的屬性] 索引標籤，然後選擇 [管理屬性]。
4. 在 [存取控制屬性] 頁面上，選擇 [新增屬性]，然後輸入 [機碼] 和 [值] 詳細資訊。您可以在這裡將來自身分識別來源的屬性對應至 IAM 身分中心作為工作階段標記傳遞的屬性。



Key 代表您指定給要在策略中使用之屬性的名稱。這可以是任意名稱，但您必須在為存取控制所撰寫的原則中指定該名稱。例如，假設您使用 Okta (外部 IdP) 做為身分識別來源，且需要將組織的成本中心資料作為工作階段標記傳遞。在 Key 中，您可以輸入類似的匹配名稱，CostCenter如您的密鑰名稱。重要的是要注意，無論您在這裡選擇哪個名稱，

它也必須在您的aws:PrincipalTag ####（即"ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"）中命名完全相同。

> **Note**
>
> 對您的金鑰使用單一值屬性，例如，**Manager**。IAM 身分中心不支援 ABAC 的多值屬性，例如。**Manager, IT Systems**

值代表來自您設定的身分識別來源的屬性內容。您可以在此輸入中所列之適當身分識別來源表格中的任何值AWS Managed Microsoft AD 目錄的屬性對應。例如，使用上述範例中提供的前後關聯，您可**${path:enterprise.costCenter}**以檢閱受支援的 IdP 屬性清單，並確定支援屬性的最接近相符項目，然後在「值」欄位中輸入該屬性。請參閱上面提供的屏幕截圖以供參考。請注意，除非您使用透過 SAML 判斷提示傳遞屬性的選項，否則您無法在此清單之外使用外部 IdP 屬性值。

5. 選擇儲存變更。

現在您已設定對應存取控制屬性，您必須完成 ABAC 組態程序。若要這麼做，請建立 ABAC 規則，並將其新增至您的權限集和/或以資源為基礎的原則。這是必要的，以便您可以將 AWS 資源的存取權授與使用者身分。如需詳細資訊，請參閱 在 IAM 身分中心建立 ABAC 的許可政策。

停止以屬性進行存取控制

使用下列程序來停用 ABAC 功能，並刪除所有已設定的屬性對應。

若要停用存取控制的屬性

1. 開啟 IAM 身分中心主控台。
2. 選擇設定
3. 在 [設定] 頁面上，選擇 [存取控制的屬性] 索引標籤，然後選擇 [停用]。
4. 在 [停用存取控制屬性] 對話方塊中，檢閱資訊，並在準備好時輸入 DELETE，然後選擇 [確認]。

> **Important**
>
> 此步驟會刪除所有已配置的屬性。刪除後，將不會傳遞從身份識別來源接收的任何屬性以及您先前配置的任何自訂屬性。

在 IAM 身分中心建立 ABAC 的許可政策

您可以建立權限原則，根據設定的屬性值決定誰可以存取您的 AWS 資源。當您啟用 ABAC 並指定屬性時，IAM 身分中心會將已驗證使用者的屬性值傳送至 IAM，以用於政策評估。

aws:PrincipalTag 條件金鑰

您可以使用`aws:PrincipalTag`條件索引鍵來建立存取控制規則，在權限集中使用存取控制屬性。例如，在下列信任原則中，您可以標記組織中的所有資源與各自的成本中心。您也可以使用單一權限集，授予開發人員存取其成本中心資源的權限。現在，每當開發人員使用單一登入及其成本中心屬性聯合到帳戶時，他們只能存取各自成本中心中的資源。隨著團隊在專案中增加了更多開發人員和資源，您只需要使用正確的成本中心標記資源即可。然後，您會在開發人員聯合到 AWS AWS 帳戶工作階段中傳遞成本中心資訊。因此，隨著組織將新資源和開發人員加入成本中心，開發人員可以管理與其成本中心相符的資源，而無需任何權限更新。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"
                }
            }
        }
    ]
}
```

如需詳細資訊，請參閱 IAM 使用者指南中的aws:PrincipalTag和 EC2：根據相符的主體和資源標籤啟動或停止執行個體。

如果策略在其條件中包含無效屬性，則策略條件將失敗，並拒絕存取。如需詳細資訊，請參閱 錯誤：當使用者嘗試使用外部身分識別提供者登入時，發生未預期的錯誤。

身分識別提供者

將單一登入存取權新增至 AWS 帳戶，IAM 身分中心會在每個項目中建立 IAM 身分提供者 AWS 帳戶。IAM 身分供應商可協助保 AWS 帳戶 護您的安全，因為您不必在應用程式中散發或內嵌長期安全登入資料，例如存取金鑰。

修復 IAM 身分識別提供者

如果您不小心刪除或修改了身分識別提供者，則必須手動重新套用使用者和群組指派。重新套用使用者和群組指派會重新建立身分識別提供者。如需詳細資訊，請參閱：

- 管理存取 AWS 帳戶
- 管理應用程式的存取

服務連結角色

服務連結角色是預先定義的 IAM 許可，可讓 IAM Identity Center 委派和強制執行哪些使用者對組織中特定的特定 AWS 帳戶 使用者具有單一登入存取權限。 AWS Organizations此服務會在其組織 AWS 帳戶 內的每個角色中佈建服務連結角色，藉此啟用此功能。然後，該服務允許其他 AWS 服務（例如 IAM 身份中心）利用這些角色執行與服務相關的任務。如需詳細資訊，請參閱AWS Organizations 和服務連結角色。

啟用 IAM 身分中心時，IAM 身分中心會在組織內的所有帳戶中建立服務連結角色。 AWS Organizations IAM 身分中心也會在隨後新增至組織的每個帳戶中建立相同的服務連結角色。此角色可讓 IAM 身分中心代表您存取每個帳戶的資源。如需詳細資訊，請參閱 管理存取 AWS 帳戶。

在每個角色中建立的服務連結角色 AWS 帳戶 都會命名為`AWSServiceRoleForSSO`。如需更多詳細資訊，請參閱 針對 IAM 身分中心使用服務連結角色。

管理應用程式的存取

使用 AWS IAM Identity Center，您可以控制誰可以對您的應用程式擁有單一登入存取權。使用者在使用其目錄認證登入後，即可順暢存取這些應用程式。

IAM 身分中心透過 IAM 身分中心與應用程式服務供應商之間的信任關係，安全地與這些應用程式通訊。視應用程式類型而定，可以使用不同的方式建立此信任。

IAM 身分中心支援兩種應用程式類型：AWS 受管應用程式和客戶受管應用程式 AWS 受管理的應用程式是直接從相關應用程式主控台內或透過應用程式 API 進行設定。客戶受管應用程式必須新增至 IAM 身分中心主控台，並為 IAM 身分中心和服務提供者設定適當的中繼資料。

將應用程式設定為與 IAM 身分中心搭配使用後，您可以管理哪些使用者或群組存取應用程式。依預設，不會將任何使用者指派給應用程式。

您也可以授與員工存取組織 AWS 帳戶 中特定項 AWS Management Console 目的存取權。如需詳細資訊，請參閱 管理存取 AWS 帳戶。

主題

AWS 受管理應用

AWS 受管理應用程式與 IAM 身分中心整合，可用於驗證和目錄服務。

將 AWS 受管應用程式與 IAM Identity Center 整合，可讓您輕鬆指派使用者存取權限，而無需為每個應用程式設定個別的聯合或使用者和群組同步。您可以連線一次想要用於驗證的身分識別來源，並收到使用者和群組指派的單一檢視。啟用受信任身分傳播的應用程式管理員能夠根據使用者或使用者的群組成員資格來定義和稽核其應用程式資源的存取權，而無需將其對應至 IAM 角色。

AWS 受管理的應用程式提供管理使用者介面，可讓您用來管理應用程式資源的存取。例如，QuickSight 管理員可以根據使用者的群組成員資格指派存取儀表板。大多數 AWS 受管理的應用程式也提供一種 AWS Management Console 體驗，可讓您將使用者指派給應用程式。這些應用程式的主控台體驗可能會整合這兩種功能，以便將使用者指派功能與管理應用程式資源存取權限相結合。

AWS 與 IAM 身分中心整合的受管理應用程式包括：

AWS 與 IAM 身分中心整合的受管理應用程式

AWS 受管理應用	與 IAM 身分中心的組織執行個體整合	與 IAM 身分中心的帳戶執行個體整合	透過 IAM 身分中心啟用受信任的身分傳播
Amazon Athena	 是	 是	 是
Amazon CodeCatalyst	 是	 是	 否
Amazon EMR 筆記本	 是	 否	 否
Amazon 在亞馬 Amazon EC2 上的 EMR	 是	 是	 是
Amazon EMR Studio	 是	 是	 是
Amazon Kendra	 是	 否	 否

AWS 受管理應用	與 IAM 身分中心的組織執行個體整合	與 IAM 身分中心的帳戶執行個體整合	透過 IAM 身分中心啟用受信任的身分傳播
Amazon Managed Grafana	 是	 否	 否
Amazon Monitron	 是	 否	 否
Amazon Nimble Studio	 是	 否	 否
Amazon Pinpoint	 是	 否	 否
Amazon Q Business	 是	 是	 否
Amazon Q 開發者	 是	 是 *	 否
Amazon QuickSight	 是	 是	 是
Amazon Redshift	 是	 是	 是

AWS 受管理應用	與 IAM 身分中心的組織執行個體整合	與 IAM 身分中心的帳戶執行個體整合	透過 IAM 身分中心啟用受信任的身分傳播
Amazon S3 訪問授權	 是	 是	 是
Amazon SageMaker 一室	 是	 否	 否
Amazon WorkSpaces 網站	 是	 否	 否
AWS CLI	 是	 否	 否
AWS Deadline Cloud	 是	 是	 否
AWS IoT Events	 是	 否	 否
AWS IoT Fleet Hub	 是	 否	 否
AWS IoT SiteWise	 是	 否	 否

AWS 受管理應用	與 IAM 身分中心的組織執行個體整合	與 IAM 身分中心的帳戶執行個體整合	透過 IAM 身分中心啟用受信任的身分傳播
AWS Lake Formation	 是	 是	 是
AWS Supply Chain	 是	 否	 否
AWS Systems Manager	 是	 否	 否
AWS Verified Access	 是	 否	 否

* 除非您的使用者需要在 AWS 主控台中存取 Amazon Q，否則支援 IAM 身分中心的帳戶執行個體。

主題

- 控制存取
- 協調管理工作
- 設定 IAM 身分中心以共用身分資訊
- 在中共用身分資訊的注意事項 AWS 帳戶
- 啟用識別感知主控台工作階段
- 限制 AWS 受管理應用程式的使用
- 檢視 AWS 管理應用程式的詳細資訊
- 停用 AWS 受管理應用程式

控制存取

AWS 受管理應用程式的存取控制方式有兩種：

- 應用程式的初始項目 — IAM 身分中心會透過指派給應用程式來管理這項工作。依預設， AWS 受管理的應用程式需要指派。
- 對應用程式資源的存取 — 應用程式會透過其控制的獨立資源指定來管理此資源。

協調管理工作

如果您是應用程式管理員，則可以選擇是否要求指派應用程式。如果需要指派，當使用者登入 AWS 存取入口網站時，只有直接或透過群組指派指派給應用程式的使用者才能檢視應用程式磚。或者，如果不需要指派，您可以允許所有 IAM 身分中心使用者進入應用程式。在此情況下，應用程式會管理資源的存取權，而且存取入口網站的所有使用者都可以看到應 AWS 用程式磚。

如果您是 IAM 身分中心管理員，則可以使用 IAM 身分中心主控台移除 AWS 受管應用程式的指派。移除指定之前，建議您先與應用程式管理員協調。如果您打算修改決定是否需要指派的設定，還是自動化應用程式指派，也應該與應用程式管理員協調。

設定 IAM 身分中心以共用身分資訊

IAM 身分識別中心提供包含使用者和群組屬性的身分識別存放區，但登入認證除外。您可以使用下列其中一種方法，讓 IAM 身分中心身分識別存放區中的使用者和群組保持更新：

- 使用 IAM 身分中心身分存放區做為主要身分識別來源。如果選擇此方法，則可以從 IAM 身分中心主控台或 AWS Command Line Interface (AWS CLI) 管理使用者、他們的登入認證和群組。如需詳細資訊，請參閱 在 IAM 身分中心管理身分識別。
- 針對來自下列任一身分識別來源的使用者和群組設定佈建 (同步處理) 至您的 IAM 身分識別中心身分存放區：
  - 作用中目錄 — 如需詳細資訊，請參閱Connect 至目Microsoft AD錄。
  - 外部身分識別提供者 — 如需詳細資訊，請參閱Connect 至外部身分識別提供者。

  如果選擇此佈建方法，則會繼續從身分識別來源中管理使用者和群組，而這些變更會同步至 IAM Identity Center 身分識別存放區。

無論您選擇哪種身分來源，IAM 身分中心都可以與 AWS 受管理的應用程式共用使用者和群組資訊。如此一來，您就可以將身分來源連線至 IAM 身分中心一次，然後與中的多個應用程式共用身分資訊 AWS

雲端。如此一來，就不需要針對每個應用程式獨立設定同盟和身分識別佈建。此共享功能還可以讓您的用戶輕鬆訪問許多不同的應用程序 AWS 帳戶。

在中共用身分資訊的注意事項 AWS 帳戶

IAM 身分中心支援跨應用程式最常用的屬性。這些屬性包括名字和姓氏、電話號碼、電子郵件地址、地址和慣用語言。仔細考慮哪些應用程序和哪些帳戶可以使用這些個人身份信息。

您可以使用下列其中一種方式來控制對此資訊的存取。您可以選擇僅在 AWS Organizations 管理帳戶或中的所有帳戶中啟用存取權 AWS Organizations。或者，您可以使用服務控制策略（SCP）來控制哪些應用程序可以訪問其中 AWS Organizations帳戶的信息。例如，如果您僅在 AWS Organizations 管理帳戶中啟用存取權，則成員帳戶中的應用程式將無法存取這些資訊。但是，如果您在所有帳戶中啟用存取權，則可以使用 SCP 來禁止所有應用程式存取，但您要允許的應用程式除外。

啟用識別感知主控台工作階段

主控台的身分識別感知工作階段會提供一些額外的使用者內容來個人化該使用者的體驗，藉此強化使用者的 AWS 主控台工作階段。 AWS 主控台中 Amazon Q 的使用者目前支援此功能。

您可以啟用身分識別感知主控台工作階段，而不必立即變更現有存取模式或聯合至 AWS 主控台。如果您的使用者透過 IAM 登入 AWS 主控台 (例如，如果他們以 IAM 使用者身分登入或透過 IAM 的聯合存取登入)，他們可以繼續使用這些方法。如果您的使用者登入 AWS 存取入口網站，他們可以繼續使用其 IAM 身分中心使用者登入資料。

主題

- 先決條件和考量事項
- 如何啟用 identity-aware-console 工作階段
- 身分識別感知主控台工作階段如何

先決條件和考量事項

啟用身分識別感知主控台工作階段之前，請檢閱下列先決條件和考量事項：

- 您必須為需要在主控台中存取 Amazon Q 的使用者啟用身分識別感知主控台工作階段。 AWS
- 身分識別感知主控台工作階段目前僅支援與主控台中的 Amazon Q 搭配使用。 AWS
- 身分識別感知主控台工作階段需要 IAM 身分中心的組織執行個體。
- 如果您在選擇加入 AWS 區域中啟用 IAM 身分中心，則不支援與 Amazon Q 整合。
- 啟用身分識別感知主控台工作階段後，就無法停用此功能。

- 若要啟用身分識別感知主控台工作階段，您必須具備下列權限：
  - `sso:CreateApplication`
  - `sso:GetSharedSsoConfiguration`
  - `sso:ListApplications`
  - `sso:PutApplicationAssignmentConfiguration`
  - `sso:PutApplicationAuthenticationMethod`
  - `sso:PutApplicationGrant`
  - `sso:PutApplicationAccessScope`
  - `signin:CreateTrustedIdentityPropagationApplicationForConsole`
  - `signin:ListTrustedIdentityPropagationApplicationForConsole`
  -
- 若要讓使用者能夠使用身分識別感知主控台工作階段，您必須在以身分識別為基礎的原則中授予他們`sts:setContext`權限。如需詳細資訊，請參閱授與使用者使用識別感知主控台工作階段的權限

如何啟用 identity-aware-console 工作階段

您可以在 Amazon Q 主控台或 IAM 身分中心主控台中啟用身分感知主控台工作階段。

在 Amazon Q 主控台中啟用身分識別感知主控台工作階段

啟用身分識別感知主控台工作階段之前，您必須擁有已連線身分識別來源的 IAM Identity Center 組織執行個體。如果您已設定 IAM 身分中心，請跳至步驟 3。

1. 開啟 IAM 身分中心主控台。選擇啟用，然後建立 IAM 身分中心的組織執行個體。如需相關資訊，請參閱啟用 AWS IAM Identity Center。
2. 將您的身分來源 Connect 到 IAM 身分中心，並將使用者佈建到 IAM 身分中心。您可以選擇預設的 IAM 身分中心目錄做為身分識別來源，也可以使用其他身分提供者。如需詳細資訊，請參閱 入門教學課程。
3. 完成 IAM 身分中心的設定後，請開啟 Amazon Q 主控台，並按照 Amazon Q 開發人員使用者指南中的訂閱中的步驟進行操作。請務必啟用身分識別感知主控台工作階段。

> **Note**
>
> 如果您沒有足夠的許可來啟用身分感知主控台工作階段，您可能需要請 IAM 身分中心管理員在 IAM Identity Center 主控台中為您執行此任務。如需詳細資訊，請參閱下一程序。

在 IAM 身分中心主控台中啟用身分感知主控台工作階段

如果您是 IAM 身分中心管理員，其他管理員可能會要求您在 IAM 身分中心主控台中啟用身分感知主控台工作階段。

1. 開啟 IAM 身分中心主控台。
2. 在導覽窗格中，選擇設定。
3. 在 [啟用識別感知工作階段] 下，選擇 [啟用]
4. 在第二個訊息中，選擇 [啟用]。
5. 啟用身分識別感知主控台工作階段後，「設定」頁面頂端會顯示確認訊息。
6. 在「詳細資訊」段落中，識別感知工作階段的狀態為「已啟用」。

身分識別感知主控台工作階段如何

透過身分感知主控台工作階段， AWS 主控台中 Amazon Q 的使用者可以登入 AWS、開啟 AWS Management Console 或其他 AWS 網站、選擇 Amazon Q 圖示，然後開始聊天或使用其他支援的功能。如需詳細資訊，請參閱 Amazon Q 開發人員使用者指南。

IAM 身分中心可增強使用者目前的主控台工作階段，以包含作用中的 IAM 身分中心使用者的 ID 和 IAM 身分中心工作階段 ID。

身分識別感知主控台工作階段包含下列三個值：

- 身分識別存放區使用者 ID (身份存儲：UserId)-此值可用來唯一識別身分識別身分來源中連線至 IAM 身分中心的使用者。
- 身分識別存放區目錄 ARN (身份存儲：IdentityStoreArn)-此值是連線至 IAM 身分識別中心的身分存放區的 ARN，您可以在其中查詢屬性。`identitystore:UserId`
- IAM 身分中心工作階段 ID-此值表示使用者的 IAM 身分中心工作階段是否仍然有效。

這些值是相同的，但是以不同的方式獲得，並在過程的不同點添加，具體取決於用戶登錄的方式：

- IAM 身分中心 (AWS 存取入口網站)：在此情況下，使用中的 IAM 身分中心工作階段中已提供使用者的身分存放區使用者 ID 和 ARN 值。IAM 身分中心透過僅新增工作階段 ID 來增強目前的工作階段。
- 其他登入方法：如果使用者以 AWS IAM 使用者、IAM 角色或使用 IAM 的聯合身分使用者身分登入，則不會提供這些值。IAM 身分中心透過新增身分識別存放區使用者 ID、身分存放區目錄 ARN 和工作階段 ID 來增強目前的工作階段。

限制 AWS 受管理應用程式的使用

首次啟用 IAM 身分中心時， AWS 允許在中的所有帳戶中自動使用 AWS 受管理的應用程式 AWS Organizations。若要限制應用程式，您必須實作 SCP。除了指定帳戶外，您可以使用 SCP 封鎖存取 IAM 身分中心使用者和群組資訊，並防止啟動應用程式。

檢視 AWS 管理應用程式的詳細資訊

使用應用程式的主控台或 API 將 AWS 受管應用程式連線至 IAM 身分中心後，該應用程式便會向 IAM 身分中心註冊。在 IAM 身分中心註冊應用程式後，您可以在 IAM 身分中心主控台中檢視有關該應用程式的詳細資訊。

在 IAM 身分中心主控台中檢視 AWS 受管應用程式的相關資訊

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 選擇AWS 受管理的應用程式標籤。
4. 在應用程式清單中，選擇您要檢視其詳細資訊的應用程式名稱。
5. 應用程式的相關資訊包括是否需要使用者和群組指派，以及指派的使用者和群組，以及識別傳播的信任應用程式 (如果適用)。如需有關受信任識別傳播的資訊，請參閱跨應用程式的可信身分傳播。

停用 AWS 受管理應用程式

若要防止使用者對 AWS 受管理應用程式進行驗證，您可以在 IAM Identity Center 主控台中停用該應用程式。

> **Warning**
>
> 停用應用程式會刪除此應用程式的所有使用者許可、中斷應用程式與 IAM Identity Center 的連線，並使應用程式無法存取。如果您是 IAM 身分中心管理員，建議您先與應用程式管理員協調，然後再執行此工作。

停用 AWS 受管理的應用程式

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。

3. 在 [應用程式] 頁面的 [受AWS 管理的應用程式] 下，選擇您要停用的應用程式。
4. 選取應用程式後，選擇 [動作]，然後選擇 [停用]。
5. 在 [暫停應用程式] 對話方塊中選擇 [暫停]。
6. 在AWS 受管理的應用程式清單中，應用程式狀態顯示為非作用中。

客戶管理的應用

透過 IAM 身分中心，您可以建立或連結員工使用者，並集中管理其所有使用者 AWS 帳戶 和應用程式的存取權限。IAM 身分中心充當中央身分識別服務，並為您的使用者提供不同的驗證方式。如果您已經使用身分識別提供者 (IdP)，IAM 身分中心可與您的 IdP 整合，以便您可以將使用者和群組佈建至 IAM 身分中心，並使用 IdP 進行驗證。

如果您使用支援 SAML 2.0 的客戶受管應用程式，您可以透過 SAML 2.0 將 IdP 聯合至 IAM 身分中心，並使用 IAM 身分中心來管理使用者對這些應用程式的存取權限。身分識別中心提供支援 SAML 2.0 的常用應用程式目錄，例如 Salesforce 和 Microsoft 365。此目錄可在 IAM 身分中心主控台取得。您也可以設定自己的 SAML 2.0 應用程式。

> **Note**
>
> 如果您有支援 OAuth 2.0 的客戶管理應用程式，而您的使用者需要從這些應用程式存取 AWS 服務，則可以使用受信任的身分傳播。透過受信任的身分傳播，使用者可以登入應用程式，而且該應用程式可以在要求中傳遞使用者身分，以存取 AWS 服務中的資料。如需詳細資訊，請參閱 將受信任的身分傳播與客戶管理的應用。

主題

- SAML 2.0 和 OAuth
- 設定客戶管理的 SAML 2.0 應用程式

SAML 2.0 和 OAuth

IAM 身分識別中心可讓您為使用者提供 SAML 2.0 或 OAuth 2.0 應用程式的單一登入存取權。下列主題提供 SAML 2.0 和 OAuth 2.0 的高階概觀。

主題

- SAML 2.0

- OAuth 2.0

SAML 2.0

SAML 2.0 是一種業界標準，用於安全地交換 SAML 判斷提示，該宣告會在 SAML 授權單位 (稱為身分識別提供者或 IdP) 和 SAML 2.0 取用者 (稱為服務提供者或 SP) 之間傳遞使用者相關資訊。IAM Identity Center 會使用此資訊，為獲授權在存取入口網站內使用應用程式的使用者提供聯合單一登入 AWS 存取權。

OAuth 2.0

OAuth 2.0 是一種協議，允許應用程序在不共享密碼的情況下安全地訪問和共享用戶數據。此功能為使用者提供安全且標準化的方式，允許應用程式存取其資源。不同的 OAuth 2.0 授予流程可促進訪問權限。

IAM Identity Center 可讓在公用用戶端上執行的應用程式擷取臨時登入資料，以便代表其使用者以程式設計方式存取 AWS 帳戶 和服務。公用用戶端通常是用來在本機執行應用程式的桌上型電腦、筆記型電腦或其他行動裝置。在公用用戶端上執行的 AWS 應用程式範例包括 AWS Command Line Interface (AWS CLI) 和 AWS 軟體開發套件 (SDK)。 AWS 工具組為了讓這些應用程式能夠取得登入資料，IAM 身分中心支援以下部分 OAuth 2.0 流程：

- 授權碼與證明密鑰進行代碼交換（RFC 6749 和 RFC 7636）
- 裝置授權授權 (RFC 8628)

> **Note**
>
> 這些授權類型只能在支援此功能的 AWS 服務 情況下使用。這些服務可能完全不支持此授權類型 AWS 區域。如需區域差異，請參 AWS 服務 閱相關文件。

OpenID Connect（OIDC）是一種基於 OAuth 2.0 框架的身份驗證協議。OIDC 會指定如何使用 OAuth 2.0 進行驗證。透過 IAM 身分中心 OIDC 服務 API，應用程式會註冊 OAuth 2.0 用戶端，並使用其中一個流程取得存取權杖，以便為受 IAM 身分識別中心保護的 API 提供許可。應用程序指定訪問範圍以聲明其預期的 API 用戶。身為 IAM Identity Center 管理員設定身分識別來源之後，您的應用程式最終使用者必須完成登入程序 (如果他們尚未完成登入程序)。接著，您的使用者必須同意才能允許應用程式進行 API 呼叫。這些 API 呼叫是使用使用者的權限進行的。作為回應，IAM 身分中心會將存取權杖傳回至包含使用者同意的存取範圍的應用程式。

使用 OAuth 2.0 授予流程

OAuth 2.0 授予流程只能透過支援流程的 AWS 受管理應用程式使用。若要使用 OAuth 2.0 流程，您的 IAM 身分中心執行個體和您使用的任何 AWS 受支援的受管理應用程式必須部署在單 AWS 區域一執行個體中。請參閱每個文件的說明文件， AWS 服務 以判斷 AWS 受管應用程式的區域可用性，以及您要使用的 IAM 身分中心執行個體。

若要使用使用 OAuth 2.0 流程的應用程式，最終使用者必須輸入應用程式將在其中連線的 URL，並向您的 IAM 身分中心執行個體註冊。視應用程式而定，身為管理員，您必須為使用者提供 IAM 身分中心執行個體的AWS 存取入口網站 URL 或發行者 URL。您可以在 IAM 身分中心主控台設定頁面上找到這兩個設定。如需有關設定用戶端應用程式的其他資訊，請參閱該應用程式的文件。

登入應用程式並提供同意的使用者體驗取決於應用程式是否使用使用 PKCE 授予授權碼或裝置授權。

使用 PKCE 授予授權碼

在具有瀏覽器的裝置上執行的應用程式會使用此流程。

1. 瀏覽器視窗隨即開啟。
2. 如果用戶尚未通過身份驗證，瀏覽器將其重定向到完成用戶身份驗證。
3. 驗證後，使用者會看到同意畫面，其中顯示下列資訊：
   - 應用程式的名稱
   - 應用程式要求同意使用的存取範圍
4. 用戶可以取消同意過程，也可以給予同意，應用程序會根據用戶的權限繼續訪問。

裝置授權

在具有或不使用瀏覽器的設備上運行的應用程序都可以使用此流程。當應用程式啟動流程時，應用程式會顯示 URL 和使用者程式碼，使用者稍後必須在流程中進行驗證。使用者程式碼是必要的，因為起始流程的應用程式可能在與使用者提供同意的裝置上執行的裝置不同。該代碼可確保用戶同意他們在另一台設備上啟動的流程。

1. 當流程從具有瀏覽器的裝置啟動時，會開啟瀏覽器視窗。當流程從沒有瀏覽器的裝置啟動時，使用者必須在其他裝置上開啟瀏覽器，並前往應用程式顯示的 URL。
2. 在任何一種情況下，如果用戶尚未通過身份驗證，瀏覽器將其重定向到完成用戶身份驗證。
3. 驗證後，使用者會看到同意畫面，其中顯示下列資訊：
   - 應用程式的名稱
   - 應用程式要求同意使用的存取範圍

- 應用程式呈現給使用者的使用者程式碼

4. 用戶可以取消同意過程，也可以給予同意，應用程序會根據用戶的權限繼續訪問。

存取範圍

範圍定義了可透過 OAuth 2.0 流程存取之服務的服務存取權。範圍是服務（也稱為資源服務器）的一種方式，用於對與操作和服務資源相關的權限進行分組，並且它們指定了 OAuth 2.0 客戶端可以請求的粗粒度操作。當 OAuth 2.0 用戶端向 IAM 身分中心 OIDC 服務註冊時，用戶端會指定要宣告其預期動作的範圍，使用者必須為其提供同意。

OAuth 2.0 客戶端使用 OAuth 2.0（RFC 6749）第 3.3 節中定義的`scope`值來指定要請求訪問令牌的權限。客戶端在請求訪問令牌時最多可以指定 25 個範圍。當使用者透過 PKCE 授予授權碼或裝置授權授予流程期間提供同意時，IAM Identity Center 會將範圍編碼為其傳回的存取權杖。

AWS 將範圍新增至 IAM 身分中心以獲得支援 AWS 服務。下表列出 IAM 身分中心 OIDC 服務在註冊公用用戶端時支援的範圍。

註冊公用用戶端時，IAM 身分中心 OIDC 服務支援的存取範圍

範圍	描述	支援的服務
`sso:account:access`	存取 IAM 身分中心受管帳戶和權限集。	IAM Identity Center
`codewhisperer:analysis`	啟用 Amazon Q 開發人員程式碼分析的存取權。	AWS 建構家 ID 和 IAM 身分識別中心
`codewhisperer:completions`	啟用對 Amazon Q 內嵌程式碼建議的存取。	AWS 建構家 ID 和 IAM 身分識別中心
`codewhisperer:conversations`	啟用對 Amazon Q 聊天的存取權。	AWS 建構家 ID 和 IAM 身分識別中心
`codewhisperer:taskassist`	啟用 Amazon Q 開發人員代理程式的存取以進行軟體開發。	AWS 建構家 ID 和 IAM 身分識別中心

範圍	描述	支援的服務
codewhisperer:transformations	啟用 Amazon Q 開發人員代理程式的存取以進行程式碼轉換	AWS 建構家 ID 和 IAM 身分識別中心
codecatalyst:read_write	讀取和寫入您的 Amazon CodeCatalyst 資源，允許存取所有現有資源。	AWS 建構家 ID 和 IAM 身分識別中心

設定客戶管理的 SAML 2.0 應用程式

如果您使用支援 SAML 2.0 的客戶受管應用程式，您可以透過 SAML 2.0 將 IdP 聯合至 IAM 身分中心，並使用 IAM 身分中心來管理使用者對這些應用程式的存取權限。您可以從 IAM 身分中心主控台的常用應用程式目錄中選取 SAML 2.0 應用程式，也可以設定自己的 SAML 2.0 應用程式。

> **Note**
>
> 如果您有支援 OAuth 2.0 的客戶管理應用程式，而您的使用者需要從這些應用程式存取 AWS 服務，則可以使用受信任的身分傳播。透過受信任的身分傳播，使用者可以登入應用程式，而且該應用程式可以在要求中傳遞使用者身分，以存取 AWS 服務中的資料。如需詳細資訊，請參閱 將受信任的身分傳播與客戶管理的應用。

主題

- IAM 身分中心應用程式目錄
- 設定您自己的 SAML 2.0 應用程式

IAM 身分中心應用程式目錄

您可以使用 IAM 身分中心主控台中的應用程式目錄來新增許多與 IAM 身分中心搭配使用的常用 SAML 2.0 應用程式。例子包括銷售力量，盒子和 Microsoft 365。

大多數應用程式都提供有關如何在 IAM 身分中心和應用程式服務提供者之間設定信任的詳細資訊。在目錄中選取應用程式之後，您可以在應用程式的組態頁面中找到此資訊。設定應用程式後，您可以視需要將存取權指派給 IAM 身分中心中的使用者或群組。

主題

- 從應用程式類別目錄設定應用程式

從應用程式類別目錄設定應用程式

使用此程序，在 IAM 身分中心和應用程式的服務提供者之間設定 SAML 2.0 信任關係。

在開始此程序之前，先取得服務提供者的中繼資料交換檔案，以便更有效率地設定信任。如果你沒有這個文件，你仍然可以使用這個過程來手動配置信任它。

從應用程式類別目錄新增及設定應用程式

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 選擇「客戶管理」標籤。
4. 選擇新增應用程式。
5. 在 [選取應用程式類型] 頁面的 [設定] 偏好設定下，選擇 [我要從目錄中選取應用程式]。
6. 在 [應用程式類別目錄] 下，開始在搜尋方塊中輸入您要新增的應用程式名稱。
7. 當應用程式出現在搜尋結果中時，請從清單中選擇該應用程式的名稱，然後選擇 [下一步]。
8. 在 [設定應用程式] 頁面上，[顯示名稱] 和 [說明] 欄位會預先填入應用程式的相關詳細資訊。您可以編輯此資訊。
9. 在 IAM 身分中心中繼資料下，執行下列動作：

    a. 在 IAM 身分中心 SAML 中繼資料檔案下，選擇 [下載] 以下載身分識別提供者中繼資料。

    b. 在 [IAM 身分中心憑證] 下方，選擇 [下載憑證] 以下載身分提供者憑證。

    > **Note**
    >
    > 稍後當您從服務供應商的網站設定應用程式時，您將需要這些檔案。請遵循該供應商的說明執行。

10. (選擇性) 在應用程式屬性下，您可以指定應用程式啟動 URL、轉送狀態和工作階段持續時間。如需詳細資訊，請參閱 在 IAM 身分中心主控台中設定應用程式屬性。
11. 在應用程式中繼資料下，執行下列其中一個動作

    a. 如果您有中繼資料檔案，請選擇「上傳應用程式 SAML 中繼資料檔案」。然後，選擇選擇要查找的文件並選擇元數據文件。

b. 如果您沒有中繼資料檔案，請選擇「手動輸入中繼資料值」，然後提供「應用程式 ACS URL」和「應用程式 SAML」對象值。

12. 選擇提交。您將被帶到剛剛添加的應用程序的詳細信息頁面。

設定您自己的 SAML 2.0 應用程式

您可以設定自己的應用程式，以允許使用 SAML 2.0 聯合身分識別，並將其新增至 IAM 身分中心。設定您自己的 SAML 2.0 應用程式的大部分步驟都與從 IAM 身分中心主控台的應用程式目錄設定 SAML 2.0 應用程式相同。不過，您也必須為自己的 SAML 2.0 應用程式提供其他 SAML 屬性對應。這些對應可讓 IAM 身分中心為您的應用程式正確填入 SAML 2.0 宣告。首次設定應用程式時，您可以提供此額外的 SAML 屬性對應。您也可以在 IAM 身分中心主控台的應用程式詳細資料頁面上提供 SAML 2.0 屬性對應。

使用下列程序，在 IAM 身分中心和 SAML 2.0 應用程式的服務提供者之間設定 SAML 2.0 信任關係。開始此程序前，請確定您具有服務供應商的憑證和中繼資料交換檔案，以便完成信任的設定。

若要設定您自己的 SAML 2.0 應用程式

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 選擇「客戶管理」標籤。
4. 選擇新增應用程式。
5. 在 [選取應用程式類型] 頁面的 [設定] 偏好設定下，選擇 [我有要設定的應用程式]。
6. 在「應用程式類型」下，選擇「SAML 2.0」。
7. 選擇下一步。
8. 在 [設定應用程式] 頁面的 [設定應用程式] 下，輸入應用程式的顯示名稱，例如**MyApp**。然後，輸入「描述」。
9. 在 IAM 身分中心中繼資料下，執行下列動作：

   a. 在 IAM 身分中心 SAML 中繼資料檔案下，選擇 [下載] 以下載身分識別提供者中繼資料。

   b. 在 [IAM 身分中心憑證] 下方，選擇 [下載] 以下載身分提供者憑證。

> **Note**
>
> 稍後在您從服務供應商的網站設定自訂應用程式時，將需要這些檔案。

10. (選擇性) 在應用程式屬性下，您也可以指定應用程式啟動 URL、轉送狀態和工作階段持續時間。如需詳細資訊，請參閱 在 IAM 身分中心主控台中設定應用程式屬性。
11. 在 [應用程式中繼資料] 下方，選擇 [手動輸入您的 然後，提供「應用程式 ACS URL」和「應用程式 SAML」對象值。
12. 選擇提交。您將被帶到剛剛添加的應用程序的詳細信息頁面。

跨應用程式的可信身分傳播

信任的身分識別傳播可讓 AWS 服務執行下列動作：

- 根據使用者的身分內容授權對 AWS 資源的存取權。
- 與其他 AWS 服務安全地共享用戶的身份上下文。

這些功能可讓使用者更輕鬆地定義、授與和記錄存取。

透過受信任的身分傳播，使用者可以登入應用程式，而且該應用程式可以在存取 AWS 服務中資料的要求中傳遞使用者的身分內容。由於是根據使用者的身分管理存取權限，使用者無需使用資料庫本機使用者憑證，也無需擔任 IAM 角色，便可存取資料。

主題

- 信任的身分傳播概觀
- 信任的身分傳播使用案例
- 設定信任的身分傳播
- 搭配受信任的權杖發行者使用應用

信任的身分傳播概觀

透過受信任的身分傳播，可以更輕鬆地定義、授與及記錄使用者對 AWS 資源的存取。受信任的身份傳播建立在 OAuth 2.0 授權框架上，該框架允許應用程序在不共享密碼的情況下安全地訪問和共享用戶數據。OAuth 2.0 提供對應用程式資源的安全委派存取。由於資源管理員核准或委派使用者登入的應用程式以存取其他應用程式，所以會委派存取權。

為了避免共享用戶密碼，受信任的身份傳播使用令牌。令牌為受信任的應用程序提供了一種標準方法，以聲明用戶是誰以及兩個應用程序之間允許哪些請求。 AWS 與受信任身分傳播整合的受管理應用程式會直接從 IAM 身分中心取得權杖。IAM 身分中心還為應用程序提供了一個選項，用於交換來自外部

OAuth 2.0 授權服務器的身份令牌和訪問令牌。這使得應用程序可以在外部進行身份驗證和獲取令牌 AWS，將令牌交換為 IAM 身份中心令牌，並使用新令牌向 AWS 服務發出請求。如需詳細資訊，請參閱 搭配受信任的權杖發行者使用應用。

OAuth 2.0 程序會在使用者登入應用程式時啟動。使用者登入以啟動要求以存取其他應用程式資源的應用程式。啟動（請求）應用程序可以通過從授權服務器請求令牌來代表用戶訪問接收應用程序。授權服務器返回令牌，並且啟動的應用程序將該令牌（帶有訪問請求）傳遞給接收應用程序。

信任的身分傳播使用案例

身為 IAM Identity Center 管理員，系統可能會要求您在支援此功能和連線 AWS 服務的下列啟動應用程式之間協助設定受信任的身分傳播。下列各節提供有關可啟動信任識別傳播之應用程式所支援之特定使用案例的詳細資訊。

主題

- Amazon EMR
- Amazon QuickSight
- Amazon Redshift 查詢編輯器第 2 版
- 第三方商業智慧應用
- 定制開發的應用

Amazon EMR

您可以使用 Amazon EMR 做為下列受信任身分傳播使用案例的起始應用程式。

描述	使用的其他 AWS 服務	進一步了解
透過 Amazon EMR 工作室，在亞馬 Amazon EC2 叢集上使用 Apache Spark 執行互動式分析。根據員工身分識別和關聯屬性套用存取控制，以供 AWS Glue 目錄至使用 AWS Lake Formation。	Amazon EC2 上的亞馬遜 EMR 通過 AWS Lake Formation Amazon S3 訪問授權，Amazon S3， AWS Service Catalog	• 在 Amazon EMR 管理指南中將 Amazon EMR 與 IAM 身分中心整合。 • Amazon S3 存取授權和公司目錄身分，請參閱 Amazon 簡單儲存服務使用者指南。 • 在AWS Lake Formation 開發人員指南中AWS Lake Formation 與 IAM 身分中心連線

描述	使用的其他 AWS 服務	進一步了解
	Note • 需要通過 Amazon EMR 工作室訪問。 • 僅限資料表層級存取控制。 • 不支援阿帕奇蜂巢、普雷斯托 SQL / TRINO 和 EMR 無伺服器。	• 透過AWS 大數據部落格中的 Amazon EMR 和 IAM 身分中心，使用您的公司身分進行分析
透過 Amazon EMR 工作室，在 Athena 上與 Trino 一起執行臨時分析。根據員工身分識別和關聯屬性套用存取控制，以供 AWS Glue 目錄至使用 AWS Lake Formation 。使用 Amazon S3 存取授權，在 Amazon S3 中安全存取 Athena 查詢結果儲存貯體位置。	Athena 透過 AWS Lake Formation Amazon S3 存取授權授權 **Note** 需要通過 Amazon EMR 工作室訪問。不支援從主 Amazon Athena 控台直接存取。	• 在 Amazon EMR 管理指南中將 Amazon EMR 與 IAM 身分中心整合。 • Amazon Athena 使用者指南中的使用 IAM 身分中心啟用了雅典娜工作群組。 • Amazon S3 存取授權和公司目錄身分，請參閱 Amazon 簡單儲存服務使用者指南。 • 在AWS Lake Formation 開發人員指南中 AWS Lake Formation 與 IAM 身分中心連線。 • 在AWS 大數據部落格中，將您的員工身分帶到 Amazon EMR 工作室和 Athena。

Amazon QuickSight

您可以使用 Amazon QuickSight 做為下列受信任身分傳播使用案例的起始應用程式。

描述	使用的其他 AWS 服務	進一步了解
Amazon QuickSight 用戶可以查詢 Amazon Redshift 數據。資料存取權由亞 Amazon Redshift 管理員授予。	Amazon Redshift	• 將 Redshift 與身分識別中心連線，在 Amazon Redshift 管理指南中為使用者提供單一登入體驗。 • QuickSight在 Amazon Redshift 管理指南中，透過 Amazon 將亞馬 Amazon Redshift 與 IAM 身分中心 Connect。
亞馬遜 QuickSight 使用者可以透過 AWS Lake Formation 管理員授權的存取權，在 Amazon S3 中查詢結構化資料的 Amazon Redshift Spectrum。	Amazon Redshift Spectrum，Amazon S3 結構化數據 * 通過 Amazon Redshift Spectrum 授權 AWS Lake Formation	• 將 Redshift 與身分識別中心連線，在 Amazon Redshift 管理指南中為使用者提供單一登入體驗。 • QuickSight在 Amazon Redshift 管理指南中，透過 Amazon 將亞馬 Amazon Redshift 與 IAM 身分中心 Connect。 • 在AWS Lake Formation 開發人員指南中 AWS Lake Formation 與 IAM 身分中心連線。 • 使用 Amazon Redshift 和AWS 大數據部落格中 AWS Lake Formation 的外部身分識別供應商中的使用者來簡化存取管理。
亞馬遜 QuickSight 使用者可以使用管理員授權的存取權，在 Amazon S3 中查詢結構化資料的 Amazon Redshift 資料存取權。AWS Lake Formation	Amazon Redshift 數據庫，Amazon S3 結構化數據	• QuickSight在 Amazon Redshift 管理指南中，透過 Amazon 將亞馬 Amazon Redshift 與 IAM 身分中心 Connect。

描述	使用的其他 AWS 服務	進一步了解
	* 通過 Amazon Redshift 授權 AWS Lake Formation	• 在AWS Lake Formation 開發人員指南中 AWS Lake Formation 與 IAM 身分中心連線。 • 使用 Amazon Redshift 和AWS 大數據部落格中 AWS Lake Formation 的外部身分識別供應商中的使用者來簡化存取管理。

Amazon Redshift 查詢編輯器第 2 版

您可以使用 Amazon Redshift 查詢編輯器 v2 做為下列受信任身分傳播使用案例的起始應用程式。

描述	使用的其他 AWS 服務	進一步了解
Amazon Redshift 查詢編輯器 v2 用戶可以查詢 Amazon Redshift 數據。資料存取權由亞 Amazon Redshift 管理員授予。	Amazon Redshift	• 將 Redshift 與身分識別中心連線，在 Amazon Redshift 管理指南中為使用者提供單一登入體驗。 • 在 Amazon Redshift 管理指南中 Connect 到 Amazon Redshift 數據庫。 • Okta與 Amazon Redshift 查詢編輯器 V2 整 AWS IAM Identity Center 合，在AWS 大數據部落格中使用順暢的單一登入。
Amazon Redshift 查詢編輯器 v2 使用者可以使用管理員授權的存取權，在 Amazon S3 中查詢結構化資料的 Amazon Amazon Redshift Spectrum 外部表格。 AWS Lake Formation	Amazon Redshift Spectrum，Amazon S3 結構化數據 * 通過 Amazon Redshift Spectrum 授權 AWS Lake Formation	• 將 Redshift 與身分識別中心連線，在 Amazon Redshift 管理指南中為使用者提供單一登入體驗。 • 在 Amazon Redshift 管理指南中 Connect 到 Amazon Redshift 數據庫。

描述	使用的其他 AWS 服務	進一步了解
		• 在AWS Lake Formation 開發人員指南中 AWS Lake Formation 與 IAM 身分中心連線。
亞馬遜 Redshift 查詢編輯器 v2 使用者可以使用管理員授權的存取權來查詢 Amazon Redshift 資料庫。 AWS Lake Formation	Amazon Redshift 數據庫， AWS Lake Formation	• 在 Amazon Redshift 管理指南中 Connect 到 Amazon Redshift 數據庫。 • 在AWS Lake Formation 開發人員指南中 AWS Lake Formation 與 IAM 身分中心連線。

第三方商業智慧應用

您可以使用第三方商業智慧應用程式 (例如 Tableau) 做為特定受信任身分傳播使用案例的起始應用程式。修改後的第三方商業智慧應用程式可以透過 OAuth 身分權杖或存取權杖，將 Amazon Redshift 驅動程式傳遞給使用者的身分，以使用 Amazon Redshift 管理員授權的存取權來查詢 Amazon Redshift 中的資料。

定制開發的應用

您可以使用自己的自訂開發應用程式作為下列受信任身分傳播使用案例的起始應用程式。

描述	使用的其他 AWS 服務	進一步了解
建立透過 OAuth 授權伺服器驗證使用者的應用程式，然後使用 AWS IAM Identity Center 和 IAM 取得身分增強的 IAM 角色登入資料。此登入資料用於請求存取 Amazon S3 中的非結構化資料，以及由 Amazon S3 存取授權管理員授權的存取權。	AWS IAM Identity Center、Amazon S3 非結構化資料 * 透過 Amazon S3 存取授權授權	• Amazon S3 存取授權和公司目錄身分，請參閱 Amazon 簡單儲存服務使用者指南。 • 如何透過AWS 儲存部落格中的 IAM 身分中心和 Amazon S3 存取授權 (第 1 部分) 和 (第 2 部分) 開發面向使用者的資料應用程式。
建置可與 Amazon Q Business 互動的自訂應用程式，以根據您自己	Amazon Q 業務中心 IAM 身分識別中心	• 在 Amazon Q 商務使用者指南中啟用和設定 IAM 身分中心執行個體。

描述	使用的其他 AWS 服務	進一步了解
的內容和使用者的許可回應使用者問題。		• 如何搭配 IAM 身分中心使用 AWS 受管應用程式：啟用 Amazon Q，而不必遷移AWS 安全部落格中的現有 IAM 聯合流程。

設定信任的身分傳播

受信任的身分傳播支援應用程式進行驗證的不同方式，以便將使用者的身分傳遞給 AWS 服務。受信任身分傳播的設定會根據應用程式類型及其驗證方式而有所不同。

> **Note**
>
> 如果您的客戶管理應用程式要求存取受管理的應用程式，但不使用 AWS API 進行連線，則必須設定 AWS 受信任的 Token 簽發者。

主題

- 先決條件和考量事項
- 搭配受管理的應用程式使用 AWS 受信任
- 將受信任的身分傳播與客戶管理的應用

先決條件和考量事項

在設定信任的識別傳播之前，請先檢閱下列先決條件和考量事項。

主題

- 必要條件
- 其他考量

必要條件

若要使用受信任的識別傳播，請確定您的環境符合下列先決條件。

- 已佈建使用者和群組的 IAM 身分識別中心部署

  若要使用受信任的身分傳播，您必須啟用 IAM 身分中心並佈建使用者和群組。如需相關資訊，請參閱開始使用 IAM 身分中心的常見任務。

  建議使用組織執行個體 — 建議您使用在組織管理帳戶中啟用的 IAM 身分中心的組 Organ AWS izations 執行個體。如果您計劃使用受信任的身分傳播，讓使用者能夠存取同一組織 AWS 帳戶 內不同的 AWS 服務和相關資源，則可以將 IAM Identity Center 執行個體的管理委派給成員帳戶。

  如果您打算使用 IAM Identity Center 的單一帳戶執行個體，您希望使用者透過受信任身分傳播存取的所有 AWS服務和資源，都必須位於同一個獨立帳戶 AWS 帳戶，或位於您啟用 IAM 身分中心的組織中的相同成員帳戶中。如需詳細資訊，請參閱 IAM 身分中心的帳戶執行個體。
- 適用於 AWS 受管理應用程式；連線至 IAM 身分中心

  若要使用受信任的身分傳播， AWS 受管理應用程式必須與 IAM 身分中心整合。

其他考量

請記住下列使用受信任識別傳播的其他考量。

- 請勿修改 AWS 受管理應用程式的 [需要指派] 設定

  AWS 受管理的應用程式具有預設設定組態，可決定使用者和群組是否需要指派。建議您不要修改此設定。即使您已設定允許使用者存取特定資源的精細權限，修改 [需要指派] 設定也可能會導致非預期的行為，包括中斷使用者對這些資源的存取。
- 不需要多帳戶權限（權限集）

  受信任的身分識別傳播不需要您設定多帳戶權限 (權限集)。您可以啟用 IAM 身分中心，並僅將其用於受信任的身分傳播。

搭配受管理的應用程式使用 AWS 受信任

受信任的身分識別傳播可讓 AWS 受管理的應用程式代表使用者要求存取 AWS 服務中的資料。資料存取管理是以使用者的身分為基礎，因此管理員可以根據使用者現有的使用者和群組成員資格授與存取權。使用者的身分、代表他們執行的動作以及其他事件都會記錄在服務特定記錄檔和 CloudTrail事件中。

受信任的身分傳播是以 OAuth 2.0 標準為基礎。若要使用此功能， AWS 受管理的應用程式必須與 IAM 身分中心整合。 AWS 分析服務可能會提供以驅動程式為基礎的介面，讓相容的應用程式使用受信任的

身分 例如，JDBC、ODBC 和 Python 驅動程式可讓相容的查詢工具使用受信任的身分傳播，而不需要您完成其他設定步驟。

主題

- 設定 AWS 受信任身分傳播的受管理應用程式
- AWS 受管理應用程式的信任身分傳播要求流
- 應用程序獲得令牌後
- 身分增強型 IAM 角色工作階段
- 身分增強型 IAM 角色工作階段的類型
- 設定 AWS 受管理應用程式的程序和要求流程

設定 AWS 受信任身分傳播的受管理應用程式

AWS 支援受信任身分傳播的服務提供管理使用者介面和 API，您可以使用這些介面來設定此功能。這些服務不需要在 IAM 身分中心內進行設定。

以下是設定受信任識別傳播 AWS 服務的高階程序。具體步驟會根據應用程式提供的管理介面和 API 而有所不同。

1. 使用應用程式主控台或 API 將應用程式連線到 IAM 身分中心的執行個體

   使用受 AWS 管應用程式或應用程式 API 的主控台，將應用程式連接到 IAM 身分中心的執行個體。當您針對應用程式使用主控台時，系統管理使用者介面會包含可簡化設定和連線程序的 Widget。

2. 使用應用程式主控台或 API 來設定使用者對應用程式資源的存取權

   完成此步驟即可授權使用者可存取的資源或資料。存取權是根據使用者的身分識別或群組成員資格而定。授權模式會根據應用程式而有所不同。

> **Important**
>
> 您必須完成此步驟，才能讓使用者存取 AWS 服務的資源。否則，使用者無法存取資源，即使要求的應用程式已獲授權要求存取服務。

AWS 受管理應用程式的信任身分傳播要求流

對受管理應用程式的所有 AWS 受信任身分傳播流程都必須從從 IAM Identity Center 取得 Token 的應用程式開始。此 Token 是必要的，因為它包含 IAM 身分中心已知的使用者參考，以及在 IAM 身分中心註冊的應用程式。

下列各節說明受 AWS 管理應用程式可從 IAM Identity Center 取得權杖以啟動受信任身分傳播的方式。

主題

基於 Web 的 IAM 身分中心身份驗證

針對此流程， AWS 受管應用程式會使用 IAM 身分中心進行身份驗證，提供 Web 式單一登入體驗。

當使用者開啟 AWS 受管理的應用程式時，會觸發使用 IAM 身分中心的單一登入流程。如果 IAM Identity Center 中沒有使用中的使用者工作階段，則會根據您指定的身分識別來源向使用者顯示登入頁面，而 IAM 身分中心會為該使用者建立工作階段。

IAM Identity Center 為受 AWS 管理的應用程式提供一個 Token，其中包括使用者的身分，以及應用程式註冊使用的對象 (Auds) 清單和相關範圍。然後，應用程序可以使用令牌向其他接收 AWS 服務發出請求。

以主控台為基礎的使用者啟動的驗證要求

對於此流程， AWS 受管理的應用程式會提供使用者啟動的主控台體驗。

在此情況下， AWS 受管理的應用程式會在擔任角色後從 AWS 管理主控台輸入。若要讓應用程式取得權杖，使用者必須啟動程序，以觸發應用程式來驗證使用者。這會使用 IAM 身分中心啟動身分驗證，這會將使用者重新導向至您已設定的身分識別來源。

應用程序獲得令牌後

請求的應用程式從 IAM Identity Center 取得權杖後，應用程式會定期重新整理權杖，該權杖可用於使用者工作階段的生命週期。在此期間，應用程式可能會：

- 取得有關 Token 的詳細資訊，以判斷使用者是誰，以及應用程式可與其他受 AWS 管理的應用程式搭配使用的範圍。
- 將呼叫中的 Token 傳遞給其他支援使用權杖的受 AWS 管理應用程式。

- 取得身分增強的 IAM 角色工作階段，這些工作階段可用來向使用 AWS 簽名版本 4 的其他 AWS 受管理應用程式發出請求。

  身分增強的 IAM 角色會話是 IAM 角色會話，其中包含存儲在 IAM 身份中心創建的令牌中的用戶的傳播身份。

身分增強型 IAM 角色工作階段

AWS Security Token Service 可讓應用程式取得身分增強的 IAM 角色工作階段。 AWS 在角色工作階段中支援使用者前後關聯的受管理應用程式可以根據角色工作階段中的使用者，使用識別資訊來授權存取權。這個新內容可讓應用程式透過 AWS 簽章版本 4 API 要求，向支援 AWS 受信任身分傳播的受管理應用程式發出要求。

當 AWS 受管理應用程式使用身分增強的 IAM 角色工作階段存取資源時，請 CloudTrail 記錄使用者的身分識別 (User ID)、起始工作階段以及採取的動作。

當應用程式使用身分增強的 IAM 角色工作階段向接收應用程式發出請求時，會將內容新增至工作階段，以便接收應用程式可以根據使用者的身分識別或群組成員資格或 IAM 角色授權存取權限。如果接收應用程式或要求的資源未設定為根據使用者的身分識別或群組成員資格授權存取，則接收支援受信任身分識別傳播的應用程式將會傳回錯誤訊息。

若要避免此問題，請執行下列任一項作業：

- 確認接收應用程式已連線至 IAM 身分中心。
- 使用接收應用程式的主控台或應用程式 API 來設定應用程式，以根據使用者的身分識別或群組成員資格授權資源存取權。此設定需求會因應用程式而有所不同。

如需詳細資訊，請參閱接收 AWS 受管理應用程式的文件。

身分增強型 IAM 角色工作階段的類型

應用程式透過向 AWS STS `AssumeRole` API 發出請求，並在請求的`ProvidedContexts`參數中傳遞上下文宣告，以取得身分增強的 IAM 角色工作階段。`AssumeRole`上下文斷言是從`SSO OIDC` `CreateTokenWithIAM`請求響應中可用的`idToken`聲明中獲得的。

AWS STS 可以建立兩種不同類型的身分增強 IAM 角色工作階段，具體取決於提供給請求的內容宣告：`AssumeRole`

- 只記錄使用者身分的工作階段 CloudTrail。
- 根據傳播的使用者身分識別啟用授權並將其記錄到 CloudTrail的工作階段。

若要從僅提供 CloudTrail 追蹤中註冊 AWS STS 的稽核資訊取得身分增強型 IAM 角色工作階段，請提供要`sts:audit_context`求的宣告值。`AssumeRole`若要取得也允許接收 AWS 服務授權 IAM Identity Center 使用者執行動作的工作階段，請向`AssumeRole`請求提供`sts:identity_context`宣告的值。您只能提供一個前後關聯。

使用建立的身分增強型 IAM 角色工作階段 **`sts:audit_context`**

當使用建立的身分增強型 IAM 角色工作階段向 AWS 服務提出請求時`sts:audit_context`，使用者的 IAM 身分中心`userId`會記錄到元素 CloudTrail 中。`OnBehalfOf`

```
"userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLE:MyRole",
      "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
      "accountId": "111111111111",
      "accessKeyId": "ASIAEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAEXAMPLE",
            "arn": "arn:aws:iam::111111111111:role/MyRole",
            "accountId": "111111111111",
            "userName": "MyRole"
        },
        "attributes": {
            "creationDate": "2023-12-12T13:55:22Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "11111111-1111-1111-1111-1111111111",
        "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/
d-111111111"
    }
}
```

> **Note**
>
> 這些工作階段無法用於授權身分識別中心使用者。它們仍然可用於授權 IAM 角色。

若要從中取得此類型的角色工作階段 AWS STS，AssumeRole請在要求參數中提供sts:audit_context欄位的值給ProvidedContexts要求。用arn:aws:iam::aws:contextProvider/IdentityStore作的值ProviderArn。

使用建立的身分增強型 IAM 角色工作階段 **sts:identity_context**

當使用者使用建立的身分增強型 IAM 角色工作階段向 AWS 服務提出要求時sts:identity_context，使用者的 IAM Identity Center userId 會以與使用建立 CloudTrail 的工作階段相同的方式登入該onBehalfOf元素。sts:audit_context

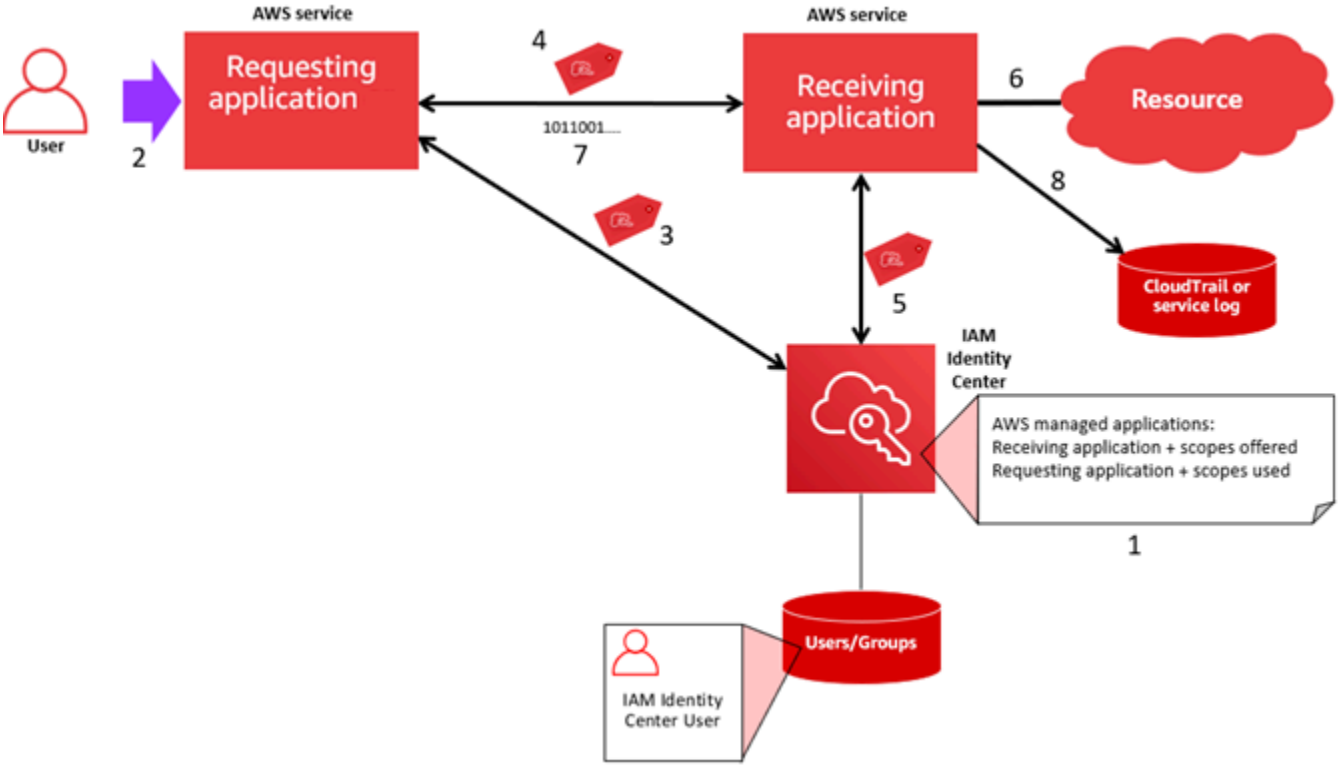
除了將 IAM 身分中心使用者記錄userId到 CloudTrail，支援的 API 也會使用此類型的工作階段，根據傳播的使用者身分來授權動作。如需支援 API 的 IAM 動作清單，請參閱受AWSIAMIdentityCenterAllowListForIdentityContext AWS 管政策。使用建立身分增強型 IAM 角色工作階段時，此 AWS 受管政策會作為工作階段政策提供。sts:identity_context此原則會阻止您將角色工作階段與不支援的 AWS 服務搭配使用。

若要從中取得此類型的角色工作階段 AWS STS，AssumeRole請在要求參數中提供sts:identity_context欄位的值給ProvidedContexts要求。用arn:aws:iam::aws:contextProvider/IdentityStore作的值ProviderArn。

設定 AWS 受管理應用程式的程序和要求流程

本節說明使用受信任識別傳播並提供 Web 式單一登入體驗之 AWS 受管理應用程式的設定程序和要求流程。

下圖提供此程序的概觀。



下列步驟提供有關此程序的其他資訊。

1. 使用受 AWS 管理應用程式或應用程式 API 的主控台執行下列作業：
   a. 將應用程式 Connect 到 IAM 身分中心的執行個體。
   b. 設定權限以授權使用者可存取的應用程式資源。
2. 當使用者開啟可要求存取資源 (要求的應用程式) 的 AWS 受管理應用程式時，要求流程便會開始。
3. 若要取得權杖以存取接收 AWS 受管理應用程式，請求的 AWS 受管理應用程式會啟動 IAM Identity Center 的登入請求。

   如果使用者未登入，IAM 身分中心會觸發使用者身分驗證流程至您指定的身分識別來源。這會為使用者建立新的 AWS 存取入口網站工作階段，其持續時間為您在 IAM 身分中心設定。然後 IAM Identity Center 會產生與工作階段相關聯的權杖，應用程式可在使用者 AWS 存取入口網站工作階段的剩餘持續時間內運作。如果使用者登出其應用程式，或者您刪除其工作階段，工作階段會在兩小時內自動結束。
4. AWS 受管理的應用程式會向接收應用程式啟動要求，並提供其 Token。
5. 接收應用程式會呼叫 IAM 身分中心，以取得使用者的身分，以及在權杖中編碼的範圍。接收應用程式也可能會提出要求，以從 Identity Center 目錄取得使用者屬性或使用者的群組成員資格。
6. 接收應用程式會使用其授權組態來判斷使用者是否有權存取要求的應用程式資源。

7. 如果使用者有權存取要求的應用程式資源，則接收應用程式會回應要求。
8. 使用者的身分、代表他們執行的動作，以及接收應用程式記錄檔和事件中記錄的其他 AWS CloudTrail 事件。記錄此資訊的特定方式會根據應用程式而有所不同。

將受信任的身分傳播與客戶管理的應用

受信任的身分傳播可讓客戶受管理的應用程式代表使用者要求存取 AWS 服務中的資料。資料存取管理是以使用者的身分為基礎，因此管理員可以根據使用者現有的使用者和群組成員資格授與存取權。使用者的身分、代表他們執行的動作以及其他事件都會記錄在服務特定記錄檔和 CloudTrail事件中。

透過受信任的身分傳播，使用者可以登入客戶管理的應用程式，而且該應用程式可以在要求中傳遞使用者的身分識別，以存取 AWS 服務中的資料。

> **Important**
>
> 若要存取 AWS 服務，客戶受管理的應用程式必須從受信任的 Token 簽發者 (IAM Identity Center 外部) 取得權杖。受信任的令牌發行者是創建簽名令牌的 OAuth 2.0 授權服務器。這些權杖會授權啟動存取 AWS 服務 (接收應用程式) 要求的應用程式。如需詳細資訊，請參閱 搭配受信任的權杖發行者使用應用。

主題

- 設定用於受信任身分傳播的客戶管理 OAuth 2.0 應用程式
- 指定信任的應用

設定用於受信任身分傳播的客戶管理 OAuth 2.0 應用程式

若要設定用於受信任身分傳播的客戶受管 OAuth 2.0 應用程式，您必須先將其新增至 IAM 身分中心。請使用下列程序將您的應用程式新增至 IAM 身分中心。

主題

- 步驟 1：選擇申請類型
- 步驟 2：指定申請詳細資料
- 步驟 3：指定驗證設定
- 步驟 4：指定應用程式認證
- 步驟 5：檢閱和設定

步驟 1：選擇申請類型

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 選擇「客戶管理」標籤。
4. 選擇新增應用程式。
5. 在 [選取應用程式類型] 頁面的 [設定] 偏好設定下，選擇 [我有要設定的應用程式]。
6. 在應用程式類型下，選擇 OAuth 2.0。
7. 選擇「下一步」以繼續下一頁步驟 2：指定申請詳細資料。

步驟 2：指定申請詳細資料

1. 在 [指定應用程式詳細資訊] 頁面的 [應用程式名稱和說明] 下，輸入應用程式的顯示名稱，例如**MyApp**。然後，輸入「描述」。
2. 在 [使用者和群組指派方法] 下，選擇下列其中一個選項：
   - 需要指派 — 僅允許指派給此應用程式的 IAM 身分中心使用者和群組存取應用程式。

     應用程式磚可見度 — 只有直接指派給應用程式或透過群組指派指派給應用程式的使用者才能在存取入口網站中檢視應用程式磚，前提是 AWS 存取入口網站中 AWS 的應用程式可見度設定為可見。
   - 不需要指派 — 允許所有經過授權的 IAM 身分中心使用者和群組存取此應用程式。

     應用程式磚可見性 — 除非 AWS 存取入口網站中的應用程式可見度設定為 [不可見]，否則所有登入 AWS 存取入口網站的使用者都可以看見應用程式磚。
3. 在 [AWS 存取入口網站] 下，輸入使用者可以存取應用程式的 URL，並指定應用程式磚在 AWS 存取入口網站中是否可見。如果您選擇 [不可見]，即使沒有指派的使用者也可以檢視應用程式磚。
4. 在「標籤 (選用)」下，選擇「新增標籤」，然後指定「機碼與值」(選用) 的值。

   如需標籤的相關資訊，請參閱標記 AWS IAM Identity Center 資源。
5. 選擇「下一步」，然後前往下一頁步驟 3：指定驗證設定。

步驟 3：指定驗證設定

若要將支援 OAuth 2.0 的客戶受管應用程式新增至 IAM 身分中心，您必須指定受信任的權杖發行者。受信任的令牌發行者是創建簽名令牌的 OAuth 2.0 授權服務器。這些權杖會授權啟動要求 (要求應用程式) 存取 AWS 受管理應用程式 (接收應用程式) 的應用程式。

1. 在 [指定驗證設定] 頁面的 [受信任的權杖發行者] 下，執行下列任一項作業：

   - 若要使用現有的受信任權杖簽發者：

     選取您要使用之受信任 Token 發行者名稱旁邊的核取方塊。

   - 若要新增受信任的權杖簽發者：

     1. 選擇建立信任的權杖發行者。
     2. 新的瀏覽器標籤隨即開啟。請遵循中的步驟 5 到 8 如何將受信任的權杖發行者新增至 IAM 身分中心主控台。
     3. 完成這些步驟後，請返回您用於應用程式設定的瀏覽器視窗，並選取您剛剛新增的受信任 Token 簽發者。
     4. 在受信任的權杖發行者清單中，選取您剛新增之受信任權杖發行者名稱旁的核取方塊。

     選取受信任的權杖簽發者之後，會顯示 [設定選取的受信任憑證發行者] 區段。

2. 在設定選取的受信任權杖發行者下，輸入 Ad 宣告。Ad 聲明可識別受信任令牌發行者生成的令牌的預定對象（收件人）。如需詳細資訊，請參閱 澳元索賠。
3. 若要避免使用者在使用此應用程式時必須重新驗證，請選取 [自動重新整理作用中應用程式工作階段的使用者驗證]。選取時，此選項會每 60 分鐘重新整理工作階段的存取權杖，直到工作階段過期或使用者結束工作階段為止。
4. 選擇「下一步」，然後前往下一頁步驟 4：指定應用程式認證。

步驟 4：指定應用程式認證

完成此程序中的步驟，以指定應用程式用來與信任的應用程式執行 Token 交換動作的認證。這些認證用於以資源為基礎的策略中。此原則需要您指定具有執行原則中指定動作之權限的主參與者。即使受信任的應用程式位於相同的應用程式中，您也必須指定主體 AWS 帳戶。

> **Note**
>
> 使用原則設定權限時，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。

此原則需要sso-oauth:CreateTokenWithIAM採取動作。

1. 在「指定應用程式證明資料」頁面上，執行下列任一項作業：

   - 若要快速指定一或多個 IAM 角色：
     1. 選擇 [輸入一或多個 IAM 角色]。
     2. 在「輸入 IAM 角色」下，指定現有 IAM 角色的 Amazon 資源名稱 (ARN)。若要指定 ARN，請使用下列語法。ARN 的區域部分是空白的，因為 IAM 資源是全域。

        ```
        arn:aws:iam::account:role/role-name-with-path
        ```

        如需詳細資訊，請參閱使用資源型政策的跨帳戶存取和使用者指AWS Identity and Access Management 南中的 IAM ARN。
   - 若要手動編輯原則 (如果您指定非AWS 認證，則需要)：
     1. 選取編輯應用程式原則。
     2. 在 JSON 文字方塊中輸入或貼上文字，以修改您的政策。
     3. 解決政策驗證期間產生的任何安全性警告、錯誤或一般警告。如需詳細資訊，請參閱AWS Identity and Access Management 使用指南中的驗證 IAM 政策。
2. 選擇「下一步」，然後前往下一頁步驟 5：檢閱和設定。

步驟 5：檢閱和設定

1. 在「檢閱並設定」頁面上，檢閱您所做的選擇。若要進行變更，請選擇您要的組態區段，選擇 [編輯]，然後進行必要的變更。
2. 完成後，選擇 [新增應用程式]。
3. 您新增的應用程式會顯示在客戶管理的應用程式清單中。
4. 在 IAM Identity Center 中設定客戶受管應用程式後，您必須為身分傳播指定一或多個 AWS 服務或受信任的應用程式。這可讓使用者登入您的客戶管理應用程式，並存取受信任應用程式中的資料。

   如需詳細資訊，請參閱 指定信任的應用 。

指定信任的應用

設定客戶管理的應用程式之後，您必須指定一或多個受信任的 AWS 服務或受信任的應用程式，以進行身分傳播。指定包含客戶管理應用程式使用者需要存取的資料的 AWS 服務。當您的使用者登入您的客戶管理應用程式時，該應用程式會將您的使用者身分傳遞給受信任的應用程式。

使用下列程序來選取服務，然後指定要信任該服務的個別應用程式。

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 選擇「客戶管理」標籤。
4. 在客戶受管應用程式清單中，選取您要啟動存取要求的 OAuth 2.0 應用程式。這是您的使用者登入的應用程式。
5. 在 [詳細資料] 頁面的 [識別傳播信任的應用程式] 下，選擇 [指定信任的應用
6. 在 [設定類型] 下，選取 [個別應用程式] 並指定存取權，然後選擇 [下一
7. 在 [選取服務] 頁面上，選擇具有客戶管理的應用程式可信任的應用程式以進行識別傳輸的 AWS 服務，然後選擇 [下一步]。

   您選取的服務會定義可信任的應用程式。您將在下一步中選擇應用程序。
8. 在 [選取應用程式] 頁面上，選擇 [個別應用程式]，針對每個可接收存取要求的應用程式選取核取方塊，然後選擇 [下一步]。
9. 在 [設定存取權] 頁面的 [組態方法] 下，執行下列任一項作業：

   - 選取每個應用程式的存取權 — 選取此選項可為每個應用程式設定不同的存取層級 選擇您要設定其存取層級的應用程式，然後選擇 [編輯存取權限]。在要套用的存取層級中，視需要變更存取層級，然後選擇 [儲存變更]。
   - 對所有應用程式套用相同層級的存取權限 — 如果您不需要針對每個應用程式設定存取層級，請選取此選項。
10. 選擇下一步。
11. 在 [檢閱組態] 頁面上，檢閱您所做的選擇。若要進行變更，請選擇您想要的組態區段，選擇 [編輯存取權]，然後進行必要的變更。
12. 完成後，選擇 [信任應用程式]。

搭配受信任的權杖發行者使用應用

受信任的 Token 發行者可讓您將受信任的身分傳播用於在外部進行驗證的 AWS應用程式。透過受信任的 Token 發行者，您可以授權這些應用程式代表其使用者提出要求，以存取 AWS 受管理的應用程式。

下列主題說明受信任權杖發行者的運作方式，並提供設定指引。

主題

受信任的權杖發行者

受信任的身分傳播提供了一種機制，可讓在外部進行驗證的 AWS 應用程式，以代表其使用者提出要求，並使用受信任的 Token 簽發者。受信任的令牌發行者是創建簽名令牌的 OAuth 2.0 授權服務器。這些權杖會授權啟動要求 (要求應用程式) 存取 AWS 服務 (接收應用程式) 的應用程式。要求應用程式會代表受信任 Token 簽發者驗證的使用者起始存取要求。受信任的令牌發行者和 IAM 身份中心都知道用戶。

AWS 接收要求的服務會根據 Identity Center 目錄中所示的使用者和群組成員資格來管理其資源的精細授權。 AWS 服務不能直接使用外部令牌發行者的令牌。

為了解決這個問題，IAM Identity Center 為請求的應用程式或要求應用程式使用的 AWS 驅動程式提供了一種方法，將受信任的權杖發行者發行的權杖交換為 IAM Identity Center 產生的權杖。IAM 身分中心產生的權杖是指對應的 IAM 身分中心使用者。請求的應用程序或驅動程序使用新令牌來啟動對接收應用程序的請求。由於新權杖會參考 IAM Identity Center 中對應的使用者，因此接收應用程式可以根據 IAM 身分中心中所表示的使用者或其群組成員資格來授權要求的存取。

> **Important**
>
> 選擇要新增為受信任權杖簽發者的 OAuth 2.0 授權伺服器是一項安全性決策，需要仔細考量。請只選擇您信任的受信任 Token 發行者，才能執行下列工作：
>
> - 驗證在權杖中指定的使用者。
> - 授權該使用者存取接收應用程式。
> - 產生權杖，讓 IAM 身分中心可以交換 IAM 身分中心建立的權杖。

受信任的權杖發行者的先決條件和考量

在設定受信任的權杖發行者之前，請先檢閱下列先決條件和考量事項。

- 受信任的權杖發行者

  您必須配置 OAuth 2.0 授權服務器（受信任的令牌發行者）。雖然受信任的權杖發行者通常是您用來做為 IAM 身分識別中心身分來源的身分識別提供者，但不一定要這樣做。如需如何設定受信任 Token 簽發者的詳細資訊，請參閱相關身分識別提供者的說明文件。

  > **Note**
  >
  > 只要將受信任權杖發行者中的每個使用者的身分對應至 IAM 身分中心中的對應使用者，您最多可以設定 10 個受信任的權杖發行者，以便與 IAM 身分中心搭配使用。

- 建立權杖的 OAuth 2.0 授權伺服器 (受信任的權杖發行者) 必須具有 OpenID Connect (OIDC) 探索端點，IAM 身分中心可用來取得公開金鑰以驗證權杖簽章。如需詳細資訊，請參閱 OIDC 探索端點網址 (發行者 URL)。
- 由受信任的令牌發行者發行的令牌

  來自受信任的令牌發行者的令牌必須滿足以下要求：

  - 該令牌必須使用 RS256 算法簽名並以 JSON 網絡令牌（JWT）格式進行簽名。
  - 令牌必須包含以下聲明：
    - 發行者（iss）— 發行令牌的實體。此值必須與受信任憑證簽發者的 OIDC 探索端點 (發行者 URL) 中設定的值相符。
    - 主旨 (sub) — 已驗證的使用者。
    - 聽眾（AUD）— 令牌的預期接收者。這是將權杖交換成 IAM 身分中心的權杖之後存取的 AWS 服務。如需詳細資訊，請參閱 澳元索賠。
    - 到期時間 (exp) — 權杖到期之後的時間。
    -
  - 令牌可以是身份令牌或訪問令牌。
  - 權杖必須具有可唯一對應至一個 IAM 身分中心使用者的屬性。
- 選擇性索償

  IAM 身分中心支援 RFC 7523 中定義的所有選擇性宣告。如需詳細資訊，請參閱第 3 節：此 RFC 的 JWT 格式和處理要求。

  例如，權杖可以包含 JTI (JWT ID) 宣告。如果存在，此聲明可防止具有相同 JTI 的令牌被重用於令牌交換。如需有關 JTI 宣告的詳細資訊，請參閱金唐國際索償詳情。
- IAM 身分中心組態可與受信任的權杖發行者搭配使用

您也必須啟用 IAM 身分中心、設定 IAM 身分識別中心的身分來源，以及佈建與受信任權杖簽發者目錄中的使用者對應的使用者。

若要這麼做，您必須執行下列其中一項作業：

- 使用跨網域身分識別管理 (SCIM) 2.0 通訊協定的系統，將使用者同步至 IAM 身分中心。
- 直接在 IAM 身分中心建立使用者。

> **Note**
>
> 如果您使用 Active Directory 網域服務做為身分識別來源，則不支援受信任的權杖發行者。

金唐國際索償詳情

如果 IAM 身分中心收到要求交換 IAM 身分中心已交換的權杖，則請求會失敗。為了檢測並防止令牌交換中重複使用令牌，您可以包含 JTI 聲明。IAM 身份中心根據令牌中的聲明防止令牌重播。

並非所有 OAuth 2.0 授權服務器都會向令牌添加 JTI 聲明。某些 OAuth 2.0 授權伺服器可能不允許您將 JTI 新增為自訂宣告。支援使用 JTI 宣告的 OAuth 2.0 授權伺服器可能會將此宣告新增至僅識別權杖、僅限存取權杖，或兩者皆新增。如需詳細資訊，請參閱 OAuth 2.0 授權伺服器的文件。

如需建置交換權杖之應用程式的相關資訊，請參閱 IAM 身分中心 API 文件。如需設定客戶管理應用程式以取得和交換正確 Token 的相關資訊，請參閱應用程式的文件。

受信任的權杖發行者組態

下列各節說明設定和使用受信任權杖簽發者所需的設定。

主題

- OIDC 探索端點網址 (發行者 URL)
- 屬性對應
- 澳元索賠

OIDC 探索端點網址 (發行者 URL)

將受信任的權杖簽發者新增至 IAM 身分中心主控台時，必須指定 OIDC 探索端點 URL。此 URL 通常由其相對 URL 引用`/.well-known/openid-configuration`。在 IAM 身分中心主控台中，此 URL 稱為簽發者 URL。

> **Note**
>
> 您必須將探索端點的 URL 貼上直到和不貼上`.well-known/openid-configuration`。如果包含`.well-known/openid-configuration`在 URL 中，則受信任的令牌發行者配置將無法正常工作。由於 IAM 身分中心不會驗證此 URL，因此如果 URL 格式不正確，受信任的權杖發行者設定將會失敗，恕不另行通知。

IAM 身分中心使用此 URL 取得有關受信任權杖發行者的其他資訊。例如，IAM 身分中心會使用此 URL 取得驗證受信任權杖發行者所產生之權杖所需的資訊。將受信任的權杖簽發者新增至 IAM 身分中心時，必須指定此 URL。要查找 URL，請參閱用於為應用程序生成令牌的 OAuth 2.0 授權服務器提供程序的文檔，或直接聯繫提供商以獲取幫助。

屬性對應

屬性對應可讓 IAM 身分中心將受信任權杖發行者所發行之權杖中表示的使用者與 IAM 身分中心中的單一使用者進行比對。將受信任的權杖簽發者新增至 IAM 身分中心時，必須指定屬性對應。此屬性對應會用於受信任憑證簽發者所產生之權杖中的宣告中。宣告中的值用於搜尋 IAM 身分中心。搜尋會使用指定的屬性來擷取 IAM 身分中心中的單一使用者，該使用者將在其中做為使用者使用 AWS。您選擇的宣告必須對應至 IAM 身分識別中心身分識別存放區中可用屬性的固定清單中的一個屬性。您可以選擇下列其中一個 IAM 身分識別中心身分存放區屬性：使用者名稱、電子郵件和外部 ID。您在 IAM 身分中心中指定的屬性值對於每個使用者而言都必須是唯一的。

澳元索賠

aud 聲明標識了旨在使用令牌的對象（收件人）。當請求存取的應用程式透過未與 IAM Identity Center 聯合的身分提供者進行驗證時，必須將該身分識別提供者設定為受信任的權杖發行者。接收存取要求的應用程式 (接收應用程式) 必須將受信任的權杖發行者所產生的權杖交換為 IAM Identity Center 所產生的權杖。

有關如何在受信任的令牌發行者中註冊時獲取接收應用程序的 aud 聲明值的詳細信息，請參閱受信任的令牌發行者的文檔或聯繫受信任的令牌發行者管理員以獲取幫助。

設定受信任的權杖發行者

若要針對在 IAM Identity Center 進行外部驗證的應用程式啟用受信任身分傳播，必須一或多個管理員設定受信任的權杖發行者。受信任的令牌發行者是 OAuth 2.0 授權服務器，它向發起請求（請求應用程序）的應用程序發出令牌。權杖會授權這些應用程式代表其使用者對接收應用程式（AWS 服務) 發出要求。

主題

協調管理角色和職責

在某些情況下，單一系統管理員可能會執行設定受信任 Token 簽發者的所有必要工作。如果有多個管理員執行這些工作，則需要密切協調。下表說明多個系統管理員如何協調設定受信任的 Token 簽發者，並將 AWS 服務設定為使用它。

> **Note**
>
> 該應用程式可以是與 IAM 身分中心整合的任何 AWS 服務，並支援受信任的身分傳播。

如需詳細資訊，請參閱 設定受信任權杖簽發者的工作。

角色	執行這些工作	與坐標
IAM 身分中心管理員	將外部 IdP 做為受信任的權杖發行者新增至 IAM 身分中心主控台。 協助在 IAM 身分中心與外部 IdP 之間設定正確的屬性對應。 將受信任的權杖發行者新增至 IAM 身分中心主控台時通知 AWS 服務管理員。	外部 IdP（受信任的令牌發行者）管理員 AWS 服務管理員
外部 IdP（受信任的令牌發行者）管理員	設定外部 IdP 以發行權杖。 協助在 IAM 身分中心與外部 IdP 之間設定正確的屬性對應。	IAM 身分中心管理員 AWS 服務管理員

角色	執行這些工作	與坐標
	提供對象名稱 (Ad 宣告) 給 AWS 服務管理員。	
AWS 服務管理員	檢查 AWS 服務主控台是否有受信任的 Token 簽發者。IAM 身分中心管理員將受信任的權杖發行者新增至 IAM 身分中心主控台後，便會顯示在 AWS 服務主控台中。 將 AWS 服務設定為使用受信任的權杖簽發者。	IAM 身分中心管理員 外部 IdP（受信任的令牌發行者）管理員

設定受信任權杖簽發者的工作

若要設定受信任的權杖發行者，IAM Identity Center 管理員、外部 IdP (受信任的權杖發行者) 管理員和應用程式管理員必須完成下列工作。

> **Note**
>
> 該應用程式可以是與 IAM 身分中心整合的任何 AWS 服務，並支援受信任的身分傳播。

1. 將受信任的權杖簽發者新增至 IAM 身分中心 — IAM 身分中心管理員使用 IAM 身分中心主控台或 API 新增受信任的權杖發行者。此配置需要指定以下內容：
   - 受信任權杖發行者的名稱
   - OIDC 探索端點 URL (在 IAM 身分中心主控台中，此 URL 稱為簽發者 URL)。
   - 使用者查詢的屬性對應。此屬性對應會用於受信任憑證簽發者所產生之權杖中的宣告中。宣告中的值用於搜尋 IAM 身分中心。搜尋會使用指定的屬性擷取 IAM 身分中心中的單一使用者。
2. 將 AWS 服務 Connect 至 IAM 身分中心 — AWS 服務管理員必須使用應用程式的主控台或應用程式 API，將應用程式連線至 IAM 身分中心。

   將受信任的權杖發行者新增至 IAM Identity Center 主控台後，也會在 AWS 服務主控台中看到該憑證，並可供 AWS 服務管理員選取。

3. 配置令牌交換的使用 — 在 AWS 服務控制台中，服務管理員將 AWS 服務配 AWS 置為接受受信任的令牌發行者發行的令牌。這些令牌交換為 IAM 身份中心生成的令牌。這需要從步驟 1 指定受信任的令牌發行者的名稱，以及與 AWS 服務相對應的 Od 聲明值。

   受信任的令牌發行者將 Ad 聲明值放在其發行的令牌中，以指示該令牌旨在供 AWS 服務使用。若要取得此值，請連絡受信任 Token 簽發者的系統管理員。

如何將受信任的權杖發行者新增至 IAM 身分中心主控台

在具有多個管理員的組織中，此工作由 IAM 身分中心管理員執行。如果您是 IAM 身分中心管理員，則必須選擇要使用哪個外部 IdP 作為受信任的權杖發行者。

將受信任的權杖發行者新增至 IAM 身分中心主控台

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上，選擇 [驗證] 索引標籤。
4. 在 [信任的權杖發行者] 底下，選擇 [建立受信任的權杖
5. 在 [設定外部 IdP 以發行受信任的權杖] 頁面上，在 [受信任的權杖簽發者詳細資料] 下，執行下列動作：

   - 對於發行者 URL，請指定外部 IdP 的 OIDC 探索 URL，該 URL 將為受信任的身分傳播發行權杖。您必須指定探索端點的 URL，直到和不指定為止`.well-known/openid-configuration`。外部 IdP 的管理員可以提供此 URL。

     > **Note**
     >
     > 注意此 URL 必須符合為受信任身分傳播所發行之權杖中的發行者 (iss) 宣告中的 URL。

   - 對於受信任的權杖發行者名稱，請在 IAM 身分中心和應用程式主控台中輸入名稱以識別此受信任的權杖簽發者。
6. 在「對應屬性」下，執行下列操作：

   - 對於身分識別提供者屬性，請從清單中選取要對應至 IAM 身分識別中心身分識別存放區中的屬性的屬性。
   - 對於 IAM 身分中心屬性，請選取屬性對應的對應屬性。
7. 在「標籤 (選用)」下，選擇「新增標籤」，為「機碼」指定值，並選擇性地為「值」指定值。

如需標籤的相關資訊，請參閱標記 AWS IAM Identity Center 資源。

8. 選擇建立信任的權杖發行者。
9. 完成建立受信任的 Token 簽發者之後，請連絡應用程式管理員，讓他們知道受信任的 Token 簽發者的名稱，以便他們可以確認受信任的 Token 簽發者在適用的主控台中可見。
10. 應用程式管理員必須在適用的主控台中選取這個受信任的 Token 簽發者，才能讓使用者從為受信任識別傳播設定的應用程式存取應用程式。

如何在 IAM 身分中心主控台中檢視或編輯受信任的權杖發行者設定

將受信任的權杖發行者新增至 IAM 身分中心主控台後，您可以檢視和編輯相關設定。

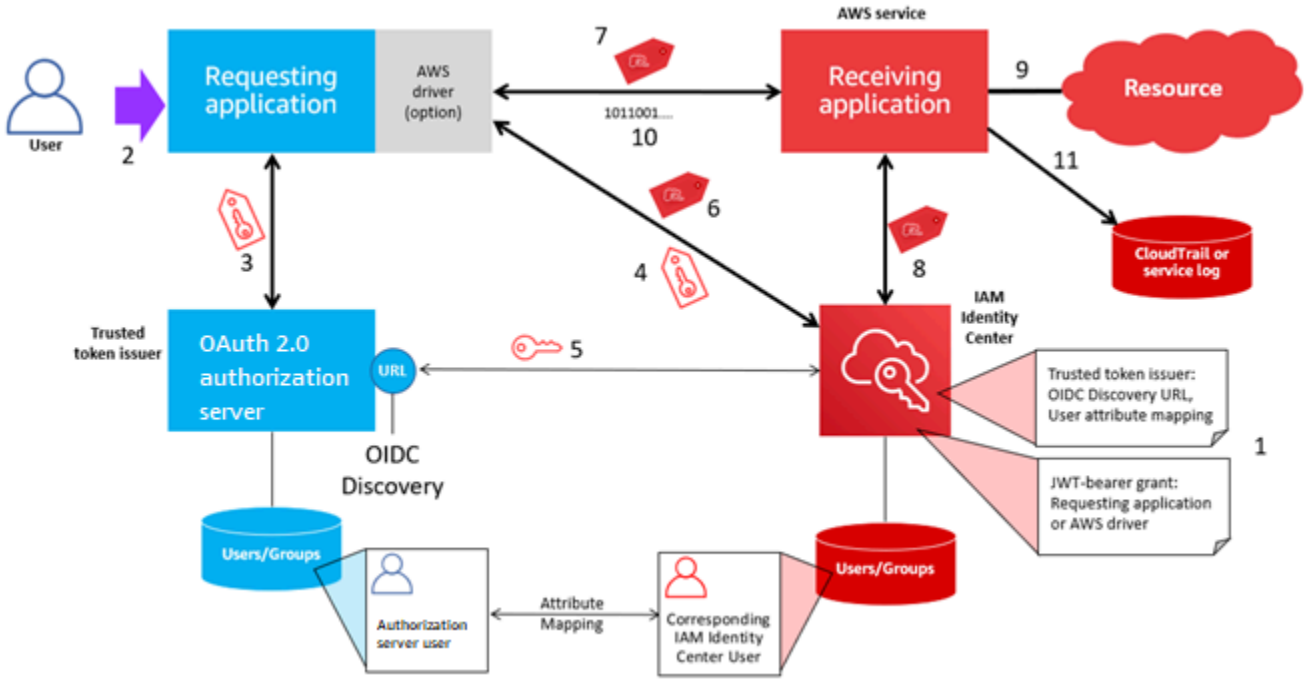
如果您打算編輯受信任的 Token 簽發者設定，請記住，這樣做可能會導致使用者失去設定為使用受信任 Token 簽發者之任何應用程式的存取權。為避免中斷使用者存取，建議您在編輯設定之前，針對設定為使用受信任 Token 簽發者的任何應用程式，先與系統管理員協調。

在 IAM 身分中心主控台中檢視或編輯受信任的權杖發行者設定

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上，選擇 [驗證] 索引標籤。
4. 在「受信任的權杖發行者」下，選取您要檢視或編輯的受信任權杖發行者。
5. 選擇動作，然後選擇編輯。
6. 在 [編輯受信任的權杖簽發者] 頁面上，視需要檢視或編輯設定。您可以編輯受信任的權杖簽發者名稱、屬性對應和標籤。
7. 選擇儲存變更。
8. 在 [編輯受信任的權杖發行者] 對話方塊中，系統會提示您確認是否要進行變更。選擇確認。

針對使用受信任 Token 簽發者的應用程式設定程序和要求流程

本節說明使用受信任 Token 簽發者進行信任身分傳播的應用程式的設定程序和要求流程。下圖提供此程序的概觀。



下列步驟提供有關此程序的其他資訊。

1. 設定 IAM 身分中心和接收 AWS 受管理的應用程式，以使用受信任的權杖發行者。如需相關資訊，請參閱設定受信任權杖簽發者的工作。
2. 當使用者開啟要求的應用程式時，要求流程便會開始。
3. 要求的應用程式會向受信任的 Token 簽發者要求權杖，以啟動對接收 AWS 受管理應用程式的要求。如果用戶尚未通過身份驗證，則此過程將觸發身份驗證流程。令牌包含以下信息：
   - 使用者的主旨 (Sub)。
   - IAM 身分中心用來在 IAM 身分中心查詢對應使用者的屬性。
   - 受眾 (Ad) 聲明，其中包含受信任的權杖發行者與接收 AWS 受管理應用程式建立關聯的值。如果存在其他聲明，IAM 身分中心不會使用它們。
4. 要求的應用程式或其使用的 AWS 驅動程式會將權杖傳遞給 IAM 身分中心，並要求將權杖交換成 IAM 身分中心所產生的權杖。如果您使用 AWS 驅動程式，您可能需要針對此使用案例設定驅動程式。如需詳細資訊，請參閱相關 AWS 受管理應用程式的文件。
5. IAM 身分中心使用 OIDC 探索端點取得可用來驗證權杖真實性的公開金鑰。IAM 身分中心接著會執行下列動作：
   - 驗證權杖。
   - 搜尋身分識別中心目錄。為此，IAM 身分中心會使用權杖中指定的對應屬性。

- 驗證使用者是否有權存取接收應用程式。如果 AWS 受管理的應用程式設定為需要指派給使用者和群組，則使用者必須擁有應用程式的直接或群組型指派，否則會拒絕要求。如果 AWS 受管理的應用程式設定為不需要使用者和群組指派，處理會繼續進行。

> **Note**
>
> AWS 服務具有預設設定組態，可決定使用者和群組是否需要指派。如果您計劃將這些應用程式與信任的識別傳播搭配使用，建議您不要修改這些應用程式的 [需要指派] 設定。即使您已設定可讓使用者存取特定應用程式資源的精細權限，修改 [需要指派] 設定也可能會導致未預期的行為，包括中斷使用者對這些資源的存取。

- 驗證要求的應用程式是否已設定為針對接收 AWS 受管理的應用程式使用有效範圍。

6. 如果先前的驗證步驟成功，IAM 身分中心會建立新的權杖。新的 Token 是不透明的 (加密) 權杖，其中包含 IAM Identity Center 中對應使用者的身分、接收 AWS 受管理應用程式的對象 (Ad)，以及要求應用程式在向接收受 AWS 管理應用程式發出要求時可使用的範圍。
7. 請求的應用程式或其使用的驅動程式會向接收應用程式啟動資源請求，並將 IAM Identity Center 產生的權杖傳遞給接收應用程式。
8. 接收應用程式會呼叫 IAM 身分中心，以取得使用者的身分，以及在權杖中編碼的範圍。它也可能會發出要求，以從 Identity Center 目錄取得使用者屬性或使用者的群組成員資格。
9. 接收應用程式會使用其授權組態來判斷使用者是否有權存取要求的應用程式資源。
10. 如果使用者有權存取要求的應用程式資源，則接收應用程式會回應要求。
11. 使用者的身分、代表他們執行的動作，以及接收應用程式記錄檔和事件中記錄的其他 CloudTrail事件。記錄此資訊的特定方式會根據應用程式而有所不同。

管理 IAM 身分中心憑證

IAM 身分中心使用憑證在 IAM 身分中心和應用程式的服務提供者之間設定 SAML 信任關係。當您在 IAM 身分中心新增應用程式時，系統會自動建立 IAM 身分中心憑證，以便在設定程序期間與該應用程式搭配使用。根據預設，此自動產生的 IAM 身分中心憑證有效期為五年。

身為 IAM 身分中心管理員，您偶爾需要針對特定應用程式使用較新的憑證來取代較舊的憑證。例如，當憑證的到期日臨近時，您可能需要取代憑證。以較新的憑證取代舊憑證的程序稱為憑證輪替。

主題

- 憑證到期狀態指示器

輪換憑證前的注意事項

開始在 IAM 身分中心輪換憑證的程序之前，請考慮下列事項：

- 憑證輪換程序要求您重新建立 IAM 身分中心和服務提供者之間的信任。若要重新建立信任，請使用中輪換 IAM 身分中心憑證提供的程序。
- 使用服務提供者更新憑證可能會造成使用者暫時性的服務中斷，直到信任重新建立為止。如果可能，請在非繁忙時間仔細規劃此操作。

輪換 IAM 身分中心憑證

輪換 IAM 身分中心憑證是一個包含下列各項的多步驟程序：

- 產生新憑證
- 將新憑證新增至服務供應商的網站
- 將新憑證設定為使用中
- 刪除非作用中的憑證

請依照下列順序使用下列所有程序，完成指定應用程式的憑證輪替程序。

步驟 1：產生新憑證。

您可以將您產生的新 IAM 身分中心憑證設定為使用下列屬性：

- 有效期 — 指定新 IAM 身分中心憑證到期前所分配的時間 (以月為單位)。
- 金鑰大小 — 決定金鑰必須與其密碼編譯演算法搭配使用的位元數。您可以將此值設定為 1024 位元 RSA 或 2048 位元 RSA。如需密碼編譯中金鑰大小如何運作的一般資訊，請參閱金鑰大小。
- 演算法 — 指定 IAM 身分中心在簽署 SAML 宣告/回應時使用的演算法。您可以將這個值設定為 SHA-1 或 SHA-256。 AWS 除非您的服務供應商需要 SHA-1，否則建議盡可能使用 SHA-256。如需密碼編譯演算法如何運作的一般資訊，請參閱公開金鑰加密。

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。

3. 在應用程式清單中，選擇您要產生新憑證的應用程式。
4. 在應用程式詳細資訊頁面上，選擇組態索引標籤。在 IAM 身分中心中繼資料下，選擇 [管理憑證]。 如果您沒有 [組態] 索引標籤或無法使用組態設定，則不需要輪換此應用程式的憑證。
5. 在 [IAM 身分中心憑證] 頁面上，選擇 [產生新憑證]。
6. 在 [產生新的 IAM 身分中心憑證] 對話方塊中，為有效期、演算法和金鑰大小指定適當的值。然後選擇「產生」。

步驟 2：更新服務供應商的網站。

使用下列程序來重新建立與應用程式服務提供者的信任。

> **Important**
>
> 當您將新憑證上傳至服務提供者時，您的使用者可能無法取得驗證。若要修正此情況，請將新憑證設定為使用中，如下一個步驟所述。

1. 在 IAM 身分中心主控台中，選擇剛為其產生新憑證的應用程式。
2. 在應用程式詳細資訊頁面上，選擇編輯組態。
3. 選擇 [檢視指示]，然後依照特定應用程式服務提供者網站的指示來新增新產生的憑證。

步驟 3：將新憑證設定為作用中。

一個應用程式最多可以指派兩個憑證。IAM 身分中心將使用設定為作用中的認證來簽署所有 SAML 宣告。

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 在應用程式清單中，選擇您的應用程式。
4. 在應用程式詳細資訊頁面上，選擇組態索引標籤。在 IAM 身分中心中繼資料下，選擇 [管理憑證]。
5. 在 IAM 身分中心憑證頁面上，選取要設定為作用中的憑證，選擇 [動作]，然後選擇 [設定為作用中]。
6. 在 [將選取的憑證設定為作用中的憑證] 對話方塊中，確認您瞭解將憑證設定為使用中可能需要您重新建立信任，然後選擇 [啟動]。

步驟 4：刪除舊證書。

請使用下列程序來完成應用程式的憑證輪替程序。您只能刪除處於非作用中狀態的憑證。

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 在應用程式清單中，選擇您的應用程式。
4. 在應用程式詳細資訊頁面上，選取組態索引標籤。在 IAM 身分中心中繼資料下，選擇 [管理憑證]。
5. 在 IAM 身分中心憑證頁面上，選取您要刪除的憑證。選擇 Actions (動作)，然後選擇 Delete (刪除 VPC)。
6. 在 [刪除憑證] 對話方塊中，選擇 [刪除]。

憑證到期狀態指示器

在應用程式屬性的 [應用程式] 頁面上時，您可能會注意到狀態指示器的彩色圖示。這些圖示會出現在清單中每個憑證旁邊的 [到期日] 欄中。以下說明 IAM 身分中心用來決定每個憑證顯示哪個圖示的條件。

- 紅色 — 表示憑證目前已過期。
- 黃色 — 表示憑證將在 90 天或更短時間內到期。
- 綠色 — 表示憑證目前有效，且至少有效期為 90 天。

若要檢查憑證的目前狀態

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 在應用程式清單中，檢閱清單中的憑證狀態，如 [到期日] 欄中所指示。

在 IAM 身分中心主控台中設定應用程式屬性

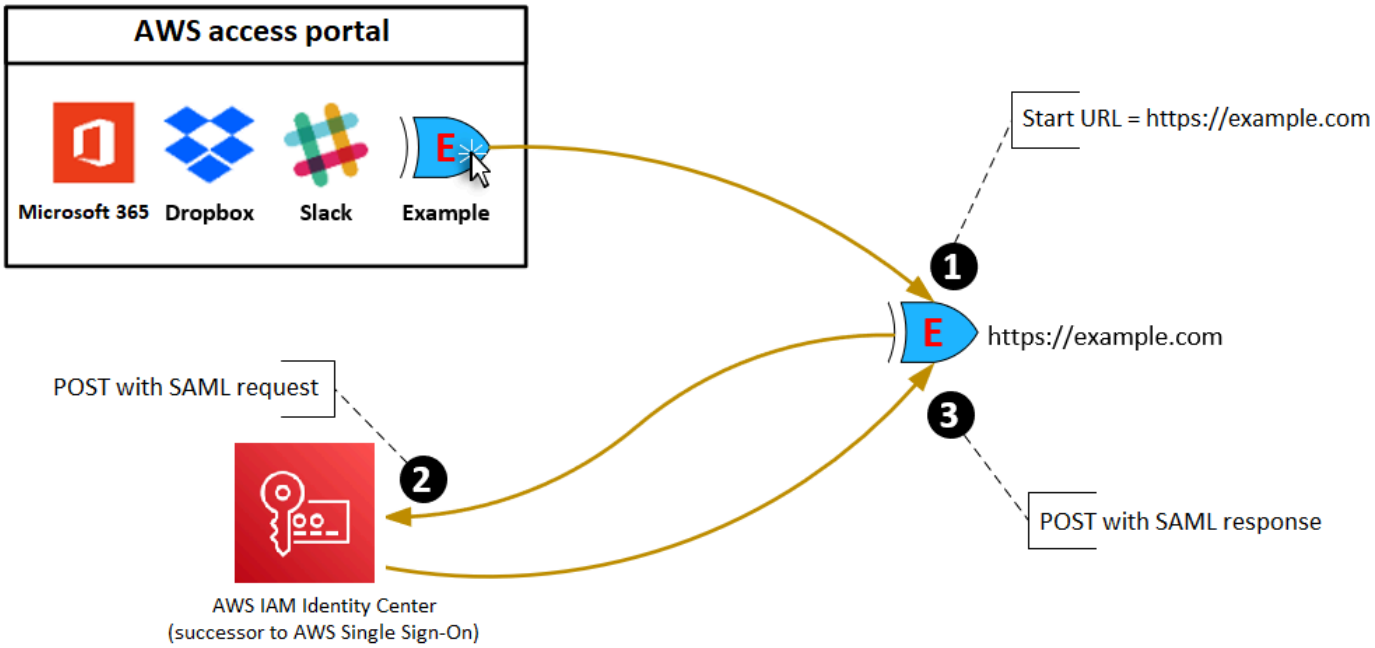
在 IAM 身分中心，您可以透過設定應用程式啟動 URL、轉送狀態和工作階段持續時間來自訂使用者體驗。

申請開始網址

您將使用應用程式啟動 URL，啟動應用程式的聯合身分流程。典型用途是僅支援服務提供者 (SP) 起始繫結的應用程式。

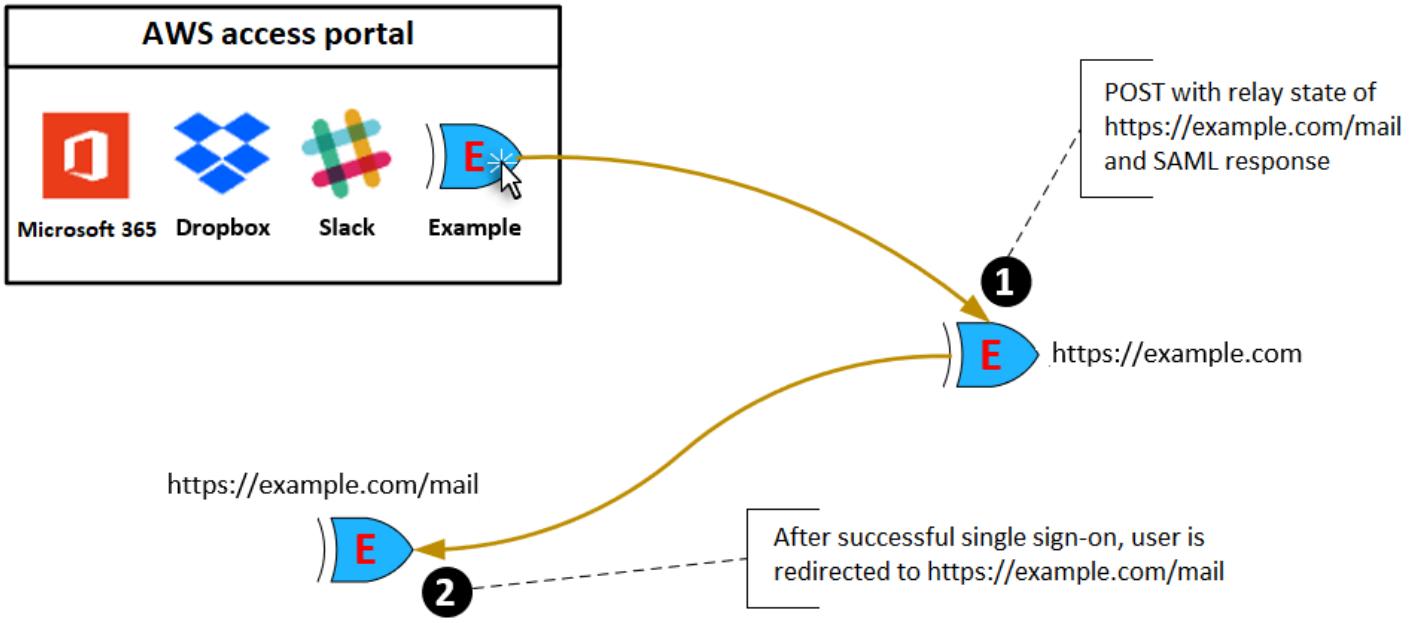
下列步驟與圖表說明當使用者在 AWS 存取入口網站中選擇應用程式時，應用程式啟動 URL 驗證工作流程：

1. 使用者的瀏覽器使用應用程式啟動 URL 的值 (本例為 https://example.com) 將身分驗證請求重新導向。
2. 該應用程序將HTMLPOST帶有一個發送SAMLRequest到 IAM 身份中心。
3. IAM 身分中心接HTMLPOST著會傳送SAMLResponse回應用程式。



繼電器狀態

進行聯合身分驗證期間，轉送狀態會將應用程式內的使用者重新導向。對於 SAML 2.0，此值將未經修改而傳遞至應用程式。設定應用程式屬性之後，IAM 身分中心會將轉送狀態值與 SAML 回應傳送給應用程式。



工作階段持續時間

工作階段持續時間是應用程式使用者工作階段有效的時間長度。對於 SAML 2.0，這是用來設定 SAML 宣告項目的`SessionNotOnOrAfter`日期。`saml2:AuthNStatement`

應用程式可以透過下列其中一種方式來解譯工作階段持續時間：

- 應用程式可以使用它來判斷使用者工作階段允許的最長時間。應用程式可能產生持續時間較短的使用者工作階段。如果應用程式僅支援持續時間不足於所設定工作階段長度的使用者工作階段，就會發生這種情況。
- 應用程式將其用於做為確切的持續時間，而且可能不允許管理員設定其值。如果應用程式僅支援特定的工作階段長度，就會發生這種情況。

如需工作階段持續時間使用方式的詳細資訊，請參閱具體應用程式的說明文件。

在 IAM 身分中心主控台中指派應用程式的使用者存取權

您可以將應用程式目錄中的 SAML 2.0 應用程式或自訂 SAML 2.0 應用程式的單一登入存取權指派給使用者。

群組指派的注意事項：

- 直接將存取權指派給群組。為了簡化存取權限的管理，建議您直接將存取權指派給群組，而非個別使用者。透過群組，您可以授與或拒絕使用者群組的權限，而不必將這些權限套用至每個使用者。如果

使用者移至不同的組織，您只需將該使用者移至其他群組即可。然後，使用者會自動接收新組織所需的權限。

- 不支援巢狀群組。將使用者存取權指派給應用程式時，IAM 身分中心不支援新增至巢狀群組的使用者。如果使用者新增至巢狀群組，他們可能會在登入期間收到「您沒有任何應用程式」訊息。必須針對使用者所屬的直接群組進行指派。

指派應用程式的使用者或群組存取權

> **Important**
>
> 對於 AWS 受管理的應用程式，您必須直接從相關應用程式主控台內或透過 API 新增使用者。

1. 開啟 IAM 身分中心主控台。

   > **Note**
   >
   > 如果您在中管理使用者 AWS Managed Microsoft AD，請確定 IAM Identity Center 主控台使用 AWS Managed Microsoft AD 目錄所在的 AWS 區域，然後再執行下一步。

2. 選擇 Applications (應用程式)。
3. 在應用程式清單中，選擇您要指派存取權的應用程式名稱。
4. 在應用程式詳細資訊頁面的指派使用者區段中，選擇指派使用者。
5. 在「指派使用者」對話方塊中，輸入使用者或群組名稱。您也可以搜尋使用者和群組。您可以指定多個使用者或群組，方法是在他們出現在搜尋結果中時選取適用的帳戶。
6. 選擇 Assign users (指派使用者)。

在 IAM 身分中心主控台中移除使用者存取權

使用此程序可移除使用者存取應用程式目錄或自訂 SAML 2.0 應用程式中的 SAML 2.0 應用程式。

移除使用者對應用程式的存取權

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 在應用程式清單中，選擇您要從中移除使用者存取權的應用程式。

4. 在應用程式詳細資訊頁面的 [指派的使用者] 區段中，選取要移除的使用者或群組，然後選擇 [移除存取權] 按鈕。
5. 在 Remove access (移除存取) 對話方塊中，驗證使用者或群組名稱。然後選擇 Remove access (移除存取)。

將應用程式中的屬性對應至 IAM 身分中心屬性

某些服務供應商需要自訂 SAML 聲明來傳遞有關使用者登入的其他資料。在這種情況下，請使用下列程序來指定應用程式使用者屬性應如何對應至 IAM Identity Center 中對應的對應屬性。

將應用程式屬性對應至 IAM 身分中心的屬性

1. 開啟 IAM 身分中心主控台。
2. 選擇 Applications (應用程式)。
3. 在應用程式清單中，選擇您要對應屬性的應用程式。
4. 在應用程式詳細資訊頁面上，選擇動作，然後選擇編輯屬性對應。
5. 選擇新增屬性對應。
6. 在第一個文字方塊中，輸入應用程式屬性。
7. 在第二個文字方塊中，輸入要對應至應用程式屬性的 IAM 身分中心屬性的屬性。例如，您可能想要將應用程式屬性對應**Username**至 IAM 身分中心使用者屬性**email**。若要查看 IAM 身分中心中允許的使用者屬性清單，請參閱中的表格AWS Managed Microsoft AD 目錄的屬性對應。
8. 在表格的第三欄中，從功能表中選擇屬性的適當格式。
9. 選擇儲存變更。

彈性設計和區域行為

IAM 身分中心服務是全受管的，並使用高可用性和耐用性的AWS服務，例如 Amazon S3 和 Amazon EC2。為了在可用區域中斷時確保可用性，IAM 身分中心會跨多個可用區域運作。如需 IAM 身分中心可用性設計目標的相關資訊，請參閱可靠性支柱指南中的附錄 A：針對特定AWS服務設計的可用性。

您可以在AWS Organizations管理帳戶中啟用 IAM 身分中心。這是必要的，以便 IAM 身分中心可以佈建、取消佈建和更新所有角色。AWS 帳戶當您啟用 IAM 身分中心時，它會部署AWS 區域到目前選取的。如果您想要部署到特定區域AWS 區域，請在啟用 IAM 身分中心之前變更區域選擇。

> **Note**
>
> IAM 身分中心只能從其主要區域控管其權限集和應用程式的存取權。當 IAM 身分中心在單一區域中運作時，建議您考慮與存取控制相關的風險。

雖然 IAM 身分中心會決定您啟用服務所在區域的存取權，但卻AWS 帳戶是全球性的。這表示使用者登入 IAM 身分中心後，當他們AWS 帳戶透過 IAM 身分中心存取時，他們就可以在任何區域中運作。但是 SageMaker，大多數AWS受管應用程式 (例如 Amazon) 都必須安裝在與 IAM 身分中心相同的區域，使用者才能驗證這些應用程式並將存取權指派給這些應用程式。如需將應用程式與 IAM 身分中心搭配使用時的區域限制的相關資訊，請參閱應用程式的文件。

您也可以使用 IAM 身分中心來驗證和授權存取 SAML 型應用程式，這些應用程式可透過公用 URL 存取，而不論建置應用程式的平台或雲端為何。

我們不建議使用做IAM 身分中心的帳戶執行個體為實作恢復能力的方法，因為它會建立第二個獨立的控制點，而且未連接到您的組織執行個體。

設定緊急存取 AWS Management Console

IAM 身分中心是從高可用性AWS基礎架構建立而成，並使用可用區域架構來消除單一故障點。若要在不太可能發生 IAM 身分中心或中AWS 區域斷的情況下提供額外的保護層，我們建議您設定可用來提供對AWS Management Console.

目錄

- 如何設計您的關鍵營運角色
- 如何規劃您的存取模式
- 如何設計緊急角色、帳戶和群組對應
- 如何建立緊急存取設定
- 緊急準備工作
- 緊急容錯移轉程
- 恢復正常操作
- 一次性設定直接 IAM 聯合應用程式 Okta

概要

AWS 讓您可以：

- 將您的第三方 IdP Connect 到 IAM 身分中心。
- 使用以 SAML 2.0 為基礎的聯盟，Connect 您的第三方 IdP 連線到個人AWS 帳戶。

如果您使用 IAM 身分中心，您可以使用這些功能來建立緊急存取設定，如以下各節所述。此設定可讓您使用 IAM 身分中心做為AWS 帳戶存取機制。如果 IAM 身分中斷，您的緊急作業使用者可以使用與存取其帳戶相同的登入資料，AWS Management Console透過直接聯合登入。當 IAM 身分中心無法使用，但 IAM 資料平面和您的外部身分識別提供者 (IdP) 可用時，此組態可用。

> **Important**
>
> 我們建議您在發生中斷之前部署此設定，因為如果您建立所需 IAM 角色的存取權限也中斷，則無法建立組態。此外，請定期測試此組態，以確保您的團隊瞭解 IAM 身分中斷時該如何處理。

緊急出入配置概要

若要設定緊急存取，您必須完成下列工作：

1. 在中建立組織中的緊急作業帳戶AWS Organizations。
2. 使用以 SAML 2.0 為基礎的聯盟，Connect 您的 IdP 連線到緊急作業帳戶。
3. 在緊急作業帳戶中，為協力廠商身分識別提供者聯盟建立角色。此外，使用您所需的權限，在每個工作負載帳戶中建立緊急作業角色。

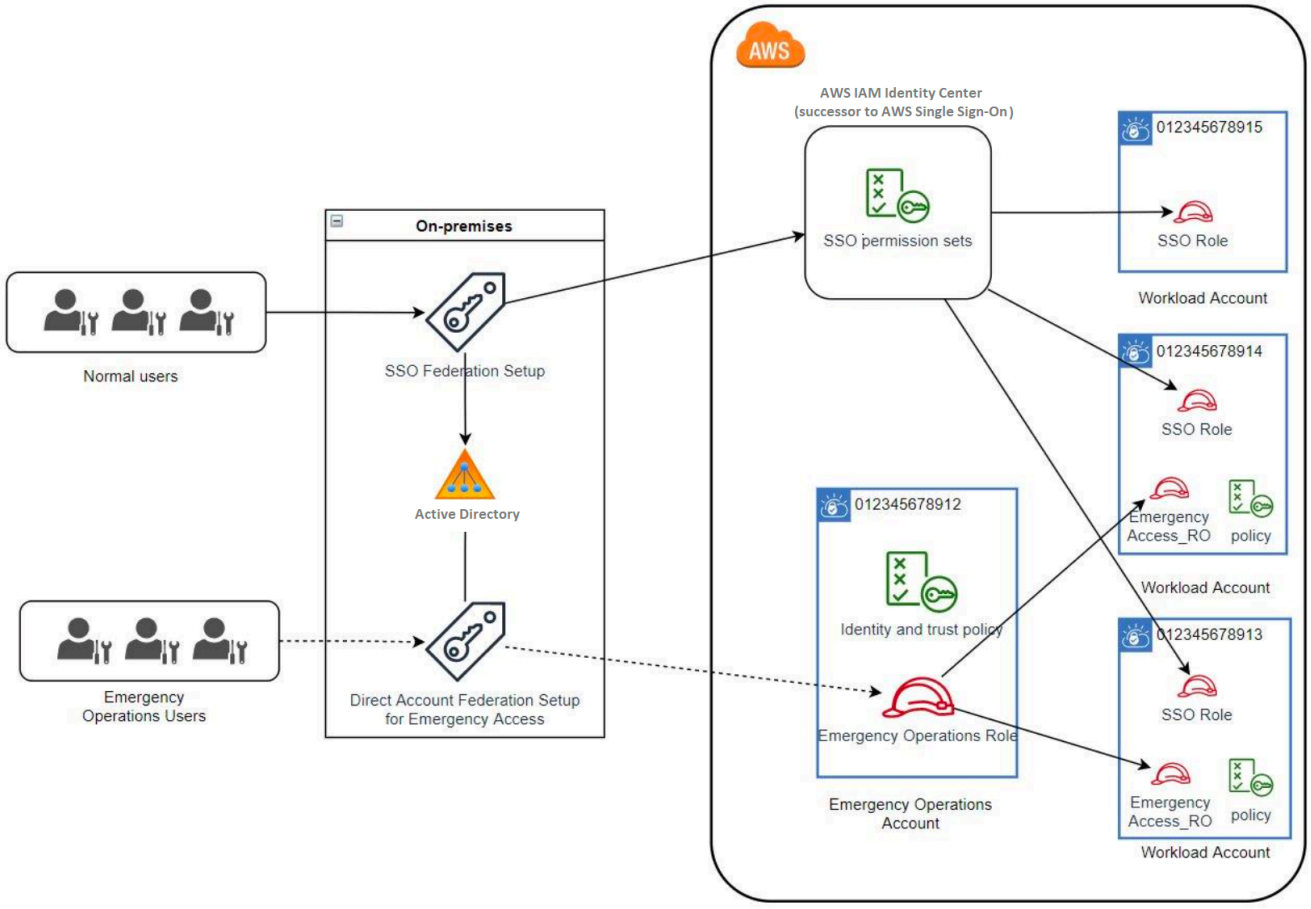
4. 針對您在緊急操作帳戶中建立的 IAM 角色，委派工作負載帳戶的存取權。要授權訪問您的緊急操作帳戶，請在 IdP 中創建一個緊急操作組，沒有成員。
5. 透過在 IdP 中建立可啟用 SAML 2.0 聯合存取的規則，讓 IdP 中的緊急作業群組使用緊急作業角色。AWS Management Console

在正常操作期間，沒有人可以訪問緊急操作帳戶，因為您 IdP 中的緊急操作組沒有成員。如果 IAM 身分中心發生中斷，請使用您的 IdP 將受信任的使用者新增至 IdP 中的緊急作業群組。然後，這些使用者可以登入您的 IdP、瀏覽至AWS Management Console，並在緊急作業帳戶中擔任緊急作業角色。從那裡，這些使用者可以在需要執行作業工作的工作負載帳戶中將角色切換為緊急存取角色。

如何設計您的關鍵營運角色

透過此設計，您可以設定透過 IAM 聯合AWS 帳戶的單一單一資料，以便使用者擔任關鍵作業角色。關鍵作業角色具有信任原則，可讓使用者在工作負載帳戶中擔任相應角色。工作負載帳戶中的角色可提供使用者執行基本工作所需的權限。

下圖提供了設計概述。



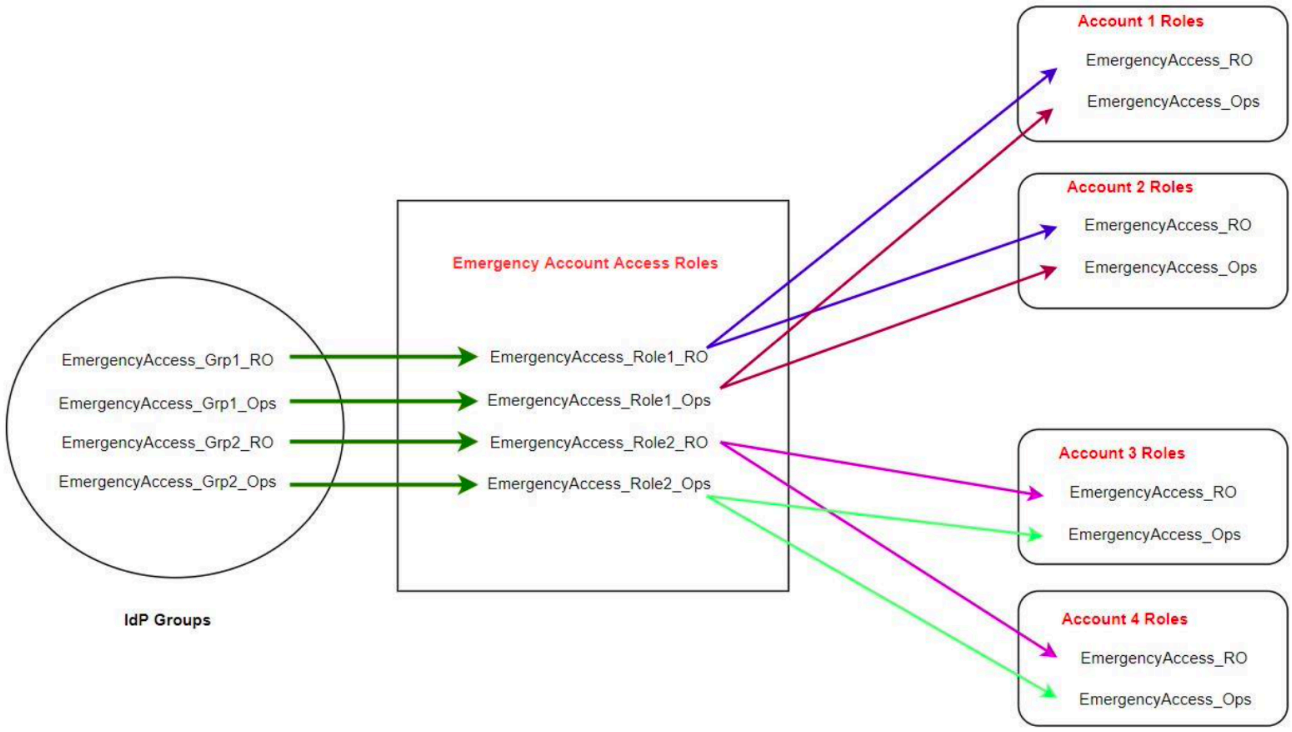
如何規劃您的存取模式

在設定緊急存取之前，請先建立存取模式運作方式的計劃。使用下列流程來建立此計劃。

1. 識別 IAM 身分中心發生中斷期間，緊急操作員存取至關重要的AWS 帳戶地方。例如，您的生產帳戶可能是必不可少的，但您的開發和測試帳戶可能不是。
2. 針對該帳戶集合，識別您在帳戶中所需的特定重要角色。在這些帳戶中，在定義角色可以執行的操作時保持一致。如此可簡化您建立跨帳戶角色的緊急存取帳戶中的工作。我們建議您從這些帳戶中的兩個不同角色開始：唯讀 (RO) 和作業 (Ops)。如有必要，您可以建立更多角色，並將這些角色對應至設定中更不同的緊急存取使用者群組。
3. 識別並建立 IdP 中的緊急存取群組。群組成員是您將存取權委派給其緊急存取角色的使用者。
4. 定義這些群組可以在緊急存取帳戶中擔任的角色。若要這麼做，請在 IdP 中定義產生宣告的規則，以列出群組可存取的角色。然後，這些群組可以在緊急存取帳戶中擔任您的「唯讀」或「操作」角色。在這些角色中，他們可以在您的工作負載帳戶中擔任相應的角色。

如何設計緊急角色、帳戶和群組對應

下圖顯示如何將緊急存取群組對應至緊急存取帳戶中的角色。此圖還顯示了跨帳戶角色信任關係，這些關係可讓緊急存取帳戶角色存取工作負載帳戶中對應的角色。我們建議您的應急計劃設計使用這些映射作為起點。



如何建立緊急存取設定

使用下列對應表格建立您的緊急存取設定。此表格反映了一個計劃，其中包括工作負載帳戶中的兩個角色：唯讀 (RO) 和 Operations (Ops)，以及對應的信任原則和權限原則。信任原則可讓緊急存取帳戶角色存取個別工作負載帳戶角色。個別工作負載帳戶角色也具有角色在帳戶中可執行的動作的權限原則。權限策略可以是AWS管理策略或客戶管理的策略。

帳戶	要建立的角色	信任政策	許可政策
帳戶 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess

帳戶	要建立的角色	信任政策	許可政策
帳戶 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
帳戶二	Emergency Access_RO	Emergency Access_Role2_RO	ARN: AW: IAM:: aws: 策略/ReadOnlyAccess
帳戶二	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
緊急存取帳戶	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	AssumeRole 帳號中的角色資源

在此對應計劃中，緊急存取帳戶包含兩個唯讀角色和兩個作業角色。這些角色信任您的 IdP 可以透過在宣告中傳遞角色的名稱來驗證並授權您選取的群組存取角色。工作負載帳戶 1 和帳戶 2 中有對應的唯讀和作業角色。對於工作負載帳戶 1，`EmergencyAccess_RO`角`EmergencyAccess_Role1_RO`色信任緊急存取帳戶中的角色。此表格會指定工作負載帳戶唯讀和作業角色之間的類似信任模式，以及對應的緊急存取角色。

緊急準備工作

若要準備緊急存取設定，我們建議您在緊急情況發生之前執行下列工作。

1. 在您的 IdP 中設定直接的 IAM 聯合應用程式。如需詳細資訊，請參閱 一次性設定直接 IAM 聯合應用程式 Okta。
2. 在緊急存取帳戶中建立 IdP 連線，以便在事件期間存取。

3. 如上述對應表格所述，在緊急存取帳戶中建立緊急存取角色。
4. 在每個工作負載帳戶中建立具有信任和權限原則的臨時作業角色。
5. 在 IdP 中建立暫時作業群組。群組名稱將取決於暫存作業角色的名稱。
6. 測試直接 IAM 聯合。
7. 停用 IdP 中的 IdP 聯合應用程式，以防止常規使用。

緊急容錯移轉程

當 IAM Identity Center 執行個體無法使用時，且您判斷必須提供AWS管理主控台的緊急存取權限時，我們建議您執行下列容錯移轉程序。

1. IdP 管理員可在您的 IdP 中啟用直接 IAM 聯合應用程式。
2. 使用者透過您現有的機制 (例如電子郵件要求、Slack 通道或其他形式的通訊) 要求存取臨時作業群組。
3. 您新增至緊急存取群組的使用者登入 IdP、選取緊急存取帳戶，然後使用者選擇要在緊急存取帳戶中使用的角色。透過這些角色，他們可以在對應的工作負載帳戶中擔任具有跨帳戶信任且具有緊急帳戶角色的角色。

恢復正常操作

檢查 AWSHealth 情況儀表板以確認 IAM 身分中心服務的健康狀態何時恢復。若要恢復正常作業，請執行下列步驟。

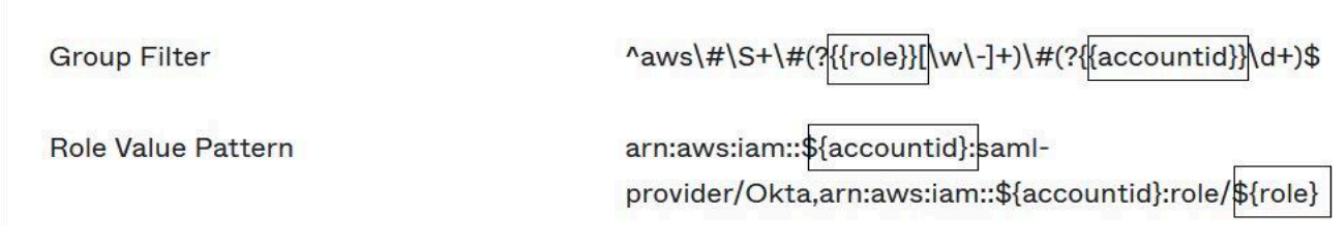
1. IAM 身分中心服務的狀態圖示指出服務正常後，請登入 IAM 身分中心。
2. 如果您可以成功登入 IAM 身分中心，請與緊急存取使用者通知 IAM 身分中心可用。指示這些使用者登出，並使用AWS存取入口網站重新登入 IAM 身分中心。
3. 所有緊急存取使用者登出後，請在 IdP 中停用 IdP 同盟應用程式。建議您在下班時間後執行此工作。
4. 從 IdP 中的緊急存取群組中移除所有使用者。

您的緊急存取角色基礎結構會保留為備份存取計劃，但現在已停用。

一次性設定直接 IAM 聯合應用程式 Okta

1. 以具有管理權限的使用者身分登入您的Okta帳戶。

2. 在Okta管理控制台的應用程式下，選擇應用程式。
3. 選擇瀏覽應用程式目錄。搜尋並選擇 [AWS帳戶同盟]。然後選擇「新增整合」。
4. AWS依照如何為聯合帳戶設定 SAML 2.0 中的步驟，設定直接 AWS IAM 聯合。
5. 在 [登入選項] 索引標籤上，選取 SAML 2.0 並輸入群組篩選器和角色值模式設定。使用者目錄的群組名稱取決於您設定的篩選器。



在上圖中，role變數適用於緊急存取帳戶中的緊急作業角色。例如，如果您在中建立EmergencyAccess_Role1_RO角色 (如對應表格中所述) AWS 帳戶123456789012，並且如上圖所示配置群組篩選器設定，則您的群組名稱應為aws#EmergencyAccess_Role1_RO#123456789012。

6. 在您的目錄 (例如，Active Directory 中的目錄) 中，建立緊急存取群組，並指定目錄的名稱 (例如aws#EmergencyAccess_Role1_RO#123456789012)。使用現有的佈建機制，將使用者指派給此群組。
7. 在緊急存取帳戶中，設定自訂信任原則，以提供中斷期間所需的緊急存取角色所需的權限。以下是附加至EmergencyAccess_Role1_RO角色之自訂信任原則的範例陳述式。如需圖解，請參閱下圖中的緊急帳戶如何設計緊急角色、帳戶和群組對應。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
            "sts:SetSourceIdentity",
            "sts:TagSession"
         ],
         "Condition":{
            "StringEquals":{
               "SAML:aud":"https:~/~/signin.aws.amazon.com/saml"
```

```
            }
         }
      }
   ]
}
```

8. 以下是附加至EmergencyAccess_Role1_RO角色之權限原則的範例陳述式。如需圖解，請參閱下圖中的緊急帳戶如何設計緊急角色、帳戶和群組對應。

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Action":"sts:AssumeRole",
         "Resource":[
            "arn:aws:iam::<account 1>:role/EmergencyAccess_RO",
            "arn:aws:iam::<account 2>:role/EmergencyAccess_RO"
         ]
      }
   ]
}
```

9. 在工作負載帳戶上，設定自訂信任原則。以下是附加至EmergencyAccess_RO角色之信任原則的範例陳述式。在此範例中，帳戶123456789012是緊急存取帳戶。如需圖解，請參閱下圖中的工作負載帳戶如何設計緊急角色、帳戶和群組對應。

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> 大多數可 IdPs 讓您停用應用程式整合，直到需要為止。我們建議您在 IdP 中停用直接 IAM 聯合應用程式，直到需要緊急存取為止。

中的安全性 AWS IAM Identity Center

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。若要深入瞭解適用於的規範遵循計劃 AWS IAM Identity Center，請參閱合規方案的AWS 服務範圍。
- 雲端中的安全性 — 您的責任取決於您使用的 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。

本文件可協助您瞭解如何在使用 IAM 身分中心時套用共同的責任模型。以下主題說明如何設定 IAM 身分中心，以符合安全性和合規目標。您也會學到如何使用其他可 AWS 協助您監控和保護 IAM 身分中心資源的服務。

主題

- IAM 身分識別中心的身分識別與存取管理
- IAM 身分識別中心主控台和 API 授權
- AWS STS IAM 身分中心的條件內容金鑰
- IAM 身分中心中的記錄和監控
- IAM 身分中心的合規驗證
- IAM 身分中心的彈性
- IAM 身分中心的基礎設施安全

IAM 身分識別中心的身分識別與存取管理

存取 IAM 身分中心需要 AWS 可用來驗證您的請求的登入資料。這些認證必須具有存取 AWS 資源的權限，例如 AWS 受管理的應用程式。

AWS 存取入口網站的身份驗證是由您連線到 IAM 身分中心的目錄所控制。不過，使用者可從 AWS 存取入口網站中使用的授權是由兩個因素決定： AWS 帳戶

1. 誰已 AWS 帳戶 在 IAM 身分中心主控台中被指派存取權限。如需詳細資訊，請參閱 單一登入存取權 AWS 帳戶。
2. IAM Identity Center 主控台中的使用者已授與哪些等級的許可，以允許他們適當的存取權限 AWS 帳戶。如需詳細資訊，請參閱 建立、管理及刪除權限集。

以下各節說明身為系統管理員的您可以如何控制 IAM 身分中心主控台的存取權，或是從 IAM 身分中心主控台委派 day-to-day 工作的管理存取權。

- 身分驗證
- 存取控制

身分驗證

了解如何 AWS 使用 IAM 身分進行存取。

存取控制

您可以擁有有效的登入資料來驗證您的請求，但除非您擁有許可，否則無法建立或存取 IAM 身分中心資源。例如，您必須擁有權限才能建立 IAM 身分中心連線的目錄。

以下各節說明如何管理 IAM 身分中心的許可。我們建議您先閱讀概觀。

- 管理 IAM 身分中心資源存取許可的概觀
- IAM 身分中心的身分型政策範例
- 針對 IAM 身分中心使用服務連結角色

管理 IAM 身分中心資源存取許可的概觀

每個 AWS 資源都擁有 AWS 帳戶，建立或存取資源的權限由權限原則控制。為了提供存取權，帳戶管理員可以將許可新增至 IAM 身分 (亦即使用者、群組和角色)。某些服務 (例如 AWS Lambda) 還支持向資源添加權限。

> **Note**
>
> 帳戶管理員 (或管理員使用者) 是具有管理員權限的使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 最佳實務。

主題

IAM 身分識別中心資源和作業

在 IAM 身分中心，主要資源是應用程式執行個體、設定檔和權限集。

了解資源所有權

資源擁有者 AWS 帳戶 是建立資源的人。也就是說，資源擁有者是驗證建立資源 AWS 帳戶 之請求的主體實體 (帳戶、使用者或 IAM 角色) 的身份。下列範例說明其如何運作：

- 如果 AWS 帳戶根使用者 建立 IAM 身分中心資源 (例如應用程式執行個體或權限集)，您 AWS 帳戶就是該資源的擁有者。
- 如果您在 AWS 帳戶中建立使用者，並授與該使用者建立 IAM 身分中心資源的許可，則該使用者可以建立 IAM 身分中心資源。不過，您的 AWS 帳戶 (使用者所屬) 擁有資源。
- 如果您在 AWS 帳戶中建立具有建立 IAM 身分中心資源的許可的 IAM 角色，則任何可以擔任該角色的人都可以建立 IAM 身分中心資源。您的 AWS 帳戶角色所屬，擁有 IAM 身分中心資源。

管理資源存取

許可政策描述誰可以存取哪些資源。下一節說明可用來建立許可政策的選項。

> **Note**
>
> 本節討論在 IAM 身分中心的內容中使用 IAM。它不提供 IAM 服務的詳細資訊。如需完整的 IAM 文件，請參閱《IAM 使用者指南》中的什麼是 IAM？。如需有關 IAM 政策語法和說明的資訊，請參閱《IAM 使用者指南》中的 AWS IAM 政策參考。

連接至 IAM 身分的政策稱為身分識別型政策 (IAM 政策)。連接到資源的政策稱為「資源類型」政策。IAM 身分中心僅支援以身分識別為基礎的政策 (IAM 政策)。

主題

- 身分類型政策 (IAM 政策)
- 資源型政策

身分類型政策 (IAM 政策)

您可以將許可新增至 IAM 身分。例如，您可以執行下列動作：

- 將許可政策附加至您的使用者或群組 AWS 帳戶— 帳戶管理員可以使用與特定使用者相關聯的許可政策來授與該使用者新增 IAM Identity Center 資源 (例如新應用程式) 的許可。
- 將許可政策連接至角色 (授予跨帳戶許可)：您可以將身分識別型許可政策連接至 IAM 角色，藉此授予跨帳戶許可。

  如需有關使用 IAM 來委派許可的詳細資訊，請參閱《IAM 使用者指南》中的存取管理。

下列許可政策會授予使用者執行開頭為 `List` 之所有動作的許可。這些動作會顯示 IAM 身分中心資源的相關資訊，例如應用程式執行個體或權限集。請注意，元素中的萬用字`Resource`元 (*) 表示該帳戶擁有的所有 IAM 身分中心資源都允許執行動作。

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

如需將身分型政策與 IAM 身分中心搭配使用的詳細資訊，請參閱。IAM 身分中心的身分型政策範例如需使用者、群組、角色和許可的相關資訊，請參閱《IAM 使用者指南》中的身分 (使用者、群組和角色)。

資源型政策

其他服務 (例如 Amazon S3) 也支援以資源為基礎的許可政策。例如，您可以將政策連接至 S3 儲存貯體，以管理該儲存貯體的存取許可。IAM 身分中心不支援以資源為基礎的政策。

指定策略元素：動作、效果、資源和主參與者

對於每個 IAM 身分中心資源 (請參閱IAM 身分識別中心資源和作業)，服務會定義一組 API 作業。為了授予這些 API 操作的許可，IAM 身分中心會定義一組您可以在政策中指定的動作。請注意，執行 API 操作可能需要多個動作的許可。

以下是基本的政策元素：

- 資源 – 在政策中，您可以使用 Amazon Resource Name (ARN) 來識別要套用政策的資源。
- 動作：使用動作關鍵字識別您要允許或拒絕的資源操作。例如，該`sso:DescribePermissionsPolicies`權限允許使用者權限執行 IAM 身分中心`DescribePermissionsPolicies`作業。
- 效果 - 您可以指定使用者要求特定動作時會有什麼效果；可為允許或拒絕。如果您未明確授予存取 (允許) 資源，則隱含地拒絕存取。您也可以明確拒絕資源存取，這樣做可確保使用者無法存取資源，即使不同政策授予存取也是一樣。
- 委託人：在以身分為基礎的政策 (IAM 政策) 中，政策所連接的使用者就是隱含委託人。對於資源型政策，您可以指定想要收到許可的使用者、帳戶、服務或其他實體 (僅適用於資源型政策)。IAM 身分中心不支援以資源為基礎的政策。

如需進一步了解有關 IAM 政策語法和說明的詳細資訊，請參閱《IAM 使用者指南》中的 AWS IAM 政策參考。

在政策中指定條件

當您授予許可時，可以使用存取原則語言來指定要讓政策生效而須滿足的條件。例如，建議只在特定日期之後套用政策。如需使用政策語言指定條件的詳細資訊，請參閱IAM 使用者指南中的條件。

欲表示條件，您可以使用預先定義的條件金鑰。IAM 身分中心沒有特定條件金鑰。但是，您可以視需要使用某些 AWS 條件索引鍵。如需完整 AWS 金鑰清單，請參閱 IAM 使用者指南中的可用全域條件金鑰。

IAM 身分中心的身分型政策範例

本主題提供 IAM 政策範例，您可以建立這些政策以授與使用者和角色管理 IAM 身分中心的權限。

> **Important**
>
> 我們建議您先檢閱介紹性主題，其中說明可用來管理 IAM 身分中心資源存取權的基本概念和選項。如需詳細資訊，請參閱 管理 IAM 身分中心資源存取許可的概觀。

本主題中的各節涵蓋下列內容：

- 自訂原則範例
- 使用 IAM 身分中心主控台所需的許可

自訂原則範例

本節提供需要自訂 IAM 政策的常見使用案例範例。這些範例原則是以識別為基礎的原則，不會指定「主參與者」元素。這是因為使用以身分識別為基礎的原則，您不會指定取得權限的主體。而是將原則附加至主體。將以身分為基礎的許可政策附加到 IAM 角色時，角色信任策略中識別的主體將獲得許可。您可以在 IAM 中建立身分型政策，並將其附加到使用者、群組和/或角色。您也可以在 IAM 身分中心建立權限集時，將這些政策套用至 IAM 身分中心使用者。

> **Note**
>
> 當您為環境建立原則，並確定在生產環境中部署這些原則之前測試正面（「授與存取」）和負面（「拒絕存取」）測試案例時，請使用這些範例。如需有關測試 IAM 政策的詳細資訊，請參閱 IAM 使用者指南中的使用 IAM 政策模擬器測試 IAM 政策。

主題

- 範例 1：允許使用者檢視 IAM 身分中心
- 範例 2：允許使用者 AWS 帳戶 在 IAM 身分中心管理許可
- 範例 3：允許使用者在 IAM 身分中心管理應用程式
- 範例 4：允許使用者管理身分識別中心目錄中的使用者和群組

範例 1：允許使用者檢視 IAM 身分中心

下列許可政策會將唯讀權限授與使用者，以便他們可以檢視 IAM 身分中心中設定的所有設定和目錄資訊。

> **Note**
>
> 此政策僅供範例使用。在生產環境中，建議您使用 IAM 身分中心的`ViewOnlyAccess` AWS 受管政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListOrganizationalUnitsForParent",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListPermissionSets",
                "sso:DescribePermissionSet",
                "sso:GetInlinePolicyForPermissionSet",
                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

範例 2：允許使用者 AWS 帳戶 在 IAM 身分中心管理許可

下列權限原則會授與權限，讓使用者建立、管理及部署您的權限集 AWS 帳戶。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeleteInlinePolicyFromPermissionSet",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet",
                "sso:UpdatePermissionSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMListPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AccessToSSOProvisionedRoles",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
```

```
                "iam:PutRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetSAMLProvider"
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
        }
    ]
}
```

> **Note**
>
> 只有在允許使用者在 AWS Organizations 管理帳戶中建立指派時`"Sid": "IAMListPermissions"`，才需要列在和`"Sid": "AccessToSSOProvisiondRoles"`區段下列出的其他權限。在某些情況下，您可能還需要新增`iam:UpdateSAMLProvider`至這些區段。

範例 3：允許使用者在 IAM 身分中心管理應用程式

下列許可政策授予許可，允許使用者在 IAM 身分中心檢視和設定應用程式，包括 IAM 身分中心目錄中預先整合的 SaaS 應用程式。

> **Note**
>
> 若要管理應用程式的使用者和群組指派，需要在下列原則範例中使用的`sso:AssociateProfile`作業。它也可讓使用者使用現有的權限集，將使用者和群組指派給這些使用者和群組。 AWS 帳戶 如果使用者必須在 IAM 身分中心管理 AWS 帳戶 存取權，並且需要管理權限集所需的許可，請參閱範例 2：允許使用者 AWS 帳戶 在 IAM 身分中心管理許可。

自 2020 年 10 月起，其中許多操作僅可通過 AWS 控制台進行。此範例原則包含「讀取」動作 (例如清單、取得和搜尋)，這些動作與此案例的主控台無錯誤作業相關。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:ImportApplicationInstanceServiceProviderMetadata",
                "sso:DeleteApplicationInstance",
                "sso:DeleteProfile",
                "sso:DisassociateProfile",
                "sso:GetApplicationTemplate",
                "sso:UpdateApplicationInstanceServiceProviderConfiguration",
                "sso:UpdateApplicationInstanceDisplayData",
                "sso:DeleteManagedApplicationInstance",
                "sso:UpdateApplicationInstanceStatus",
                "sso:GetManagedApplicationInstance",
                "sso:UpdateManagedApplicationInstanceStatus",
                "sso:CreateManagedApplicationInstance",
                "sso:UpdateApplicationInstanceSecurityConfiguration",
                "sso:UpdateApplicationInstanceResponseConfiguration",
                "sso:GetApplicationInstance",
                "sso:CreateApplicationInstanceCertificate",
                "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
                "sso:UpdateApplicationInstanceActiveCertificate",
                "sso:DeleteApplicationInstanceCertificate",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationTemplates",
                "sso:ListApplications",
                "sso:ListApplicationInstances",
                "sso:ListDirectoryAssociations",
                "sso:ListProfiles",
                "sso:ListProfileAssociations",
                "sso:ListInstances",
                "sso:GetProfile",
                "sso:GetSSOStatus",
                "sso:GetSsoConfiguration",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeUsers",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

範例 4：允許使用者管理身分識別中心目錄中的使用者和群組

以下許可政策授予許可，允許使用者在 IAM 身分中心建立、檢視、修改和刪除使用者和群組。

在某些情況下，對 IAM 身分中心中的使用者和群組進行直接修改會受到限制。例如，選取 Active Directory 或啟用「自動佈建」的外部身分識別提供者作為身分識別來源時。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso-directory:ListGroupsForUser",
                "sso-directory:DisableUser",
                "sso-directory:EnableUser",
                "sso-directory:SearchGroups",
                "sso-directory:DeleteGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:DescribeDirectory",
                "sso-directory:UpdateUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:SearchUsers",
                "sso:ListDirectoryAssociations",
                "sso-directory:RemoveMemberFromGroup",
                "sso-directory:DeleteUser",
                "sso-directory:DescribeUsers",
                "sso-directory:UpdateGroup",
                "sso-directory:CreateGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

使用 IAM 身分中心主控台所需的許可

若要讓使用者在不發生錯誤的情況下使用 IAM 身分中心主控台，則需要其他許可。如果建立的 IAM 政策比所需的最低權限更嚴格，則控制台將無法按照具有該政策的使用者預期運作。下列範例列出了在 IAM Identity Center 主控台中確保無錯誤操作所需的一組許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
                "sso:DescribePermissionSetProvisioningStatus",
                "sso:DescribePermissionsPolicies",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
                "sso:GetPermissionSet",
                "sso:GetPermissionsPolicy",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:ListAccountAssignmentCreationStatus",
                "sso:ListAccountAssignmentDeletionStatus",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationInstances",
                "sso:ListApplications",
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetProvisioningStatus",
                "sso:ListPermissionSets",
```

```
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:ListTagsForResource",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeUsers",
                "sso-directory:ListGroupsForUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS IAM 身分中心的受管政策

若要建立 IAM 客戶受管政策，只為您的團隊提供他們所需的許可，需要時間和專業知識。若要快速開始使用，您可以使用 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需 AWS 受管政策的更多相關資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。

AWS 服務會維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，ReadOnlyAccess AWS 受管理的策略提供對所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

新的命名空間下提供了可讓您列出和刪除使用者工作階段的新動作`identitystore-auth`。此命名空間中動作的任何其他權限都會在此頁面上更新。建立自訂 IAM 政策時，請避免使用 * after，`identitystore-auth`因為這適用於目前或 future 命名空間中存在的所有動作。

AWS 受管理的策略： AWSSSOMasterAccountAdministrator

`AWSSSOMasterAccountAdministrator`原則會為主參與者提供必要的管理動作。此原則適用於執行 AWS IAM Identity Center 管理員工作角色的主參與者。隨著時間的推移，系統會更新所提供的動作清單，以符合 IAM Identity Center 的現有功能以及管理員所需的動作。

您可將 AWSSSOMasterAccountAdministrator 政策連接到 IAM 身分。
將AWSSSOMasterAccountAdministrator原則附加至身分識別時，即授與系統管理 AWS IAM Identity Center 權限。具有此政策的主體可以在 AWS Organizations 管理帳戶和所有成員帳戶中存取 IAM 身分中心。此主體可以完整管理所有 IAM 身分中心作業，包括建立 IAM 身分中心執行個體、使用者、權限集和指派的能力。主體也可以在整個 AWS 組織成員帳戶中實例化這些指派，並在 AWS Directory Service 受管目錄和 IAM 身分中心之間建立連線。當新的系統管理功能發行時，帳戶管理員會自動獲得這些權限。

權限分組

此政策會根據提供的許可集分組到陳述式中。

- AWSSSOMasterAccountAdministrator— 允許 IAM 身分中心將名為的服務角色傳遞AWSServiceRoleforSSO給 IAM 身分中心，以便稍後可以擔任該角色並代表他們執行動作。當個人或應用程式嘗試啟用 IAM 身分中心時，這是必要的。如需詳細資訊，請參閱 管理存取 AWS 帳戶。
- AWSSSOMemberAccountAdministrator— 允許 IAM 身分中心在多帳戶 AWS 環境中執行帳戶管理員動作。如需詳細資訊，請參閱 AWS 受管理的策略： AWSSSOMemberAccountAdministrator。
- AWSSSOManageDelegatedAdministrator— 允許 IAM 身分中心為您的組織註冊和取消註冊委派的系統管理員。

若要檢視此策略的權限，請參閱AWS 受管理AWSSSOMasterAccountAdministrator的策略參考中的。

關於此政策的其他資訊

第一次啟用 IAM 身分中心時，IAM 身分中心服務會在 AWS Organizations 管理帳戶 (之前的主帳戶) 中建立服務連結的角色，以便 IAM 身分中心可以管理您帳戶中的資源。需要的動作為iam:CreateServiceLinkedRole和iam:PassRole，顯示在下列程式碼片段中。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSSSOCreateSLR",
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition": {
            "StringLike": {
```

```
                "iam:AWSServiceName": "sso.amazonaws.com"
            }
         }
      },
      {
         "Sid":"AWSSSOMasterAccountAdministrator",
         "Effect":"Allow",
         "Action":"iam:PassRole",
         "Resource":"arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition":{
             "StringLike":{
               "iam:PassedToService":"sso.amazonaws.com"
             }
         }
      },
   ]
}
```

AWS 受管理的策略： AWSSSOMemberAccountAdministrator

AWSSSOMemberAccountAdministrator原則會為主參與者提供必要的管理動作。此政策適用於擔任 IAM 身分識別中心管理員工作角色的主體。隨著時間的推移，系統會更新所提供的動作清單，以符合 IAM Identity Center 的現有功能以及管理員所需的動作。

您可將 AWSSSOMemberAccountAdministrator 政策連接到 IAM 身分。將AWSSSOMemberAccountAdministrator原則附加至身分識別時，即授與系統管理 AWS IAM Identity Center 權限。具有此政策的主體可以在 AWS Organizations 管理帳戶和所有成員帳戶中存取 IAM 身分中心。此主體可以完整管理所有 IAM 身分中心作業，包括建立使用者、權限集和指派的能力。主體也可以在整個 AWS 組織成員帳戶中實例化這些指派，並在 AWS Directory Service 受管目錄和 IAM 身分中心之間建立連線。當新的系統管理功能發行時，帳戶管理員會自動獲得這些權限。

若要檢視此策略的權限，請參閱AWS 受管理AWSSSOMemberAccountAdministrator的策略參考中的。

關於此政策的其他資訊

IAM 身分識別中心管理員在其身分識別中心目錄存放區 (sso-directory) 中管理使用者、群組和密碼。帳戶管理員角色包含下列動作的權限：

- "sso:*"
- "sso-directory:*"

IAM 身分中心管理員需要有限的權限才能執行日常工 AWS Directory Service 作，才能執行下列動作。

- "ds:DescribeTrusts"
- "ds:UnauthorizeApplication"
- "ds:DescribeDirectories"
- "ds:AuthorizeApplication"
- “ds:CreateAlias”

這些許可允許 IAM 身分中心管理員識別現有目錄並管理應用程式，以便將其設定為與 IAM 身分中心搭配使用。如需有關每個動作的詳細資訊，請參閱 AWS Directory Service API 權限：動作、資源和條件參考。

IAM 身分中心使用 IAM 政策將許可授與 IAM 身分中心使用者。IAM 身分識別中心管理員會建立權限集，並將政策附加到他們。IAM Identity Center 管理員必須擁有列出現有政策的許可，以便他們可以選擇要搭配建立或更新的權限集使用哪些原則。若要設定安全和功能性許可，IAM 身分中心管理員必須具有執行 IAM 存取分析器政策驗證的許可。

- "iam:ListPolicies"
- "access-analyzer:ValidatePolicy"

IAM 身分中心管理員需要有限的存取權限，才能 AWS Organizations 執行日常工作：

- "organizations:EnableAWSServiceAccess"
- "organizations:ListRoots"
- "organizations:ListAccounts"
- "organizations:ListOrganizationalUnitsForParent"
- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"
- "organizations:ListDelegatedAdministrators"
- "organizations:RegisterDelegatedAdministrator"
- "organizations:DeregisterDelegatedAdministrator"

這些許可讓 IAM 身分中心管理員能夠使用組織資源 (帳戶) 執行基本 IAM 身分中心管理任務，例如：

- 識別屬於組織的管理帳戶
- 識別屬於組織的成員帳戶
- 啟用帳戶的 AWS 服務存取權
- 設定和管理委派的管理員

如需將委派管理員與 IAM 身分中心搭配使用的詳細資訊，請參閱委派管理。如需這些權限如何搭配使用的詳細資訊 AWS Organizations，請參閱AWS Organizations 搭配其他 AWS 服務使用。

AWS 受管理的策略： AWSSSODirectoryAdministrator

您可將 `AWSSSODirectoryAdministrator` 政策連接到 IAM 身分。

此政策授予 IAM 身分中心使用者和群組的管理許可。附加此政策的主體可以對 IAM 身分中心使用者和群組進行任何更新。

若要檢視此策略的權限，請參閱AWS 受管理AWSSSODirectoryAdministrator的策略參考中的。

AWS 受管理的策略： AWSSSOReadOnly

您可將 `AWSSSOReadOnly` 政策連接到 IAM 身分。

此政策授予唯讀許可，允許使用者在 IAM 身分中心檢視資訊。附加此政策的主體無法直接檢視 IAM 身分中心使用者或群組。附加此政策的主體無法在 IAM 身分中心進行任何更新。例如，具有這些許可的主體可以檢視 IAM 身分中心設定，但無法變更任何設定值。

若要檢視此策略的權限，請參閱AWS 受管理AWSSSOReadOnly的策略參考中的。

AWS 受管理的策略： AWSSSODirectoryReadOnly

您可將 `AWSSSODirectoryReadOnly` 政策連接到 IAM 身分。

此政策授予唯讀許可，允許使用者在 IAM 身分中心檢視使用者和群組。附加此政策的主體無法檢視 IAM 身分中心指派、權限集、應用程式或設定。附加此政策的主體無法在 IAM 身分中心進行任何更新。例如，具有這些許可的主體可以檢視 IAM Identity Center 使用者，但無法變更任何使用者屬性或指派 MFA 裝置。

若要檢視此策略的權限，請參閱AWS 受管理AWSSSODirectoryReadOnly的策略參考中的。

AWS 受管理的策略： AWSIdentitySyncFullAccess

您可將 AWSIdentitySyncFullAccess 政策連接到 IAM 身分。

附加此原則的主參與者具有完整存取權限，可以建立和刪除同步設定檔、將同步設定檔與同步目標建立關聯或更新、建立、列出和刪除同步處理篩選器，以及開始或停止同步處理。

許可權詳細

若要檢視此策略的權限，請參閱AWS 受管理AWSIdentitySyncFullAccess的策略參考中的。

AWS 受管理的策略： AWSIdentitySyncReadOnlyAccess

您可將 AWSIdentitySyncReadOnlyAccess 政策連接到 IAM 身分。

此原則會授與唯讀權限，讓使用者檢視有關識別同步化設定檔、篩選器和目標設定的資訊。附加此原則的主體無法對同步處理設定進行任何更新。例如，具有這些權限的主體可以檢視識別同步處理設定，但無法變更任何設定檔或篩選器值。

若要檢視此策略的權限，請參閱AWS 受管理AWSIdentitySyncReadOnlyAccess的策略參考中的。

AWS 受管理的策略： AWSSSOServiceRolePolicy

您無法將該AWSSSOServiceRolePolicy政策附加到 IAM 身分。

此政策附加至服務連結角色，該角色允許 IAM Identity Center 委派和強制執行哪些使用者具有中特定 AWS 帳戶 的單一登入存取權限。 AWS Organizations啟用 IAM 時，會在組織 AWS 帳戶 內的所有角色中建立服務連結角色。IAM 身分中心也會在隨後新增至組織的每個帳戶中建立相同的服務連結角色。此角色可讓 IAM 身分中心代表您存取每個帳戶的資源。在每個角色中建立的服務連結角色 AWS 帳戶 都會命名為AWSServiceRoleForSSO。如需詳細資訊，請參閱 針對 IAM 身分中心使用服務連結角色。

AWS 受管理的策略： AWSIAMIdentityCenterAllowListForIdentityContext

假設具有 IAM 身分中心身分內容的角色時， AWS Security Token Service (AWS STS) 會自動將AWSIAMIdentityCenterAllowListForIdentityContext政策附加到該角色。

此政策提供當您將受信任的身分傳播與 IAM 身分中心身分內容中假定的角色搭配使用時所允許的動作清單。使用此前後關聯呼叫的所有其他動作都會遭到封鎖。身份上下文作為傳遞ProvidedContext。

若要檢視此策略的權限，請參閱AWS 受管理AWSIAMIdentityCenterAllowListForIdentityContext的策略參考中的。

IAM 身分中心更新受 AWS 管政策

下表說明自此服務開始追蹤這些變更以來，IAM 身分中心 AWS 受管政策的更新。如需有關此頁面變更的自動警示，請訂閱 IAM 身分中心文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包括支援 Amazon EMR 中受信任身分傳播的elasticmapreduce:DescribeStep 、、、和elasticmapreduce:ListSteps 動作。elasticmapreduce:AddJobFlowSteps elasticmapreduce:DescribeCluster elasticmapreduce:CancelSteps	2024年5月17日
AWSIAMIdentityCenterAllowListForIdentityContext	此原則現在包括qapps:CreateQApp 、、、、qapps:PredictProblemStatementFromConversation 、qapps:PredictQAppFromProblemStatement 、、qapps:CopyQApp 、、qapps:GetQApp 、qapps:ListQApps 、、qapps:UpdateQApp 、、qapps:DeleteQApp 、qapps:AssociateQAppWithUser 、、qapps:DisassociateQAppFromUser 、、qapps:ImportDocume	2024 年 4 月 30 日

變更	描述	日期
	ntToQApp 、qapps:ImportDocumentToQAppSession qapps:CreateLibraryItem 、和qapps:StopQAppSession 動作 qapps:GetLibraryItem qapps:UpdateLibraryItem qapps:CreateLibraryItemReview qapps:ListLibraryItems qapps:CreateSubscriptionToken qapps:StartQAppSession ，以支援支援這些工作階段的 AWS 受管理應用程式的身分識別感知主控台工作階段。	
AWSSSOMasterAccountAdministrator	此原則現在包含支援這些工signin:ListTrustedIdentityPropagationApplicationsForConsole 作階段之 AWS 受管理應用程式的身分識別感知主控台工作階段的signin:CreateTrustedIdentityPropagationApplicationForConsole 和動作。	2024年4月26日

變更	描述	日期
AWSSSOMemberAccountAdministrator	此原則現在包含支援這些工signin:ListTrustedIdentityPropagationApplicationsForConsole 作階段之 AWS 受管理應用程式的身分識別感知主控台工作階段的signin:CreateTrustedIdentityPropagationApplicationForConsole 和動作。	2024年4月26日
AWSSSOReadOnly	此原則現在包含支援這些工signin:ListTrustedIdentityPropagationApplicationsForConsole 作階段之 AWS 受管理應用程式的身分識別感知主控台工作階段的動作。	2024年4月26日
AWSIAMIdentityCenterAllowListForIdentityContext	此原則現在包含支援這些工qbusiness:PutFeedback 作階段之 AWS 受管理應用程式的身分識別感知主控台工作階段的動作。	2024年4月26日

變更	描述	日期
AWSIAMIdentityCenterAllowListForIdentityContext	此原則現在包含q:StartConversation 、、、、、q:SendMessage q:ListConversations 、和 q:UpdateTroubleshootingCommandResult 動作 q:GetConversation q:StartTroubleshootingAnalysis q:GetTroubleshootingResults q:StartTroubleshootingResolutionExplanation ，以支援這些工作階段的 AWS 受管理應用程式支援身分識別感知主控台工作階段。	2024年4月24日
AWSIAMIdentityCenterAllowListForIdentityContext	此原則現在包含支援這些工sts:SetContext 作階段之 AWS 受管理應用程式的身分識別感知主控台工作階段的動作。	2024年4月19 日
AWSIAMIdentityCenterAllowListForIdentityContext	此原則現在包含、、和qbusiness:DeleteConversation 動作 qbusiness:Chat qbusiness:ChatSync qbusiness:ListConversations qbusiness:ListMessages ，以支援這些工作階段的 AWS 受管理應用程式支援身分識別感知主控台工作階段。	2024年4月11日

變更	描述	日期
AWSIAMIdentityCenterAllowListForIdentityContext	此原則現在包含s3:GetAccessGrantsInstanceForPrefix 和s3:GetDataAccess 處理行動。	2023 年 11 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	此政策提供當您將受信任的身分傳播與 IAM 身分中心身分內容中假定的角色搭配使用時所允許的動作清單。	2023 年 11 月 15 日
AWSSSODirectoryReadOnly	此原則現在包含具有新權限identitystore-auth 的新命名空間，可讓使用者列出並取得工作階段。	2023 年 2 月 21 日
AWSSSOServiceRolePolicy	此原則現在允許對管理帳戶採取UpdateSAMLProvider 動作。	2022 年 10 月 20 日
AWSSSOMasterAccountAdministrator	此原則現在包含具有新權限identitystore-auth 的新命名空間，以允許管理員列出和刪除使用者的工作階段。	2022 年 10 月 20 日
AWSSSOMemberAccountAdministrator	此原則現在包含具有新權限identitystore-auth 的新命名空間，以允許管理員列出和刪除使用者的工作階段。	2022 年 10 月 20 日
AWSSSODirectoryAdministrator	此原則現在包含具有新權限identitystore-auth 的新命名空間，以允許管理員列出和刪除使用者的工作階段。	2022 年 10 月 20 日

變更	描述	日期
AWSSSOMasterAccountAdministrator	此原則現在包含新的撥ListDelegatedAdministrators入權限 AWS Organizations。此原則現在也包含一個權限子集AWSSSOManageDelegatedAdministrator，其中包含呼叫RegisterDelegatedAdministrator和的權限DeregisterDelegatedAdministrator。	2022 年 8 月 16 日
AWSSSOMemberAccountAdministrator	此原則現在包含新的撥ListDelegatedAdministrators入權限 AWS Organizations。此原則現在也包含一個權限子集AWSSSOManageDelegatedAdministrator，其中包含呼叫RegisterDelegatedAdministrator和的權限DeregisterDelegatedAdministrator。	2022 年 8 月 16 日
AWSSSOReadOnly	此原則現在包含新的撥ListDelegatedAdministrators入權限 AWS Organizations。	2022 年 8 月 11 日
AWSSSOServiceRolePolicy	此原則現在包含呼叫DeleteRolePermissionsBoundary和的新權限PutRolePermisionsBoundary。	2022 年 7 月 14 日

變更	描述	日期
AWSSSOServiceRolePolicy	此原則現在包含允許呼叫的`ListAWSServiceAccessForOrganization` and `ListDelegatedAdministrators` 新權限 AWS Organizations。	2022 年 5 月 11 日
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	新增 IAM 存取分析器許可，以允許主體使用政策檢查進行驗證。	2022 年 4 月 28 日
AWSSSOMasterAccountAdministrator	此政策現在允許所有 IAM 身分識別中心身分存放區服務動作。 如需 IAM 身分中心身分識別存放區服務中可用動作的相關資訊，請參閱 IAM 身分識別中心身分存放區 API 參考。	2022 年 3 月 29 日
AWSSSOMemberAccountAdministrator	此政策現在允許所有 IAM 身分識別中心身分存放區服務動作。	2022 年 3 月 29 日
AWSSSODirectoryAdministrator	此政策現在允許所有 IAM 身分識別中心身分存放區服務動作。	2022 年 3 月 29 日
AWSSSODirectoryReadOnly	此政策現在授予 IAM 身分中心身分識別存放區服務讀取動作的存取權。若要從 IAM 身分中心身分存放區服務擷取使用者和群組資訊，需要此存取權。	2022 年 3 月 29 日

變更	描述	日期
AWSIdentitySyncFullAccess	此原則允許完整存取身分識別同步權限。	2022 年 3 月 3 日
AWSIdentitySyncReadOnlyAccess	此原則會授與唯讀權限，讓主體檢視身分識別同步設定。	2022 年 3 月 3 日
AWSSSOReadOnly	此政策授予唯讀許可，允許主體檢視 IAM 身分中心組態設定。	2021 年 8 月 4 日
IAM 身分中心開始追蹤變更	IAM 身分中心開始追蹤 AWS 受管政策的變更。	2021 年 8 月 4 日

針對 IAM 身分中心使用服務連結角色

AWS IAM Identity Center 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 IAM 身分中心的唯一 IAM 角色類型。它是由 IAM 身分中心預先定義的，其中包含服務代表您呼叫其他服 AWS 務所需的所有許可。如需詳細資訊，請參閱 服務連結角色。

服務連結角色可讓您輕鬆設定 IAM 身分中心，因為您不必手動新增必要的許可。IAM 身分中心會定義其服務連結角色的許可，除非另有定義，否則只有 IAM 身分中心可以擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

IAM 身分中心的服務連結角色許可

IAM 身分中心使用名為的服務連結角色AWSServiceRoleForSSO來授與 IAM 身分中心許可，以代表您管理 AWS 資源，包括 IAM 角色、政策和 SAML IdP。

服 AWSServiceRoleForSSO 務連結角色會信任下列服務擔任該角色：

- `IAM Identity Center`

AWSServiceRoleForSSO 服務連結的角色許可政策允許身分識別中心針對路徑「/aws-保留 / sso.amazonaws.com/」路徑上的角色完成下列工作，且名稱前置詞為「_」：AWSReservedSSO

- iam:AttachRolePolicy
- iam:CreateRole
- iam:DeleteRole
- iam:DeleteRolePermissionsBoundary
- iam:DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetRole
- iam:ListRolePolicies
- iam:PutRolePolicy
- iam:PutRolePermissionsBoundary
- iam:ListAttachedRolePolicies

AWSServiceRoleForSSO 服務連結的角色許可政策允許 IAM 身分中心在名稱前綴為「AWSSSO_」的 SAML 提供者上完成以下操作：

- iam:CreateSAMLProvider
- iam:GetSAMLProvider
- iam:UpdateSAMLProvider
- iam:DeleteSAMLProvider

AWSServiceRoleForSSO 服務連結的角色許可政策允許 IAM 身分中心在所有組織上完成下列工作：

- organizations:DescribeAccount
- organizations:DescribeOrganization
- organizations:ListAccounts
- organizations:ListAWSServiceAccessForOrganization
- organizations:ListDelegatedAdministrators

AWSServiceRoleForSSO 服務連結角色許可政策允許 IAM 身分中心在所有 IAM 角色 (*) 上完成下列工作：

- iam:listRoles

AWSServiceRoleForSSO 服務連結的角色許可政策允許身分與存取權管理身分中心在「arn: aw: iam::: *: 角色/sso.amazonaws.com/」上完成下列項目：aws-service-roleAWSServiceRoleForSSO

- iam:GetServiceLinkedRoleDeletionStatus
- iam:DeleteServiceLinkedRole

角色許可政策允許 IAM 身分中心對資源完成以下動作。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"IAMRoleProvisioningActions",
         "Effect":"Allow",
         "Action":[
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:DeleteRolePermissionsBoundary",
            "iam:PutRolePermissionsBoundary",
            "iam:PutRolePolicy",
            "iam:UpdateRole",
            "iam:UpdateRoleDescription",
            "iam:UpdateAssumeRolePolicy"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ],
         "Condition":{
            "StringNotEquals":{
               "aws:PrincipalOrgMasterAccountId":"${aws:PrincipalAccount}"
            }
         }
      },
      {
         "Sid":"IAMRoleReadActions",
         "Effect":"Allow",
         "Action":[
            "iam:GetRole",
            "iam:ListRoles"
```

```
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"IAMRoleCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:ListRolePolicies",
            "iam:ListAttachedRolePolicies"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ]
      },
      {
         "Sid":"IAMSLRCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus",
            "iam:DeleteRole",
            "iam:GetRole"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
         ]
      },
      {
        "Sid": "IAMSAMLProviderCreationAction",
        "Effect": "Allow",
        "Action": [
          "iam:CreateSAMLProvider"
      ],
      "Resource": [
         "arn:aws:iam::*:saml-provider/AWSSSO_*"
       ],
      "Condition": {
         "StringNotEquals": {
```

```
            "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
          }
        }
      },
      {
        "Sid": "IAMSAMLProviderUpdateAction",
        "Effect": "Allow",
        "Action": [
          "iam:UpdateSAMLProvider"
        ],
        "Resource": [
           "arn:aws:iam::*:saml-provider/AWSSSO_*"
        ]
      },
      {
         "Sid":"IAMSAMLProviderCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteSAMLProvider",
            "iam:GetSAMLProvider"
         ],
         "Resource":[
            "arn:aws:iam::*:saml-provider/AWSSSO_*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "organizations:DescribeAccount",
            "organizations:DescribeOrganization",
            "organizations:ListAccounts",
            "organizations:ListAWSServiceAccessForOrganization",
            "organizations:ListDelegatedAdministrators"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowUnauthAppForDirectory",
         "Effect":"Allow",
         "Action":[
            "ds:UnauthorizeApplication"
         ],
```

```
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"AllowDescribeForDirectory",
            "Effect":"Allow",
            "Action":[
               "ds:DescribeDirectories",
               "ds:DescribeTrusts"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"AllowDescribeAndListOperationsOnIdentitySource",
            "Effect":"Allow",
            "Action":[
               "identitystore:DescribeUser",
               "identitystore:DescribeGroup",
               "identitystore:ListGroups",
               "identitystore:ListUsers"
            ],
            "Resource":[
               "*"
            ]
         }
      ]
}
```

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

為 IAM 身分中心建立服務連結角色

您不需要手動建立一個服務連結角色。啟用後，IAM 身分中心會在組織內的所有帳戶中建立服務連結角色。 AWS IAM 身分中心也會在隨後新增至組織的每個帳戶中建立相同的服務連結角色。此角色可讓 IAM 身分中心代表您存取每個帳戶的資源。

備註

- 如果您已登入 AWS Organizations 管理帳戶，則該帳戶會使用您目前登入的角色，而非服務連結角色。這樣可以防止權限升級。
- 當 IAM 身分中心在 AWS Organizations 管理帳戶中執行任何 IAM 操作時，所有操作都會使用 IAM 主體的登入資料進行。 CloudTrail 如此一來，登入可讓您查看管理帳戶中所有權限變更的使用者。

Important

如果您在 2017 年 12 月 7 日之前使用 IAM 身分中心服務，那麼當它開始支援服務連結角色時，IAM 身分中心就會在您的帳戶中建立該 AWSServiceRoleForSSO 角色。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。

編輯 IAM 身分中心的服務連結角色

IAM 身分中心不允許您編輯 AWSServiceRoleForSSO 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 IAM 身分中心的服務連結角色

您不需要手動刪除 AWSServiceRoleForSSO 角色。從 AWS 組織中移除時，IAM 身分中心會自動清除資源，並從該 AWS 帳戶資源中刪除服務連結角色。 AWS 帳戶

您也可以使用 IAM 主控台、IAM CLI 或 IAM API 手動刪除服務連結角色。若要執行此操作，您必須先手動清除服務連結角色的資源，然後才能手動刪除它。

Note

如果 IAM 身分中心服務在您嘗試刪除資源時使用該角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

若要刪除使用的 IAM 身分中心資源 AWSServiceRoleForSSO

1. 移除使用者和群組存取適用於所有具有存取權的使用者和群組 AWS 帳戶。
2. 刪除權限集您已與相關聯的 AWS 帳戶.

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台、IAM CLI 或 IAM API 刪除 AWSServiceRoleForSSO服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

IAM 身分識別中心主控台和 API 授權

現有的 IAM 身分識別中心主控台 API 支援雙重授權，可讓您在有更新的 API 可用時維持對現有 API 作業的使用。如果您擁有在 2023 年 11 月 15 日和 2020 年 10 月 15 日之前建立的 IAM 身分中心的現有執行個體，則可以使用下表判斷哪些 API 作業現在會對應至該日期之後發行的較新 API 作業。

主題

- 二零二三年十一月之後的空口
- 2020 年 10 月之後的 API 動作

二零二三年十一月之後的空口

在 2023 年 11 月 15 日之前建立的 IAM 身分中心執行個體，只要沒有明確拒絕任何動作，就會同時執行新舊的 API 動作。2023 年 11 月 15 日之後建立的執行個體會在 IAM 身分中心主控台中使用較新的 API 動作進行授權。

2023 年 11 月 15 日之前使用的主控台作業名稱	二 ○ 二三年十一月十五日之後使用的 API 動作
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance | CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance | DeleteManagedApplicationInstance	DeleteApplication

2023 年 11 月 15 日之前使用的主控台作業名稱	二○二三年十一月十五日之後使用的 API 動作
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments
UpdateApplicationInstanceDisplayData | UpdateApplicationInstanceStatus | UpdateManagedApplicationInstanceStatus	UpdateApplication

2020 年 10 月之後的 API 動作

在 2020 年 10 月 15 日之前建立的 IAM 身分中心執行個體，只要沒有明確拒絕任何動作，就會同時執行新舊的 API 動作。2020 年 10 月 15 日之後建立的執行個體會在 IAM 身分中心主控台中使用較新的 API 動作來進行授權。

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances | GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles | GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS IAM 身分中心的條件內容金鑰

當主體向其提出要求時 AWS，會將請求資訊 AWS 收集到要求前後關聯中，此內容可用來評估和授權請求。您可以使用 JSON 政策的 `Condition` 元素，來比較請求內容中的鍵和您在政策中指定的鍵值。請求信息由不同的來源提供，包括發出請求的主體，資源，對其發出的請求以及有關請求本身的元數據。服務特定的條件金鑰已定義為與個別 AWS 服務搭配使用。

IAM 身分中心包含內 AWS STS 容提供者，可讓 AWS 受管應用程式和第三方應用程式為 IAM 身分中心定義的條件金鑰新增值。這些金鑰包含在 IAM 角色中。當應用程式將權杖傳遞給時，就會設定索引鍵值 AWS STS。該應用程序以下列任一方式獲得它傳遞給 AWS STS 的令牌：

- 使用 IAM 身分中心進行身份驗證期間
- 與受信任的令牌發行者交換令牌以進行受信任的身份傳播後。在這種情況下，應用程序從受信任的令牌發行者獲取令牌，並從 IAM 身份中心將該令牌交換為令牌。

這些金鑰通常由與信任身分傳播整合的應用程式使用。在某些情況下，當金鑰值存在時，您可以在建立的 IAM 政策中使用這些金鑰來允許或拒絕許可。

例如，您可能想要根據的值提供對資源的條件式存取UserId。此值表示哪個 IAM 身分中心使用者正在使用此角色。這個例子類似於使用SourceId. 不過SourceId，與其不同的是，的值UserId 代表識別身分存放區中已驗證的特定使用者。該值存在於應用程序獲取然後傳遞給 AWS STS的令牌中。它不是可以包含任意值的通用字符串。

主題

- 身份存儲：UserId
- 身份存儲：IdentityStoreArn
- 身份中心：ApplicationArn
- 身份中心：CredentialId
- 身份中心：InstanceArn

身份存儲：UserId

此內容金鑰是 IAM 身分中心使用者UserId的身分識別中心使用者，該使用者是 IAM 身分中心發出的內容宣告的主題。上下文斷言被傳遞給 AWS STS。您可以使用此金鑰，將代表提出請求UserId的 IAM Identity Center 使用者與您在政策中指定之使用者的識別碼進行比較。

- 可用性 — 當使用 AWS CLI 或 AWS STS AssumeRole API 作業中的任何 AWS STS assume-role命令假設角色時，此金鑰會在設定由 IAM Identity Center 發出的內容宣告之後包含在請求內容中。
- 數據類型-字符串
- 值類型 - 單一值

身份存儲：IdentityStoreArn

此內容金鑰是身分存放區的 ARN，該身分存放區連接至發出內容宣告的 IAM 身分中心執行個體。它也是您可以在其中查詢屬性的識別身分存放區identitystore:UserID。您可以在原則中使用此金鑰來判斷是否identitystore:UserID來自預期的識別身分存放區 ARN。

- 可用性 — 當使用 AWS CLI 或 AWS STS AssumeRole API 作業中的任何 AWS STS assume-role命令假設角色時，此金鑰會在設定由 IAM Identity Center 發出的內容宣告之後包含在請求內容中。
- 數據類型 -ARN，字符串
- 值類型 - 單一值

身份中心：ApplicationArn

此內容金鑰是 IAM 身分中心向其發出內容宣告之應用程式的 ARN。您可以在原則中使用此金鑰來判斷是否`identitycenter:ApplicationArn`來自預期的應用程式。使用此金鑰可協助防止未預期的應用程式存取 IAM 角色。

- 可用性 — 此金鑰包含在 AWS STS `AssumeRole` API 作業的要求內容中。請求內容包括 IAM 身分中心發出的內容宣告。
- 數據類型 -ARN，字符串
- 值類型 - 單一值

身份中心：CredentialId

此內容金鑰是身分增強型角色認證的隨機識別碼，僅用於記錄。由於此索引鍵值無法預測，因此建議您不要將它用於原則中的內容宣告。

- 可用性 — 此金鑰包含在 AWS STS `AssumeRole` API 作業的要求內容中。請求內容包括 IAM 身分中心發出的內容宣告。
- 數據類型-字符串
- 值類型 - 單一值

身份中心：InstanceArn

此內容金鑰是 IAM 身分中心執行個體的 ARN，該執行個體針對. `identitystore:UserID` 您可以使用此金鑰來判斷`identitystore:UserID`和內容宣告是否來自預期的 IAM 身分中心執行個體 ARN。

- 可用性 — 此金鑰包含在 AWS STS `AssumeRole` API 作業的要求內容中。請求內容包括 IAM 身分中心發出的內容宣告。
- 數據類型 -ARN，字符串
- 值類型 - 單一值

IAM 身分中心中的記錄和監控

最佳實務是應該監控您的組織，以確保所做的變更都會記錄。這有助於您確保可以調查任何未預期的變更，並且可以復原不想要的變更。 AWS IAM Identity Center 目前支援兩種 AWS 服務，可協助您監視組織及其中發生的活動。

主題

使用記錄 IAM 身分識別中心 API 呼叫 AWS CloudTrail

AWS IAM Identity Center 與服務整合 AWS CloudTrail，可提供 IAM 身分中心中使用者、角色或服務所採取的動作記錄的 AWS 服務。 CloudTrail 將 IAM 身分中心的 API 呼叫擷取為事件。擷取的呼叫包括來自 IAM 身分中心主控台的呼叫，以及對 IAM 身分中心 API 作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 IAM 身分識別中心的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向 IAM Identity Center 提出的要求、提出請求的 IP 位址、提出請求的人員、提出要求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

主題

IAM 身分識別中心資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動在 IAM Identity Center 中發生時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以查看，搜索和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需您 AWS 帳戶的持續事件記錄 (包括 IAM 身分識別中心的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合

- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件和從多個帳戶接收 CloudTrail日誌文件

在您的中啟用 CloudTrail 記錄時 AWS 帳戶，對 IAM 身分中心動作進行的 API 呼叫會在記錄檔中追蹤。IAM 身分中心記錄會與其他 AWS 服務記錄一起寫入記錄檔中。 CloudTrail 根據時間週期和檔案大小決定何時建立和寫入新檔案。

支援下列 IAM 身分中心 CloudTrail 作業：

主控台 API 作業	公有 API 操作
AssociateDirectory	AttachManagedPolicyToPermissionSet
AssociateProfile	CreateAccountAssignment
BatchDeleteSession	CreateInstanceAccessControlAttributeConfiguration
BatchGetSession	CreatePermissionSet
CreateApplicationInstance	DeleteAccountAssignment
CreateApplicationInstanceCertificate	DeleteInlinePolicyFromPermissionSet
CreatePermissionSet	DeleteInstanceAccessControlAttributeConfiguration
CreateProfile	DeletePermissionSet
DeleteApplicationInstance	DescribeAccountAssignmentCreationStatus
DeleteApplicationInstanceCertificate	DescribeAccountAssignmentDeletionStatus
DeletePermissionsPolicy	DescribeInstanceAccessControlAttributeConfiguration

主控台 API 作業	公有 API 操作
DeletePermissionSet	DescribePermissionSet
DeleteProfile	DescribePermissionSetProvisioningStatus
DescribePermissionsPolicies	DetachManagedPolicyFromPermissionSet
DisassociateDirectory	GetInlinePolicyForPermissionSet
DisassociateProfile	ListAccountAssignmentCreationStatus
GetApplicationInstance	ListAccountAssignmentDeletionStatus
GetApplicationTemplate	ListAccountAssignments
GetMfaDeviceManagementForDirectory	ListAccountsForProvisionedPermissionSet
GetPermissionSet	ListInstances
GetSSOStatus	ListManagedPoliciesInPermissionSet
ImportApplicationInstanceServiceProviderMetadata	ListPermissionSetProvisioningStatus
ListApplicationInstances	ListPermissionSets
ListApplicationInstanceCertificates	ListPermissionSetsProvisionedToAccount
ListApplicationTemplates	ListTagsForResource
ListDirectoryAssociations	ProvisionPermissionSet

主控台 API 作業	公有 API 操作
ListPermissionSets	PutInlinePolicyToPermissionSet
ListProfileAssociations	TagResource
ListProfiles	UntagResource
ListSessions	UpdateInstanceAccessControlAttributeConfiguration
PutMfaDeviceManagementForDirectory	UpdatePermissionSet
PutPermissionsPolicy	
StartSSO	
UpdateApplicationInstanceActiveCertificate	
UpdateApplicationInstanceDisplayData	
UpdateApplicationInstanceServiceProviderConfiguration	
UpdateApplicationInstanceStatus	
UpdateApplicationInstanceResponseConfiguration	
UpdateApplicationInstanceResponseSchemaConfiguration	
UpdateApplicationInstanceSecurityConfiguration	
UpdateDirectoryAssociation	

主控台 API 作業	公有 API 操作
UpdateProfile	

如需 IAM 身分中心公開 API 作業的詳細資訊，請參閱 IAM 身分中心 API 參考指南。

支援下列 IAM 身分識別中心身分存放區 CloudTrail 作業：

- AddMemberToGroup
- CompleteVirtualMfaDeviceRegistration
- CompleteWebAuthnDeviceRegistration
- CreateAlias
- CreateExternalIdPConfigurationForDirectory
- CreateGroup
- CreateUser
- DeleteExternalIdPConfigurationForDirectory
- DeleteGroup
- DeleteMfaDeviceForUser
- DeleteUser
- DescribeDirectory
- DescribeGroups
- DescribeUsers
- DisableExternalIdPConfigurationForDirectory
- DisableUser
- EnableExternalIdPConfigurationForDirectory
- EnableUser
- GetAWSSPConfigurationForDirectory
- ListExternalIdPConfigurationsForDirectory
- ListGroupsForUser
- ListMembersInGroup
- ListMfaDevicesForUser
- PutMfaDeviceManagementForDirectory

- RemoveMemberFromGroup
- SearchGroups
- SearchUsers
- StartVirtualMfaDeviceRegistration
- StartWebAuthnDeviceRegistration
- UpdateExternalIdPConfigurationForDirectory
- UpdateGroup
- UpdateMfaDeviceForUser
- UpdatePassword
- UpdateUser
- VerifyEmail

支援下列 IAM 身分中心 OIDC CloudTrail 動作：

- CreateToken
- RegisterClient
- StartDeviceAuthorization

支援下列 IAM 身分中心入口網站 CloudTrail 動作：

- Authenticate
- Federate
- ListApplications
- ListProfilesForApplication
- ListAccounts
- ListAccountRoles
- GetRoleCredentials
- Logout

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 請求是以根使用者還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。

- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

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

了解 IAM 身分中心記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示 IAM 身分中心主控台中發生之系統管理員 (samadams@example.com) 的 CloudTrail 記錄項目：


```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"08966example",
            "accessKeyId":"AKIAIIJM2K4example",
            "userName":"samadams"
         },
         "eventTime":"2017-11-29T22:39:43Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"DescribePermissionsPolicies",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":{
            "permissionSetId":"ps-79a0dde74b95ed05"
         },
         "responseElements":null,
         "requestID":"319ac6a1-d556-11e7-a34f-69a333106015",
         "eventID":"a93a952b-13dd-4ae5-a156-d3ad6220b071",
         "readOnly":true,
         "resources":[
```

```
         ],
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```

下列範例顯示在 AWS 存取 CloudTrail 入口網站中發生之一般使用者 (bobsmith@example.com) 動作的記錄項目：

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"Unknown",
            "principalId":"example.com//
S-1-5-21-1122334455-3652759393-4233131409-1126",
            "accountId":"08966example",
            "userName":"bobsmith@example.com"
         },
         "eventTime":"2017-11-29T18:48:28Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"ListApplications",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":null,
         "responseElements":null,
         "requestID":"de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
         "eventID":"e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```

下列範例顯示 IAM 身分中心 OIDC 中發生之使用者 (bobsmith@example.com) 動作的 CloudTrail 記錄項目：

```
{
```

```
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "Unknown",
        "principalId": "example.com//S-1-5-21-1122334455-3652759393-4233131409-1126",
        "accountId": "08966example",
        "userName": "bobsmith@example.com"
      },
      "eventTime": "2020-06-16T01:31:15Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "CreateToken",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "clientId": "clientid1234example",
        "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "grantType": "urn:ietf:params:oauth:grant-type:device_code",
        "deviceCode": "devicecode1234example"
      },
      "responseElements": {
        "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "tokenType": "Bearer",
        "expiresIn": 28800,
        "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
      "readOnly": false,
      "resources": [
        {
          "accountId": "08966example",
          "type": "IdentityStoreId",
          "ARN": "d-1234example"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "08966example"
}
```

了解 IAM 身分中心登入事件

AWS CloudTrail 記錄所有 AWS IAM Identity Center 身分識別來源的成功和失敗的登入事件。原生 SSO 和 Active Directory (AD Connector 和 AWS Managed Microsoft AD) 來源的身分識別會包含其他登入事件，這些事件會在每次提示使用者解決特定認證挑戰或因素時擷取，以及該特定認證驗證要求的狀態。只有在使用者完成所有必要的認證挑戰之後，使用者才會登入，這會導致`UserAuthentication`事件被記錄。

下表擷取每個 IAM 身分中心登入 CloudTrail 事件名稱、其用途，以及對不同身分識別來源的適用性。

事件名稱	事件目的	身分識別來源適用性
`CredentialChallenge`	用於通知 IAM 身分中心已要求使用者解決特定的憑證挑戰，並指定所需`CredentialType` 的資料 (例如 PASSWORD 或 TOTP)。	原生 IAM 身分中心使用者、AD Connector 和 AWS Managed Microsoft AD
`CredentialVerification`	用來通知使用者已嘗試解決特定`CredentialChallenge` 要求，並指定該認證是成功還是失敗。	原生 IAM 身分中心使用者、AD Connector 和 AWS Managed Microsoft AD
`UserAuthentication`	用於通知使用者受到挑戰的所有驗證需求都已成功完成，且使用者已成功登入。未能成功完成所需認證挑戰的使用者將導致不會記錄任何*`UserAuthentication`* 事件。	所有識別來源

下表擷取特定登入 CloudTrail 事件中包含的其他有用事件資料欄位。

事件名稱	事件目的	登入事件適用性	範例值
AuthWorkflowID	用來關聯整個登入序列中發出的所有事件。對於每個使用者登入，IAM 身分中心可能會發出多個事件。	CredentialChallenge，CredentialVerification，UserAuthentication	「AuthWorkflow識別碼」：「9de74b32-8362-4a01-524」
CredentialType	用於指定受到挑戰的認證或因素。 UserAuthentication 事件將包含在使用者登入順序中成功驗證的所有CredentialType 值。	CredentialChallenge，CredentialVerification，UserAuthentication	CredentialType「:「密碼」或「」:CredentialType「密碼, TOTP」(可能的值包括:密碼, TOTP, 網絡驗證, 外部 IDP, 重新輸出)
DeviceEnrollmentRequired	用於指定使用者在登入期間必須註冊 MFA 裝置，以及使用者成功完成該要求。	UserAuthentication	「DeviceEnrollmentRequired「：「真實的」
LoginTo	用於指定成功登入順序後的重新導向位置。	UserAuthentication	LoginTo「:" https://mydirectory.awsapps.com/start/...」

IAM 身分中心登入案例的範例事件

下列範例顯示不同登入案例的預期 CloudTrail 事件順序。

主題

- 僅使用密碼驗證時成功登入
- 使用外部身分識別提供者驗證時成功登入
- 使用密碼和 TOTP 身份驗證器應用程序進行身份驗證時成功登錄
- 使用密碼進行身份驗證並強制 MFA 註冊時需要成功登錄

- 僅使用密碼驗證時登入失敗

僅使用密碼驗證時成功登入

下列事件序列會擷取僅密碼成功登入的範例。

CredentialChallenge (密碼)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:33:58Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

成功 CredentialVerification (密碼)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


成功 UserAuthentication (僅限密碼)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
```

```
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


使用外部身分識別提供者驗證時成功登入

下列事件序列會擷取使用外部身分識別提供者透過 SAML 通訊協定驗證時成功登入的範例。

成功 UserAuthentication (外部身分識別提供者)


```
{
```

```
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":""
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"EXTERNAL_IDP"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


使用密碼和 TOTP 身份驗證器應用程序進行身份驗證時成功登錄

下列事件順序會擷取登入期間需要多重要素驗證，且使用者使用密碼和 TOTP 驗證器應用程式成功登入的範例。

CredentialChallenge (密碼)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:13Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
   "eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


成功 CredentialVerification (密碼)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
```

```
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


CredentialChallenge (TOTP)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
```

```
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


成功 CredentialVerification (TOTP)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
```

```
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

成功 UserAuthentication (密碼 + TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
```

```
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFfO01O8qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMlui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD,TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


使用密碼進行身份驗證並強制 MFA 註冊時需要成功登錄

下列事件序列會擷取密碼成功登入的範例，但使用者必須在完成登入之前成功完成註冊 MFA 裝置。

CredentialChallenge (密碼)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:02Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
```

```
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
   "eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

成功 CredentialVerification (密碼)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
   "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
```

```
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

成功 UserAuthentication (密碼 + 需要 MFA 註冊)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:14Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HLlN2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY EgU3fhOL3QWvWiquYnDPMyPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi5OYI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD",
      "DeviceEnrollmentRequired":"true"
```

```
   },
   "requestID":"74d24604-a365-4237-8c4a-350795494b92",
   "eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

僅使用密碼驗證時登入失敗

下列事件序列會擷取僅限密碼登入失敗的範例。

CredentialChallenge (密碼)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:15Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
   "eventID":"d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
```

```
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

失敗 CredentialVerification (密碼)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:21Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
   "eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
```

```
        "CredentialVerification":"Failure"
    }
}
```

Amazon EventBridge

IAM 身分中心可以與 Amazon EventBridge 合作，在組織中發生管理員指定的動作時引發事件。例如，由於這類動作的靈敏度，多數管理員會想要在每次有人在組織中建立新帳戶，或在成員帳戶的管理員嘗試離開組織時收到警告。您可以設定尋找這些動作的 EventBridge 規則，然後將產生的事件傳送至管理員定義的目標。目標可以是傳送電子郵件或文字訊息給其訂閱者的 Amazon SNS 主題。您也可以建立記錄動作詳細資訊的 AWS Lambda 函數，以供日後檢閱。

要進一步了解 EventBridge，包括如何設定和啟用它，請參閱 Amazon EventBridge 使用者指南。

記錄 AD 同步和可設定的 AD 同步錯誤

您可以在 Active Directory (AD) 同步處理和可設定的 AD 同步設定上啟用記錄，以接收記錄檔，其中包含同步處理程序期間可能發生之錯誤的相關資訊。使用這些記錄檔，您可以監控 AD 同步處理和可設定 AD 同步處理是否有問題，並採取適用的動作。您可以將日誌傳送到 Amazon CloudWatch 日誌日誌群組、亞馬遜簡單儲存服務 (Amazon S3) 儲存貯體或 Amazon 資料防火軟管 (支援 Amazon S3 儲存貯體和 Firehose 的跨帳戶交付)。

如需有關限制、權限和付費記錄檔的詳細資訊，請參閱啟用記錄來源 AWS 服務。

> **Note**
>
> 系統會向您收取記錄費用。如需詳細資訊，請參閱 Amazon CloudWatch 定價頁面上的付費日誌。

啟用 AD 同步和可設定的 AD 同步錯誤記錄

1. 登入 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上，選擇 [身分識別來源] 索引標籤，選擇 [動作]，然後選擇 [管理記錄檔
4. 選擇 [新增記錄傳送] 和下列其中一個目的地類型。

    a. 選擇 Amazon CloudWatch 日誌。然後選擇或輸入目的地記錄群組。

b. 選擇 Amazon S3。然後選擇或輸入目標值區。

c. 選擇「到 Firehose」。然後選擇或輸入目的地傳送串流。

5. 選擇提交。

停用 AD 同步和可設定的 AD 同步錯誤記錄

1. 登入 IAM 身分中心主控台。
2. 選擇設定。
3. 在 [設定] 頁面上，選擇 [身分識別來源] 索引標籤，選擇 [動作]，然後選擇 [管理記錄檔
4. 選擇 [移除] 做為您要移除的目的地。
5. 選擇提交。

AD 同步處理和可設定 AD 同步錯誤記錄欄位

如需可能的錯誤記錄欄位，請參閱下列清單。

`sync_profile_name`

同步設定檔的名稱。

`error_code`

代表發生錯誤類型的錯誤代碼。

`error_message`

包含所發生錯誤之詳細資訊的訊息。

`sync_source`

同步來源是實體正在同步的來源。對於 IAM 身分中心，這是由管理的作用中目錄 (AD) AWS Directory Service。同步來源包含受影響目錄的網域和 ARN。

`sync_target`

同步目標是儲存實體的目的地。對於 IAM 身分中心，這是身分識別存放區。同步目標包含受影響的識別存放區 ARN。

`source_entity_id`

造成錯誤之實體的唯一識別碼。對於 IAM 身分中心，這是實體的 SID。

`source_entity_type`

造成錯誤的實體類型。此值可以為 USER 或 GROUP。

`eventTimestamp`

錯誤發生時的時間戳記。

AD 同步和可設定的 AD 同步錯誤記錄範例

範例 1：AD 目錄的過期密碼的錯誤記錄

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "InvalidDirectoryCredentials",
        "error_message": "The password for your AD directory has expired. Please reset
 the password to allow Identity Sync to access the directory."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "eventTimestamp": "1683355579981"
}
```

範例 2：使用非唯一使用者名稱的使用者錯誤記錄

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "ConflictError",
        "error_message": "The source entity has a username conflict with the sync
 target. Please verify that the source identity has a unique username in the target."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "sync_target": {
        "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
    },
```

```
    "source_entity_id": "SID-1234",
    "source_entity_type": "USER",
    "eventTimestamp": "1683355579981"
}
```

IAM 身分中心的合規驗證

協力廠商稽核人員會評估其安全性與合規性， AWS 服務 例 AWS IAM Identity Center 如多個 AWS 法規遵循計畫的一部分。

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 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：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 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AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。

- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求，例如 PCI DSS，滿足特定合規性架構所規定的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

支援的合規標準

IAM 身分中心已針對下列標準進行稽核，並有資格作為取得合規認證所需解決方案的一部分使用。

AWS 已擴大其《Health 保險可攜性與責任法案》(HIPAA) 合規計畫，將 IAM 身分中心納入 HIPAA 合格服務。

AWS 針對想要深入瞭解如何使 AWS 服務 用處理和儲存健康資訊的客戶，提供 HIPAA 重點白皮書。如需詳細資訊，請參閱 HIPAA 合規。

資訊安全註冊評估員計畫 (IRAP) 讓澳洲政府的客戶能夠確保制定適當的法規遵循管制，並決定適當的責任模式，以滿足澳洲政府資訊安全手冊 (ISM) 由澳洲網路安全中心 (ACSC) 製作的要求。如需詳細資訊，請參閱 IRAP 資源。

IAM 身分中心在服務提供者等級 1 中提供支付卡產業 (PCI) 資料安全標準 (DSS) 3.2 版的合規證明。

使用 AWS 產品和服務來儲存、處理或傳輸持卡人資料的客戶，可以在 IAM 身分中心使用下列身分識別來源來管理自己的 PCI DSS 合規認證：

- Active Directory
- 外部識別提供者

	IAM 身分中心身分識別來源目前不符合 PCI DSS 規範。 如需 PCI DSS 的詳細資訊，包括如何要求 AWS PCI 合規性 Package 的副本，請參閱 PCI DSS 等級 1。
	系統與組織控制 (SOC) 報告是獨立的第三方檢查報告，展示 IAM Identity Center 如何實現關鍵的合規性控制和目標。這些報告可協助您和稽核人員瞭解控制項如何支援作業與法規遵循。SOC 報告有三種類型： • AWS SOC 1 報告-使用 AWS Artifact 下載 • AWS SOC 2：安全性、可用性和機密性報告-使用 AWS Artifact 下載 • AWS SOC 3：安全性、可用性和機密性報告 IAM 身分識別中心適用於 AWS SOC 1、SOC 2 和 SOC 3 報告。如需詳細資訊，請參閱 SOC 合規。

IAM 身分中心的彈性

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠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。

如需區域和可用區域的詳 AWS 細資訊，請參閱AWS 全域基礎結構。

若要進一步了解 AWS IAM Identity Center 復原能力，請參閱彈性設計和區域行為。

IAM 身分中心的基礎設施安全

作為託管服務， AWS IAM Identity Center 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透過網路存取 IAM 身分中心。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。

- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

標記 AWS IAM Identity Center 資源

標籤是一個自訂屬性標籤，您可將其新增到 AWS 資源以便輕鬆地識別、組織和搜尋資源。每個標籤有兩個部分：

- 標籤鍵 (例如，CostCenter、Environment 或 Project)。標籤鍵最大長度為 128 個字元且區分大小寫。
- 標籤值 (例如 111122223333 或 Production)。標籤值最大長度為 256 個字元，且與標籤鍵一樣需要區分大小寫。您可以將標籤的值設為空白字串，但您無法將標籤的值設為 Null。忽略標籤值基本上等同於使用空字串。

標籤可協助您識別和整理 AWS 資源。許多 AWS 服務支援標記，因此您可以將相同標籤指派給不同服務的資源，以表示相關資源。例如，您可以將相同的標籤指派給 IAM 身分中心執行個體中的特定權限集。如需有關標記策略的詳細資訊，請參閱AWS 一般參考指南中的標記AWS資源和標記最佳實務。

除了使用標籤識別、組織和追蹤AWS資源之外，您還可以在 IAM 政策中使用標籤來協助控制誰可以檢視您的資源並與之互動。若要進一步了解如何使用標籤來控制存取權限，請參閱 IAM 使用者指南中的使用標籤控制AWS資源的存取。例如，您可以允許使用者更新 IAM 身分中心權限集，但前提是 IAM 身分中心權限集的owner標籤值為該使用者名稱。

目前，您只能將標籤套用至權限集。您無法將標籤套用至 IAM 身分中心建立的對應角色AWS 帳戶。您可以使用 IAM 身分中心主控台AWS CLI或 IAM 身分中心 API 來新增、編輯或刪除權限集的標籤。

以下各節提供 IAM 身分中心標籤的詳細資訊。

標籤限制

下列基本限制適用於 IAM 身分中心資源上的標籤：

- 您可以指派給資源的標籤數目上限為 50。
- 鍵長度上限為 128 個 Unicode 字元。
- 值長度上限為 256 個 Unicode 字元。
- 標籤鍵和值的有效字元如下：

  a-z、A-Z、0-9、空格及下列字元：_.:/= +-和 @
- 金鑰和值會區分大小寫。

- 請不要使用 aws: 做為鍵的字首；它已保留供 AWS 使用

使用 IAM 身分中心主控台管理標籤

您可以使用 IAM 身分中心主控台新增、編輯和移除與執行個體或權限集相關聯的標籤。

管理 IAM 身分中心主控台的權限集標籤

1. 開啟 IAM 身分中心主控台。
2. 選擇權限集。
3. 選擇具有您要管理之標籤的權限集名稱。
4. 在 [權限] 索引標籤的 [標籤] 下，執行下列其中一個動作，然後繼續進行下一個步驟：
   a. 如果已為此權限集指派標籤，請選擇 [編輯標籤]。
   b. 如果沒有指派任何標籤給此權限集，請選擇 [新增標記]。
5. 對於每個新標籤，在「鍵」和「值」(可選) 欄中輸入值。完成時，請選擇 Save changes (儲存變更)。

若要移除標記，請在您要移除的標籤旁邊的「移除」欄中選擇 X。

管理 IAM 身分中心執行個體的標籤

1. 開啟 IAM 身分中心主控台。
2. 選擇設定。
3. 選擇 Tags (標籤) 索引標籤。
4. 針對每個標籤，在「機碼」和「值」(選用) 欄位中輸入值。完成後，請選擇「新增標籤」按鈕。

若要移除標記，請選擇您要移除的標記旁邊的「移除」按鈕。

AWS CLI 範例

提AWS CLI供可用來管理指派給權限集之標籤的命令。

指派標籤

使用下列命令將標籤指派給您的權限集。

Example **tag-resource**權限集的指令

在命令集tag-resource中使用，將標籤指派給權限sso集：

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test
```

此命令包括下列參數：

- instance-arn— 將在其下執行作業的 IAM 身分中心執行個體的 Amazon 資源名稱 (ARN)。
- resource-arn-帶有要列出標籤的資源的 ARN。
- tags – 標籤的鍵值組。

若要一次指派多個標籤，請以逗號分隔清單指定這些標籤：

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

檢視標籤

使用下列命令來檢視已指派給權限集的標籤。

Example **list-tags-for-resource**權限集的指令

使list-tags-for-resource用下列命令集來檢視指派給權限sso集的標籤：

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

移除標籤

使用下列命令從權限集中移除標籤。

Example **untag-resource**權限集的指令

使用以下命令集中移除權限sso集untag-resource中的標籤：

```
$ aws sso-admin untag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tag-keys Stage CostCenter Owner
```

處理 `--tag-keys` 參數時，請指定一或多個標籤金鑰，且不要包含標籤值。

建立權限集時套用標籤

建立權限集時，請使用下列指令來指派標籤。

Example 搭配標籤的 **`create-permission-set`** 命令

使用`create-permission-set`命令建立權限集時，您可以使用以下`--tags`參數指定標籤：

```
$ aws sso-admin create-permission-set \
> --instance-arn sso-instance-arn \
> --name permission=set-name \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

使用 IAM 身分中心 API 管理標籤

您可以在 IAM 身分中心 API 中使用下列動作來管理權限集的標籤。

IAM 身分中心執行個體標籤的 API 動作

使用下列 API 動作來指派、檢視和移除 IAM 身分中心權限集或執行個體的標籤。

- TagResource
- ListTagsForResource
- UntagResource
- CreatePermissionSet
- CreateInstance

整合AWS使用 IAM 身分識別中心的 CLI

AWS命令列介面 (CLI) 第 2 版與 IAM 身分中心整合，可簡化登入程序。開發人員可以直接登入AWS CLI使用他們通常用來登入 IAM 身分中心以及存取其指派的帳戶和角色的相同 Active Directory 或身分識別中心登入資料。例如，在系統管理員將 IAM 身分中心設定為使用 Active Directory 進行驗證之後，開發人員可以登入AWS CLI直接使用 Active Directory 登入資料。

AWSCLI 與 IAM 身分中心整合可提供下列優點：

- 企業可以讓他們的開發人員使用 IAM 身分中心或 Active Directory 中的登入資料登入，方法是將 IAM 身分中心連線到他們的 Active DirectoryAWS Directory Service。
- 開發人員可以從 CLI 登入以加快存取速度。
- 開發人員可以列出並在已指派存取權的帳戶和角色之間進行切換。
- 開發人員可以在其 CLI 組態中自動產生並儲存具名的角色設定檔，並在 CLI 中參照這些設定檔，以便在所需帳戶和角色中執行命令。
- CLI 會自動管理短期認證，因此開發人員可以在不中斷的情況下安全地啟動並停留在 CLI 中，並執行長時間執行的指令碼。

整合的方式AWS使用 IAM 身分識別中心的 CLI

若要使用 AWS for WordPressAWSCLI 與 IAM 身分中心整合，您需要下載、安裝和設定AWS Command Line Interface版本 2。有關如何下載和集成的詳細步驟AWS CLI使用 IAM 身分中心，請參閱設定AWS使用 IAM 身分識別中心的 CLI中的AWS Command Line Interface使用者指南。

AWS IAM Identity Center 區域可用性

IAM 身分中心提供多種常用的功能 AWS 區域。此可用性可讓您更輕鬆地設定使用者對多個 AWS 帳戶和商務應用程式的存取權限。當您的使用者登入 AWS 存取入口網站時，他們可以選取 AWS 帳戶 他們有權限的對象，然後存取 AWS Management Console. 如需 AWS 區域 該 IAM 身分中心支援的完整清單，請參閱 IAM 身分中心端點和配額。

IAM 身分識別中心區域資料

當您首次啟用 IAM 身分中心時，您在 IAM 身分中心設定的所有資料都會儲存在您設定的區域中。此資料包括目錄組態、權限集、應用程式執行個體，以及 AWS 帳戶 應用程式的使用者指派。如果您使用 IAM 身分中心身分識別存放區，您在 IAM 身分中心建立的所有使用者和群組也會儲存在相同的區域中。我們建議您將 IAM 身分中心安裝在想要保留供使用者使用的區域，而不是您可能需要停用的區域。

AWS Organizations 一 AWS 區域 次只支援一個。若要在不同區域中啟用 IAM 身分中心，您必須先刪除目前的 IAM 身分中心組態。切換至不同區域也會變更 AWS 存取入口網站的 URL，而且您必須重新設定所有權限集和指派。

跨區域通話

IAM 身分識別中心使用 Amazon Simple Email Service (Amazon SES)，在使用者嘗試使用一次性密碼 (OTP) 作為第二個身份驗證因素登入時，傳送電子郵件給最終使用者。這些電子郵件也會針對特定的身分識別和認證管理事件傳送，例如邀請使用者設定初始密碼、驗證電子郵件地址，以及重設密碼時。Amazon SES 可在 AWS 區域 該 IAM 身分中心支援的子集中使用。

IAM 身分中心在本機提供 Amazon SES 時，會呼叫 Amazon SES 本機端點 AWS 區域。當 Amazon SES 無法在本機使用時，IAM 身分中心會以不同的方式呼叫 Amazon SES 端點 AWS 區域，如下表所示。

下表列出了 Amazon SES 區域代碼。

IAM 身分識別中心區域代碼	IAM 身分識別中心區域名稱	Amazon SES 區域代碼	Amazon SES 區域名稱
us-gov-east-1	AWS GovCloud (美國東部)	us-gov-west-1	AWS GovCloud (美國西部)

IAM 身分識別中心區域代碼	IAM 身分識別中心區域名稱	Amazon SES 區域代碼	Amazon SES 區域名稱
ap-east-1	亞太區域 (香港)	ap-northeast-2	亞太區域 (首爾)
ap-southeast-4	亞太區域 (墨爾本)	ap-southeast-2	亞太區域 (悉尼)
ap-south-2	亞太區域 (海德拉巴)	ap-south-1	亞太區域 (孟買)
eu-central-2	歐洲 (蘇黎世)	eu-central-1	歐洲 (法蘭克福)
eu-south-2	歐洲 (西班牙)	eu-west-3	Europe (Paris)
me-central-1	中東 (阿拉伯聯合大公國)	eu-central-1	歐洲 (法蘭克福)

在這些跨區域呼叫中，IAM 身分中心可能會傳送下列使用者屬性：

- 電子郵件地址
- 名字
- 姓氏
- 中的帳戶 AWS Organizations
- AWS 存取入口網站 URL
- 使用者名稱
- 目錄 ID
- 使用者 ID

在選擇加入的區域中管理 IAM 身分中心 (預設為停用的區域)

根據預設，大部分服務都 AWS 區域 會啟用所有 AWS 服務的作業。那些 區域會自動啟用，以便與 IAM 身分中心搭配使用。以下 AWS 區域 是選擇加入的區域，您必須啟用它們：

- 非洲 (開普敦)
- Asia Pacific (Hong Kong)
- 亞太區域 (雅加達)
- 亞太區域 (墨爾本)

- 亞太區域 (海德拉巴)
- 歐洲 (米蘭)
- 歐洲 (蘇黎世)
- 歐洲 (西班牙)
- 以色列 (特拉維夫)
- Middle East (Bahrain)
- 中東 (阿拉伯聯合大公國)

當您在選擇加入的管理帳戶啟用 IAM 身分中心時 AWS 區域，任何成員帳戶的下列 IAM 身分中心中繼資料都會儲存在該區域中。

- 帳戶 ID
- 帳戶名稱
- 帳戶電郵
- IAM 身分中心在成員帳戶中建立的 IAM 角色的 Amazon 資源名稱 (ARN)

如果停用安裝 IAM 身分中心的區域，IAM 身分中心也會停用。在某個區域停用 IAM 身分中心之後，該區域的使用者將無法對應用程式進行單一登入 AWS 帳戶 存取權。 AWS 在您的 IAM 身分中心組態中保留資料至少 10 天。如果您在此時間範圍內重新啟用 IAM 身分中心，您的 IAM 身分中心組態資料仍可在該區域中使用。

若要在選擇加入時重新啟用 IAM 身分中心 AWS 區域，您必須重新啟用該區域。由於 IAM 身分中心必須重新處理所有暫停的事件，因此重新啟用 IAM 身分中心可能需要一些時間。

> **Note**
>
> IAM 身分中心只能管理已啟用在 AWS 區域. AWS 帳戶 若要管理組織中所有帳戶的存取權，請在自動啟用的管理帳戶中啟用 IAM 身分中心 AWS 區域 ，以便與 IAM 身分中心搭配使用。

如需啟用與停用的詳細資訊 AWS 區域，請參閱AWS 一般參考 AWS 區域中的管理。

刪除您的 IAM 身分中心組態

刪除 IAM 身分中心組態時，該組態中的所有資料都會遭到刪除，且無法復原。下表說明根據 IAM 身分中心目前設定的目錄類型刪除哪些資料。

什麼數據被刪除	連線的目錄 (AWS Managed Microsoft AD 或 AD Connector)	IAM 身分中心身分存放區
您已設定的所有權限集 AWS 帳戶	✓	✓
您在 IAM 身分中心設定的所有應用程式	✓	✓
您已為其設定的所有使用者指派 AWS 帳戶 和應用程式	✓	✓
目錄或存放區中的所有使用者和群組	無	✓

當您需要刪除目前的 IAM 身分中心組態時，請遵循下列程序。

刪除您的 IAM 身分中心組態

1. 開啟 IAM 身分中心主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 在 [設定] 頁面上，選擇 [管理] 索引標籤。
4. 在 [刪除 IAM 身分中心設定] 區段中，選擇 [刪除]。
5. 在 [刪除 IAM 身分中心設定] 對話方塊中，選取每個核取方塊，以確認您瞭解將刪除的資料。在文字方塊中輸入您的 IAM 身分中心執行個體，然後選擇 [確認]。

AWS IAM Identity Center 配額

下表說明 IAM 身分中心內的配額。配額增加要求必須來自管理或委派的系統管理員帳戶。若要增加配額，請參閱要求增加配額。

> **Note**
>
> 如果您擁有超過 50,000 個使用者、10,000 個群組或 500 個權限集，建議您使用 AWS CLI 和 API。如需 CLI 的詳細資訊，請參閱整合AWS使用 IAM 身分識別中心的 CLI。如需 API 的詳細資訊，請參閱歡迎使用 IAM 身分中心 API 參考。

應用配額

資源	預設配額	可以提高
服務供應商 SAML 憑證 (PEM 格式) 的檔案大小	2 KB	否
SAML 判斷提示限制	5 萬個字元	否
上傳至 IAM 身分中心的 IdP 憑證檔案大小限制	新角色 UTF-8	否
各應用程式存取範圍	25	否

AWS 帳戶 配額

資源	預設配額	可以提高
IAM 身分中心允許的權限集數量	2000	是
每個允許的已佈建權限集數目 AWS 帳戶	250	是

資源	預設配額	可以提高
每個許可集合的內嵌政策數量	1	否
每個權限集合的 AWS 受管理和客戶管理策略數目	20 [1]	否
每個許可集合的內嵌政策大小上限	字節。 每個權限集合的內嵌原則中非空白字元的大小上限為 10,240 個位元組。	否
一次可更新的 IAM 角色 (權限集) 數目 AWS 帳戶	1	否

[1]AWS Identity and Access Management (IAM) 為每個角色設定 10 個受管政策的配額。若要利用此配額，請針對您要部署權限集的每個 AWS 帳戶 位置，請求增加 Service Qu額主控台內附加到IAM 角色的 IAM 配額受管政策。

> **Note**
>
> 許可集在中佈建 AWS 帳戶 為 IAM 角色，或使用中的現有 IAM 角色 AWS 帳戶，因此遵循 IAM 配額。如需與 IAM 角色相關聯之配額的詳細資訊，請參閱 IAM 和 STS 配額。

活動目錄配額

資源	預設配額	可以提高
您一次可以擁有的連線目錄數量	1	否

IAM 身分中心身分存放區配額

資源	預設配額	可以提高
IAM 身分中心支援的使用者數量	100000	是
IAM 身分中心支援的群組數目	100000	否
可用來評估使用者權限的唯一群組數目	1000	否

IAM 身分識別中心節流限制

資源	預設配額
IAM 身分識別中心 API	IAM 身分中心 API 具有每秒最多 20 筆交易 (TPS) 的集合限制。CreateAccountAssignment有 10 個未完成的非同步呼叫的最大速率。無法變更這些配額。

額外配額

資源	預設配額	可以提高
可設定的 AWS 帳戶 或應用程式總數 *	3000	是
每個帳戶的 IAM 身分中心執行個體總數	1	否
受信任令牌發行者總數	10	否

* 最多支持 3000 個應用程序 AWS 帳戶 或應用程序（總計合併）。例如，您可以設定 2750 個帳戶和 250 個應用程式，產生總共 3000 個帳戶和應用程式。

IAM 身分中心問題疑難排解

以下內容可協助您疑難排解在設定或使用 IAM 身分中心主控台時可能遇到的一些常見問題。

建立 IAM 身分中心帳戶執行個體時發生問題

建立 IAM 身分中心的帳戶執行個體時，可能會套用多項限制。如果您無法透過 IAM Identity Center 主控台建立帳戶執行個體，或是 AWS 受支援的受管應用程式的設定經驗，請驗證下列使用案例：

- 檢查其他 AWS 區域 您嘗試 AWS 帳戶 在其中創建帳戶實例的。每個 IAM 身分中心只能使用一個執行個體 AWS 帳戶。若要啟用應用程式，請切換至 IAM 身分中心執行個體，或切換至沒有 IAM 身分中心執行個體的帳戶。 AWS 區域
- 如果您的組織在 2023 年 9 月 14 日之前啟用 IAM 身分中心，則您的管理員可能需要選擇加入帳戶執行個體建立。與您的管理員合作，從管理帳戶的 IAM Identity Center 主控台啟用帳戶執行個體建立功能。
- 您的管理員可能已建立服務控制政策，以限制 IAM 身分中心帳戶執行個體的建立。與您的系統管理員合作，將您的帳戶新增至允許清單。

當您嘗試檢視預先設定為與 IAM 身分中心搭配使用的雲端應用程式清單時，您會收到錯誤訊息

當您的政策允許`sso:ListApplications`但不允許其他 IAM 身分中心 API 時，就會發生下列錯誤。更新您的政策以解決此錯誤。

該`ListApplications`權限授權多個 API：

- `ListApplications`應用程式介面。
- 與 IAM 身分中心主控台中使用的 `ListApplicationProviders` API 類似的內部 API。

為了協助解決重複問題，內部 API 現在也會授權使用該`ListApplicationProviders`動作。若要允許公`ListApplications`用 API 但拒絕內部 API，您的政策必須包含拒絕`ListApplicationProviders`動作的陳述式：

```
    "Statement": [
```

```
    {
         "Effect": "Deny",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

若要允許內部 API 但拒絕ListApplications，原則只需要允許ListApplicationProviders。如果未明確允許，則會拒絕 ListApplications API。

```
      "Statement": [
    {
         "Effect": "Allow",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    }
]
```

當您的政策更新時，請聯繫 AWS Support 以刪除此主動措施。

IAM 身分中心建立的 SAML 宣告內容相關問題

IAM 身分中心為 IAM 身分中心建立和傳送的 SAML 判斷提供網頁式偵錯體驗，包括從存取入口網站存取 AWS 帳戶 和 SAML 應用程式時，這些宣告中的屬性。 AWS 若要查看 IAM 身分中心所產生之 SAML 宣告的詳細資料，請使用下列步驟。

1. 登入 AWS 存取入口網站。
2. 當您登入入口網站時，按住 Shift 鍵，選擇應用程式磚，然後放開 Shift 鍵。
3. 檢查標題為您目前處於管理員模式的頁面上的資訊。若要保留此資訊以供 future 參考，請選擇「複製 XML」，然後將內容貼到其他位置。
4. 選擇「傳送」<application>以繼續。此選項會將宣告傳送至服務提供者。

> **Note**
>
> 某些瀏覽器設定和作業系統可能不支援此程序。這個過程已經在 Windows 10 使用火狐，鉻和邊緣瀏覽器進行了測試。

特定使用者無法從外部 SCIM 提供者同步至 IAM 身分中心

如果在 IdP 中設定用於佈建至 IAM 身分中心的使用者子集的 SCIM 同步成功，但其他使用者失敗，則您可能會看到`'Request is unparsable, syntactically incorrect, or violates schema'`類似身分識別提供者的錯誤訊息。您也可以在中看到詳細的佈建失敗訊息 AWS CloudTrail。

此問題通常表示 IdP 中的使用者是以 IAM 身分中心不支援的方式進行設定。您可以在 IAM 身分中心 SCIM 實作開發人員指南中找到 IAM 身分中心 SCIM 實作的完整詳細資訊，包括使用者物件的必要、選用和禁止參數和作業的規格。SCIM 開發人員指南應視為有關 SCIM 要求的資訊的權威性。但是，以下是導致此錯誤的幾個常見原因：

1. IdP 中的使用者物件缺少第一個 (指定) 名稱、姓氏 (系列) 名稱和/或顯示名稱。

   - 解法：新增使用者物件的第一個 (指定)、姓氏 (系列) 和顯示名稱。此外，請確定 IdP 中使用者物件的 SCIM 佈建對應已設定為傳送所有這些屬性的非空白值。

2. 為使用者傳送單一屬性的多個值 (也稱為「多值屬性」)。例如，使用者可能同時具有 IdP 中指定的公司和住家電話號碼，或者有多封電子郵件或實體地址，而您的 IdP 會設定為嘗試同步處理該屬性的多個或所有值。

   - 解決方案選項：

     i. 更新 IdP 中使用者物件的 SCIM 佈建對應，以便僅傳送指定屬性的單一值。例如，設定僅傳送每個使用者公司電話號碼的對應。

     ii. 如果可以在 IdP 上安全地從使用者物件中移除其他屬性，您可以移除其他值，為使用者設定該屬性的一個或零值。

     iii. 如果中的任何動作都不需要屬性 AWS，請從 IdP 的使用者物件的 SCIM 佈建對應中移除該屬性的對應。

3. 您的 IdP 嘗試根據多個屬性來比對目標 (在本例中為 IAM 身分中心) 中的使用者。由於使用者名稱在指定的 IAM Identity Center 執行個體中保證是唯一的，因此您只需要指定`username`用於比對的屬性即可。

- 解決方案：確保 IdP 中的 SCIM 組態僅使用單一屬性來與 IAM 身分中心中的使用者進行比對。例如，將 IdP `userPrincipalName` 中的`username`或對應至 SCIM 中的`userName`屬性，以便佈建至 IAM 身分中心，對於大多數實作來說都是正確且足夠的。

當使用者名稱為 UPN 格式時，使用者無法登入

使用者可能無法根據他們在登入頁面上輸入其使用者名稱的格式來登入 AWS 存取入口網站。在大多數情況下，使用者可以使用其一般使用者名稱、下層登入名稱 (DOMAIN\UserName) 或其 UPN 登入名稱 () 登入使用者入口網站。`UserName@Corp.Example.com`例外情況是 IAM 身分中心使用已透過 MFA 啟用的連線目錄，且驗證模式已設定為內容感知或永遠在線時。在這個案例中，使用者必須使用下層登入名稱 (DOMAIN\UserName) 登入。如需詳細資訊，請參閱 身分識別中心使用者的多因素驗證。如需用來登入 Active Directory 之使用者名稱格式的一般資訊，請參閱 Microsoft 文件集網站上的使用者名稱格式。

修改 IAM 角色時出現「無法對受保護角色執行操作」錯誤

檢閱帳戶中的 IAM 角色時，您可能會注意到以「AWSReservedSSO_」開頭的角色名稱。這些是 IAM 身分中心服務在帳戶中建立的角色，它們來自為帳戶指派權限集。嘗試從 IAM 主控台修改這些角色會導致以下錯誤：

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -
 this role is only modifiable by AWS'
```

這些角色只能從的管理帳戶中的 IAM 身分中心管理員主控台修改 AWS Organizations。修改後，您可以將變更向下推送至指派給該 AWS 帳戶。

目錄使用者無法重設密碼

當目錄使用者使用忘記密碼重設密碼？ 登入 AWS 存取入口網站期間的選項，其新密碼必須遵守預設密碼原則，如中所述在 IAM 身分中心管理身分時的密碼要求。

如果使用者輸入遵守原則的密碼，然後接收到錯誤`We couldn't update your password`，請檢查是否 AWS CloudTrail 記錄失敗。這可以通過 CloudTrail 使用以下過濾器在事件歷史記錄控制台中搜索來完成：

```
"UpdatePassword"
```

如果訊息指出下列情況，您可能需要連絡支援人員：

```
"errorCode": "InternalFailure",
      "errorMessage": "An unknown error occurred“
```

此問題的另一個可能原因是套用至使用者名稱值的命名慣例中。命名慣例必須遵循特定的模式，例如「姓氏. 給定名稱」。但是，某些使用者名稱可能很長，或包含特殊字元，這可能會導致字元在 API 呼叫中捨棄，進而導致錯誤。您可能希望以相同的方式嘗試與測試用戶重置密碼，以驗證是否出現這種情況。

如果問題仍然存在，請聯絡 S AWS upport 中心。

我的使用者在權限集中參照，但無法存取指派的帳戶或應用程式

如果您使用系統進行跨網域身分識別管理 (SCIM)，透過外部身分識別提供者進行自動佈建，則可能會發生此問題。具體而言，當使用者或使用者所屬的群組遭到刪除，然後使用身分提供者中的相同使用者名稱 (針對使用者) 或名稱 (針對群組) 重新建立時，會在 IAM Identity Center 中為新使用者或群組建立新的唯一內部識別碼。不過，IAM Identity Center 在其權限資料庫中仍有舊識別碼的參考，因此使用者或群組的名稱仍會出現在 UI 中，但存取失敗。這是因為 UI 參照的基礎使用者或群組 ID 不再存在。

若要在此情況下還原 AWS 帳戶 存取權，您可以從原先指派舊使用者或群組的存取權移除，然後將存取權重新指派給使用者或群組。 AWS 帳戶這會使用適用於新使用者或群組的正確識別碼來更新權限集。同樣地，若要還原應用程式存取權，您可以從該應用程式的指派使用者清單中移除使用者或群組的存取權，然後再次將使用者或群組新增回來。

您也可以在 AWS CloudTrail 記錄 CloudTrail 檔中搜尋參考相關使用者或群組名稱的 SCIM 同步處理事件，以檢查是否已記錄失敗。

我無法從正確配置的應用程序目錄中獲取我的應用程序

如果您從 IAM Identity Center 的應用程式目錄新增應用程式，請注意每個服務供應商都會提供自己的詳細文件。您可以從 IAM 身分中心主控台中的應用程式的 [設定] 索引標籤存取此資訊。

如果問題與設定服務供應商的應用程式和 IAM Identity Center 之間的信任有關，請務必查看說明手冊以瞭解疑難排解步驟。

錯誤：當使用者嘗試使用外部身分識別提供者登入時，發生未預期的錯誤

發生此錯誤的原因有多種，但其中一個常見原因是 SAML 請求中包含的使用者資訊與 IAM Identity Center 中使用者的資訊不相符。

若要讓 IAM 身分中心使用者在使用外部 IdP 做為身分識別來源時成功登入，必須符合下列條件：

- SAML NameID 格式 (由您的身分提供者設定) 必須是「電子郵件」
- 名稱識別碼值必須是格式正確 (RFC2822) 的字串 (user@domain.com)
- NameID 值必須與 IAM 身分中心中現有使用者的使用者名稱完全相符 (IAM 身分中心中的電子郵件地址是否符合並不重要 — 輸入比對是根據使用者名稱而定)
- SAML 2.0 聯合的 IAM 身分中心實作僅支援身分識別提供者與 IAM 身分中心之間的 SAML 回應中的 1 個宣告。它不支援加密的 SAML 宣告。
- 如果您的 IAM 身分中心帳戶存取控制的屬性已啟用，則適用下列陳述式：
  - SAML 要求中對應的屬性數目必須少於 50。
  - SAML 要求不得包含多值屬性。
  - SAML 要求不得包含多個具有相同名稱的屬性。
  - 屬性不得包含結構化 XML 作為值。
  - 名稱格式必須是 SAML 指定的格式，而不是一般格式。

> **Note**
>
> IAM 身分中心不會透過 SAML 聯盟為新使用者或群組執行「即時」建立使用者或群組。這表示使用者必須在 IAM 身分中心 (手動或透過自動佈建) 預先建立，才能登入 IAM 身分中心。

當身分識別提供者中設定的宣告消費者服務 (ACS) 端點與 IAM 身分中心執行個體提供的 ACS URL 不符時，也會發生此錯誤。請確定這兩個值完全相符。

此外，您可以移至 AWS CloudTrail 並篩選事件名稱 ExternalIdP，進一步疑難排解外部身分識別提供者登入失敗DirectoryLogin。

錯誤「訪問控制的屬性無法啟用」

如果啟用 ABAC 的使用者沒有啟存取控制的屬性用所需的iam:UpdateAssumeRolePolicy權限，就可能會發生這個錯誤。

當我嘗試為 MFA 註冊設備時，收到「不支持瀏覽器」消息

WebAuthn 目前在谷歌瀏覽器支持, 火狐瀏覽器, Microsoft 邊緣和蘋果 Safari 瀏覽器網絡瀏覽器, 以及視窗 10 和安卓平臺. 某些 WebAuthn 支援元件可能會有所不同，例如跨 macOS 和 iOS 瀏覽器的平台驗證器支援。如果使用者嘗試在不受支援的瀏覽器或平台上註冊 WebAuthn 裝置，他們會看到某些不受支援的選項呈灰色，或者會收到錯誤訊息，指出不支援所有支援的方法。在這些情況下，請參閱 FIDO2：Web 驗證（WebAuthn）以獲取有關瀏覽器/平台支持的更多信息。如需 IAM 身分中心的詳 WebAuthn 細資訊，請參閱FIDO2 驗證器。

活動目錄「域用戶」組未正確同步到 IAM 身份中心

使用中目錄網域使用者群組是 AD 使用者物件的預設「主要群組」。身分識別中心無法讀取作用中目錄主要群組及其成員資格。指派 IAM Identity Center 資源或應用程式的存取權時，請使用網域使用者群組以外的群組 (或指派為主要群組的其他群組)，讓群組成員資格正確反映在 IAM 身分中心身分存放區中。

無效的 MFA 認證錯誤

當使用者在使用 SCIM 通訊協定將帳戶完全佈建至 IAM 身分中心之前，嘗試使用外部身分提供者提供的帳戶 (例如，Okta或Microsoft Entra ID) 登入 IAM 身分中心時，就會發生此錯誤。將使用者帳戶佈建至 IAM 身分中心後，應解決此問題。確認帳戶已佈建至 IAM 身分中心。如果沒有，請檢查外部身分識別提供者中的佈建記錄。

當我嘗試使用身份驗證器應用程序註冊或登錄時，出現「發生意外錯誤」消息

以時間為基礎的一次性密碼 (TOTP) 系統 (例如 IAM Identity Center 與以程式碼為基礎的驗證器應用程式搭配使用的系統) 仰賴用戶端與伺服器之間的時間同步。請確定已安裝驗證器應用程式的裝置已正確同步至可靠的時間來源，或手動設定裝置上的時間以符合可靠來源，例如 NIST (https://www.time.gov/) 或其他本地/地區對應項目。

嘗試登錄 IAM 身份中心時，我收到一個「不是您，這是我們」錯誤

此錯誤表示您的 IAM 身分中心執行個體或外部身分識別提供者 (IdP) IAM 身分中心用作其身分識別來源時發生設定問題。我們建議您驗證以下內容：

- 在您用來登入的裝置上驗證日期和時間設定。我們建議您將日期和時間設定為自動設定。如果無法使用，建議您將日期和時間同步到已知的網路時間通訊協定 (NTP) 伺服器。
- 確認上傳至 IAM 身分中心的 IdP 憑證與您的 IdP 提供的憑證相同。您可以瀏覽至 「設定」，從 IAM 身分中心主控台檢查憑證。在身分識別來源索引標籤中選擇動作，然後選擇管理驗證。如果 IdP 和 IAM 身分中心憑證不相符，請將新憑證匯入 IAM 身分中心。
- 請確定身分識別提供者的中繼資料檔案中的 NameID 格式如下：
  - `urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress`
- 如果您使用的 AD Connector AWS Directory Service 做為身分識別提供者，請確認服務帳戶的認證正確且尚未過期。 AWS Directory Service如需詳細資訊，請參閱中的更新 AD Connector 服務帳戶認證。

我的使用者沒有收到來自 IAM 身分中心的電子郵件

IAM 身分中心服務傳送的所有電子郵件都會來自地址`no-reply@signin.aws`或`no-reply@login.awsapps.com`。您的郵件系統必須設定為接受來自這些寄件者電子郵件地址的電子郵件，並且不會將其視為垃圾郵件或垃圾郵件來處理。

錯誤：您無法刪除/修改/移除/指派管理帳戶中佈建之權限集的存取權

此訊息表示委派管理功能已啟用，而且您之前嘗試的作業只能由中具有管理帳戶權限的人成功執行 AWS Organizations。若要解決此問題，請以具有這些權限的使用者身分登入，然後嘗試再次執行工作，或將此工作指派給具有正確權限的使用者。如需詳細資訊，請參閱 註冊會員帳號。

錯誤：找不到工作階段權杖或無效

當用戶端 (例如 Web 瀏覽器、 AWS 工具組或) 嘗試在伺服器端使用已撤銷或無效的工作階段時 AWS CLI，就可能會發生此錯誤。若要修正此問題，請返回用戶端應用程式或網站，然後再試一次，包括在出現提示時再次登入。這有時可能還需要您取消擱置的請求，例如來自 IDE AWS 工具組 中的擱置連線嘗試。

文件歷史記錄

下表說明 AWS IAM Identity Center 文件的重要新增內容。我們也會經常更新文件，以處理您傳送給我們的意見回饋。

- 最新的主要文件更新：2022 年 9 月 23 日

變更	描述	日期
AWS 受管理策略的更新	已更新AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管理策略的權限。	2024年5月17日
AWS 受管理策略的更新	已更新AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管理策略的權限。	2024 年 4 月 30 日
AWS 受管理策略的更新	已更新AWSSSOMasterAccountAdministrator AWS 受管理策略的權限。	2024年4月26日
AWS 受管理策略的更新	已更新AWSSSOMemberAccountAdministrator AWS 受管理策略的權限。	2024年4月26日
AWS 受管理策略的更新	已更新AWSSSOReadOnly AWS 受管理策略的權限。	2024年4月26日
AWS 受管理策略的更新	已更新AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管理策略的權限。	2024年4月26日

AWS 受管理策略的更新	已更新AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管理策略的權限。	2024年4月24日
AWS 受管理策略的更新	已更新AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管理策略的權限。	2024年4月19 日
AWS 受管理策略的更新	已更新AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管理策略的權限。	2024年4月11日
AWS 受管理策略的更新	已更新AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管理策略的權限。	2023 年 11 月 26 日
新的 AWS 受管原則主題	已新增AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管理原則的詳細資料。	2023 年 11 月 15 日
增強型 IAM 身分中心入門指引	已新增開始使用 IAM 身分中心和建立管理使用者的新內容	2022 年 9 月 23 日
更新身分識別中心 API 參考中的使用者和群組	此更新包含身分識別中心 API 參考指南中新建立、更新和刪除 API 的參考資料。	2022 年 8 月 31 日

AWS 單一登入 (AWS SSO) 已重新命名為 AWS IAM 身分中心	AWS 介紹 AWS IAM Identity Center。IAM 身分中心擴充了 AWS Identity and Access Management (IAM) 的功能，協助您集中管理員工使用者的帳戶和應用程式存取。IAM 身分中心功能包括應用程式指派、多帳戶許可和 AWS 存取入口網站。	2022 年 7 月 26 日
在權限集中 Support 權限界限和客戶管理的原則	新增使 AWS 用具有權限集的受管理和客戶受管 AWS Identity and Access Management (IAM) 政策的內容。	2022 年 7 月 14 日
Support 手動啟用的 AWS 區域	已新增在手動啟用的區域中使用 IAM 身分中心的內容。	2022 年 6 月 15 日
AWS 受管理策略的更新	已更新`AWSSSOServiceRolePolicy` AWS 受管理策略的權限。	2022 年 5 月 11 日
Support 委派管理	已新增委派管理功能的內容。	2022 年 5 月 11 日
AWS 受管理策略的更新	更新`AWSSSOMasterAccountAdministrator` 、`AWSSSOMemberAccountAdministrator` 和`AWSSSOReadOnly` AWS 受管理策略的權限。	2022 年 4 月 28 日
Support 可設定的 AD 同步	已新增可設定 AD 同步功能的內容。	2022 年 4 月 14 日

新的 AWS 受管原則主題	已新增AWSSSOMasterAccountAdministrator AWS 受管理原則的詳細資料。	2021 年 8 月 4 日
配額更新	配額表的調整。	2020 年 12 月 21 日
新的範例政策	已新增客戶管理政策範例，並在「所需權限」區段中加入更新。	2020 年 12 月 21 日
Support 以屬性為基礎的存取控制 (ABAC)	新增 ABAC 功能的內容。	2020 年 11 月 24 日
Support MFA 強制註冊	要求使用者在登入時註冊 MFA 裝置的更新。	2020 年 11 月 23 日
Support WebAuthn	增加了新WebAuthn功能的內容。	2020 年 11 月 20 日
對於 Ping 身份的 Support	新增內容，以作為支援的外部身分識別提供者與Ping Identity產品整合。	2020 年 10 月 26 日
Support OneLogin	新增要OneLogin做為支援的外部身分識別提供者整合的內容。	2020 年 7 月 31 日
支援Okta	新增要Okta做為支援的外部身分識別提供者整合的內容。	2020 年 5 月 28 日
Support 外部身分識別提供者	將參考從目錄變更為身分識別來源，新增內容以支援外部身分識別提供者。	2019 年 11 月 26 日
新的 MFA 設定	刪除了兩步驟驗證主題，並在其中添加了新的 MFA 主題。	2019 年 10 月 24 日

新增兩步驟驗證的新設定	已新增如何為使用者啟用雙步驟驗證的內容。	2019 年 1 月 16 日
Support AWS 帳戶的工作階段持續時間	新增有關如何設定 AWS 帳戶工作階段持續時間的內容。	2018 年 10 月 30 日
使用身分識別中心目錄的新選項	已新增選擇身分識別中心目錄或連線至作用中目錄中現有目錄的內容。	2018 年 10 月 17 日
Support 應用程式上的轉送狀態和工作階段持續	新增有關應用程式轉送狀態和工作階段持續時間的內	2018 年 10 月 10 日
對新應用程式的其他支援	已新增4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvaInSync, Egnyte, Engagedly , Expensify, Freshdesk , IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice , Zoho, OpsGenie, DigiCert, WeekDone, ProdPad,並新增UserEcho至應用程式目錄。	2018 年 8 月 3 日
Support 多帳戶存取管理帳戶	已新增有關如何將多帳戶存取權委派給管理帳戶中的使用者的內容。	2018 年 7 月 9 日
Support 新應用程式	已新增DocuSign, Keeper Security,並新增SugarCRM至應用程式目錄。	2018 年 3 月 16 日

取得用於 CLI 存取的臨時認證	已新增如何取得暫時認證以執行 AWS CLI 命令的相關資訊。	2018 年 2 月 22 日
新的指南	這是 IAM 身分中心使用者指南的第一個版本。	2017 年 12 月 7 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。