



使用者指南

AWS IAM Identity Center



AWS IAM Identity Center: 使用者指南

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

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

Table of Contents

什麼是 IAM Identity Center ?	1
為什麼要使用 IAM Identity Center ?	1
IAM Identity Center 重新命名	2
舊版命名空間保持不變	2
開始使用	4
IAM Identity Center 先決條件和考量事項	5
選擇 AWS 區域	6
僅將 IAM Identity Center 用於應用程式	12
IAM Identity Center 建立的 IAM 角色	12
IAM Identity Center 和 AWS Organizations	13
IAM Identity Center 執行個體	14
AWS 帳戶 可啟用 IAM Identity Center 的類型	14
IAM Identity Center 的組織執行個體	16
IAM Identity Center 的帳戶執行個體。	16
刪除您的 IAM Identity Center 執行個體	21
啟用 IAM Identity Center	22
啟用 IAM Identity Center 的執行個體	22
確認您的身分來源	25
更新防火牆和閘道	26
允許列出網域和 URL 端點的考量事項	29
身分來源教學課程	30
Active Directory	31
CyberArk	33
先決條件	33
SCIM 考量事項	34
步驟 1：在 IAM Identity Center 中啟用佈建	34
步驟 2：在 中設定佈建 CyberArk	35
(選用) 步驟 3：在 中設定使用者屬性CyberArk以進行 IAM Identity Center 中的存取控制 (ABAC)	36
(選用) 傳遞屬性以進行存取控制	36
Google Workspace	37
考量事項	38
步驟 1：Google Workspace：設定 SAML 應用程式	38

步驟 2：IAM Identity Center 和 Google Workspace：變更 IAM Identity Center 身分來源並 Google Workspace 設定為 SAML 身分提供者	39
步驟 3：Google Workspace：啟用應用程式	40
步驟 4：IAM Identity Center：設定 IAM Identity Center 自動佈建	41
步驟 5：Google Workspace：設定自動佈建	42
傳遞存取控制的屬性 - 選用	43
將存取權指派給 AWS 帳戶	43
後續步驟	45
疑難排解	46
JumpCloud	46
先決條件	47
SCIM 考量事項	48
步驟 1：在 IAM Identity Center 中啟用佈建	48
步驟 2：在 中設定佈建 JumpCloud	49
(選用) 步驟 3：在 中設定使用者屬性 JumpCloud，以在 IAM Identity Center 中進行存取控制	49
(選用) 傳遞屬性以進行存取控制	50
Microsoft Entra ID	51
先決條件	51
考量事項	51
步驟 1：準備您的 Microsoft 租用戶	53
步驟 2：準備 AWS 您的帳戶	54
步驟 3：設定和測試 SAML 連線	57
步驟 4：設定和測試您的 SCIM 同步	60
步驟 5：設定 ABAC - 選用	64
將存取權指派給 AWS 帳戶	65
Microsoft Entra ID 用於存取其他區域的組態	67
疑難排解	67
Okta	69
考量事項	70
步驟 1：Okta：從 Okta 您的帳戶取得 SAML 中繼資料	71
步驟 2：IAM Identity Center：將 Okta 設定為 IAM Identity Center 的身分來源	71
步驟 3：IAM Identity Center 和 Okta：佈建 Okta 使用者	73
步驟 4：Okta：將來自 的使用者 Okta 與 IAM Identity Center 同步	74
傳遞存取控制的屬性 - 選用	75
將存取權指派給 AWS 帳戶	76

Okta 用於存取其他區域的組態	78
後續步驟	78
疑難排解	78
OneLogin	80
先決條件	81
步驟 1：在 IAM Identity Center 中啟用佈建	82
步驟 2：在 中設定佈建 OneLogin	82
(選用) 步驟 3：在 中設定使用者屬性OneLogin，以在 IAM Identity Center 中進行存取控制	83
(選用) 傳遞屬性以進行存取控制	84
疑難排解	84
Ping 身分	85
PingFederate	86
PingOne	92
Identity Center 目錄	97
教學課程影片	102
設定您的人力資源	103
使用者、群組和佈建	103
使用者名稱和電子郵件地址唯一性	103
Groups (群組)	103
使用者和群組佈建	104
取消佈建使用者和群組	104
管理您的身分來源	104
變更身分來源的考量事項	105
變更您的身分來源	109
IAM Identity Center 中的使用者和群組屬性	111
外部身分提供者	112
Microsoft AD 目錄	127
在 Identity Center 目錄中管理使用者	144
使用者位於 IAM Identity Center 時的佈建	145
變更您的身分來源	145
新增使用者	145
新增群組	148
將使用者新增至群組	149
刪除群組	150
刪除使用者	151

從群組中移除使用者	152
編輯使用者屬性	153
人力存取	154
了解身分驗證工作階段	154
身分驗證工作階段的類型	155
最終使用者工作階段的方法	156
當您結束工作階段時，使用者存取會發生什麼情況	156
單一登出	159
工作階段管理的最佳實務	159
設定工作階段持續時間	159
使用者互動式工作階段	159
使用者背景工作階段	160
Kiro 的延伸工作階段	162
結束人力使用者的作用中工作階段	162
身分來源、CLI AWS 和 AWS SDKs 考量事項	164
停用使用者存取	167
拒絕使用者存取	167
管理 Identity Center 目錄中使用者的存取權	169
密碼管理	169
MFA	169
設定使用者密碼	170
多重要素驗證	173
應用程式存取權限	184
AWS 受管應用程式	184
控制對應用程式的存取	185
共用身分資訊	185
限制使用 AWS 受管應用程式	186
您可以搭配 IAM Identity Center 使用的應用程式	187
設定 IAM Identity Center 以測試 AWS 受管應用程式	191
檢視和變更應用程式詳細資訊	195
停用 AWS 受管應用程式	196
啟用身分增強主控台工作階段	196
客戶受管應用程式	199
SAML 2.0 和 OAuth 2.0 應用程式	200
SAML 2.0 應用程式設定	204
信任的身分傳播	207

受信任身分傳播的優點	207
啟用信任的身分傳播	208
受信任身分傳播的運作方式	208
先決條件和考量事項	209
使用案例	211
授權服務	234
設定您自己的 OAuth 2.0 應用程式	243
設定客戶受管應用程式	244
指定信任的應用程式	247
受信任權杖發行者	248
輪換憑證	260
輪換憑證之前的考量事項	260
輪換 IAM Identity Center 憑證	260
憑證過期狀態指示燈	262
了解應用程式屬性	263
應用程式啟動 URL	263
轉送狀態	264
工作階段持續時間	264
指派使用者存取應用程式	265
移除使用者對應用程式的存取權	266
映射屬性	266
AWS 帳戶 存取	267
AWS 帳戶 類型	267
指派 AWS 帳戶 存取權	268
最終使用者體驗	269
強制執行和限制存取	270
委派和強制執行存取	270
限制從成員帳戶存取身分存放區	270
委派的管理	271
最佳實務	271
先決條件	275
註冊成員帳戶	275
取消註冊成員帳戶	276
檢視委派管理員帳戶	277
暫時提升存取	277
對 的單一登入存取 AWS 帳戶	278

將使用者或群組存取權指派給 AWS 帳戶	279
移除的使用者和群組存取權 AWS 帳戶	281
撤銷作用中的許可集工作階段	282
委派誰可以指派單一登入存取	283
許可集	284
建立套用最低權限許可的許可集	285
預先定義的許可	286
自訂許可	287
建立、管理和刪除許可集	289
設定許可集屬性	300
參考許可集	305
避免存取中斷的建議	307
自訂信任政策範例	307
屬性型存取控制	308
優勢	309
檢查清單：AWS 使用 IAM Identity Center 在 中設定 ABAC	310
存取控制的屬性	311
服務連結角色	318
AWS 存取入口網站	319
AWS 存取入口網站入門	319
設定 AWS 存取入口網站	319
您可以設定的內容	320
啟用 AWS 存取入口網站	320
自訂 AWS 存取入口網站 URL	321
確認使用者可以登入 AWS 存取入口網站	321
使用 AWS 存取入口網站	322
如何使用 AWS 存取入口網站	323
登入 AWS 存取入口網站	323
重設您的使用者密碼	325
AWS CLI 和 AWS SDK 存取	327
建立捷徑連結	331
為您的裝置註冊 MFA	333
結束作用中工作階段	335
跨多個 使用 IAM Identity Center AWS 區域	337
多區域支援的優點	337
先決條件和考量事項	337

選擇其他區域	338
將 IAM Identity Center 複寫至其他區域	338
步驟 1：建立複本金鑰	339
步驟 2：新增區域	339
步驟 3：更新外部 IdP 設定	340
步驟 4：確認防火牆和閘道允許清單	341
步驟 5：提供資訊給您的使用者	341
新增第一個區域以外的區域變更	341
複寫哪些資料？	341
透過其他 區域的人力資源存取	342
跨多個 的使用者工作階段 AWS 區域	342
AWS 主要和其他 中的存取入口網站端點 AWS 區域	343
主要和其他 中的 ACS 端點 AWS 區域	344
使用沒有多個 ACS URLs AWS 受管應用程式	345
容錯移轉至其他 區域以進行 AWS 帳戶 存取	346
AWS 帳戶 在沒有多個 ACS URLs存取彈性	346
在多個 之間部署和管理應用程式 AWS 區域	347
在多個 之間部署和管理 AWS 受管應用程式 AWS 區域	347
跨多個 AWS 區域部署和管理客戶受管應用程式	349
從 IAM Identity Center 移除區域	349
步驟 1：更新外部 IdP 組態	349
步驟 2：移除區域	349
步驟 3：刪除複本金鑰	350
其他 支援的服務 APIs AWS 區域	351
主要和其他區域中的 CloudTrail 事件	351
主要和其他區域中的 IAM Identity Center 使用案例	351
彈性設計和區域行為	354
專為可用性而設計	355
設定 的緊急存取 AWS 管理主控台	355
緊急存取組態摘要	356
如何設計關鍵操作角色	356
如何規劃您的存取模型	357
如何設計緊急角色、帳戶和群組映射	358
如何建立緊急存取組態	358
緊急準備任務	359
緊急容錯移轉程序	360

返回正常操作	360
在 中一次性設定直接 IAM 聯合應用程式 Okta	361
使用 設定一次直接 IAM 聯合應用程式 ADFS	363
安全	369
IAM Identity Center 的 Identity and Access Management	369
身分驗證	370
存取控制	370
管理存取概觀	371
身分型政策範例	374
以資源為基礎的政策範例	382
AWS 受管政策	384
使用服務連結角色	399
IAM Identity Center 主控台和 API 授權	407
2023 年 11 月之後的 API 動作	407
2020 年 10 月之後的 API 動作	408
AWS STS IAM Identity Center 的條件索引鍵	410
UserId	411
IdentityStoreArn	411
ApplicationArn	412
CredentialId	412
InstanceArn	412
日誌記錄和監控	413
使用 記錄 IAM Identity Center API 呼叫 AWS CloudTrail	413
使用 記錄 IAM Identity Center SCIM AWS CloudTrail	449
Amazon EventBridge	456
記錄可設定的 AD 同步錯誤	456
法規遵循驗證	459
支援的合規標準	459
恢復能力	461
基礎設施安全性	461
資料保護	462
傳輸中加密	462
資料隱私權	462
資料保留	463
靜態加密	463
IAM Identity Center 加密內容	464

使用加密內容控制對客戶受管金鑰的存取	465
監控 IAM Identity Center 的加密金鑰	465
AWS 受管應用程式的儲存、加密和刪除 IAM Identity Center 身分屬性	465
實作客戶受管 KMS 金鑰	466
基準 KMS 金鑰政策	474
進階 KMS 金鑰政策陳述式	478
標記資源	487
標籤限制	487
使用主控台管理標籤	488
AWS CLI 範例	489
指派標籤	489
檢視標籤	489
移除標籤	490
建立許可集時套用標籤	490
API 動作	490
將 AWS CLI 與 IAM Identity Center 整合	491
如何將 AWS CLI 與 IAM Identity Center 整合	491
私有存取的考量事項	492
配額	493
應用程式配額	493
AWS 帳戶 配額	493
Active Directory 配額	494
IAM Identity Center 身分存放區配額	495
IAM Identity Center 調節限制	495
OIDC 服務請求配額	496
其他配額	497
疑難排解	498
建立 IAM Identity Center 帳戶執行個體的問題	498
當您嘗試檢視已預先設定為與 IAM Identity Center 搭配使用的雲端應用程式清單時，會收到錯誤	498
IAM Identity Center 建立的 SAML 聲明內容相關問題	499
特定使用者無法從外部 SCIM 供應商同步到 IAM Identity Center	500
使用外部身分提供者佈建使用者或群組時發生重複的使用者或群組錯誤	501
當使用者的使用者名稱為 UPN 格式時，使用者無法登入	502
我在修改 IAM 角色時收到「無法對受保護角色執行操作」錯誤	502
目錄使用者無法重設密碼	502

許可集中會參考我的使用者，但無法存取指派的帳戶或應用程式	503
我無法從應用程式目錄正確設定我的應用程式	503
錯誤「使用者嘗試使用外部身分提供者登入時發生非預期錯誤」	504
錯誤「存取控制的屬性無法啟用」	505
當我嘗試為 MFA 註冊裝置時，會收到「瀏覽器不受支援」訊息	505
Active Directory「網域使用者」群組未正確同步至 IAM Identity Center	505
無效的 MFA 登入資料錯誤	505
當我嘗試使用驗證器應用程式註冊或登入時，收到「發生非預期的錯誤」訊息	505
我收到「這不是您，這是嘗試登入 IAM Identity Center 時的錯誤」	506
我的使用者未收到來自 IAM Identity Center 的電子郵件	506
錯誤：您無法delete/modify/remove/指派對管理帳戶中佈建之許可集的存取權	506
錯誤：找不到工作階段字符或工作階段字符無效	506
來自信任網域的群組成員不會同步到 IAM Identity Center	507
對中的客戶受管金鑰進行故障診斷 AWS IAM Identity Center	507
拒絕存取：KMS 解密許可問題	507
AWS 在 IAM Identity Center 中啟用客戶受管 KMS 金鑰的受管應用程式登入失敗	508
AWS 受管應用程式安裝和/或使用指派失敗，並在 IAM Identity Center 中啟用客戶受管 KMS 金鑰	508
KMS 許可問題：使用設定客戶受管金鑰 AWS IAM Identity Center	508
AWS 在 IAM Identity Center 中啟用客戶受管 KMS 金鑰的存取入口網站登入失敗	509
對中的多區域設定進行故障診斷 AWS IAM Identity Center	509
我想要複寫 IAM Identity Center 執行個體的區域無法在 IAM Identity Center 主控台中使用 ...	509
AWS 其他區域中的受管應用程式登入失敗	509
文件歷史紀錄	510
AWS 詞彙表	518
.....	dxix

什麼是 IAM Identity Center ？

AWS IAM Identity Center 是將您的人力資源使用者連線至 Kiro 和 Amazon Quick 等 AWS 受管應用程式和其他 AWS 資源 AWS 的解決方案。您可以連接現有的身分提供者，並從目錄同步使用者和群組，或直接在 IAM Identity Center 中建立和管理使用者。然後，您可以將 IAM Identity Center 用於下列其中一項或兩項：

- 使用者存取應用程式
- 使用者存取 AWS 帳戶

已使用 IAM 存取 AWS 帳戶？

您不需要對目前的 AWS 帳戶 工作流程進行任何變更，即可使用 IAM Identity Center 存取 AWS 受管應用程式。如果您使用[聯合身分搭配 IAM](#) 進行 AWS 帳戶 存取，您的使用者可以繼續以他們一直擁有 AWS 帳戶 的相同方式存取，而且您可以繼續使用現有的工作流程來管理該存取。

為什麼要使用 IAM Identity Center ？

IAM Identity Center 透過下列關鍵功能，簡化和簡化人力使用者對應用程式 AWS 帳戶或兩者的存取。

與 AWS 受管應用程式整合

[AWS 受管應用程式](#)，例如 Kiro，並與 IAM Identity Center Amazon Redshift 整合。IAM Identity Center 為 AWS 受管應用程式提供使用者和群組的共同檢視。

跨應用程式的信任身分傳播

透過信任的身分傳播，Amazon Quick 等 AWS 受管應用程式可以安全地與其他 AWS 受管應用程式共用使用者的身分，例如 Amazon Redshift，並根據使用者的身分授權存取 AWS 資源。您可以更輕鬆地稽核使用者活動，因為 CloudTrail 事件會根據使用者和使用者啟動的動作來記錄。這可讓您更輕鬆地了解誰存取了哪些內容。如需支援使用案例的資訊，包括end-to-end組態指引，請參閱[信任的身分傳播使用案例](#)。

一個位置可指派許可給多個 AWS 帳戶

透過多帳戶許可，IAM Identity Center 提供單一位置，讓您將許可指派給多個 中的使用者群組 AWS 帳戶。您可以根據常見的任務函數建立許可，或定義符合您安全需求的自訂許可。然後，您可以將這些許可指派給人力使用者，以控制他們對特定的存取 AWS 帳戶。

此選用功能僅適用於 IAM Identity Center [的組織執行個體](#)。

可簡化使用者存取的聯合點 AWS

透過提供一個聯合點，IAM Identity Center 可減少使用多個 AWS 受管應用程式和 所需的管理工作 AWS 帳戶。使用 IAM Identity Center 時，您只需要聯合一次，而且在使用[SAML 2.0](#)身分提供者時，您只需要管理一個憑證。IAM Identity Center 為 AWS 受管應用程式提供受信任身分傳播使用案例的使用者和群組的共同檢視，或在使用者與其他人共用資源存取權 AWS 時。

如需如何設定常用身分提供者以搭配 IAM Identity Center 使用的資訊，請參閱 [IAM Identity Center 身分來源教學課程](#)。如果您沒有現有的身分提供者，您可以[直接在 IAM Identity Center 中建立和管理使用者](#)。

兩種執行個體類型

IAM Identity Center 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實務。這是唯一可讓您管理 存取權的執行個體 AWS 帳戶，建議用於應用程式的所有生產用途。組織執行個體會部署在 AWS Organizations 管理帳戶中，並為您提供管理使用者存取權的單一點 AWS。

帳戶執行個體繫結至啟用 AWS 帳戶 它們的。僅使用 IAM Identity Center 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[IAM Identity Center 的組織和帳戶執行個體](#)。

使用者易於存取的 Web 入口網站

AWS 存取入口網站是一種易於使用的 Web 入口網站，可讓您的使用者無縫存取其所有指派的應用程式 AWS 帳戶，或同時存取兩者。

對 AWS 帳戶 和應用程式的多區域存取

當您將 IAM Identity Center 執行個體複製到其他區域時，您的人力資源可以透過所有啟用的區域存取其指派 AWS 帳戶 和應用程式，並且可以在每個啟用的區域中部署 AWS 受管應用程式。

IAM Identity Center 重新命名

在 2022 年 7 月 26 日，AWS Single Sign-On 已重新命名為 AWS IAM Identity Center。

舊版命名空間保持不變

為了回溯相容性，sso和 identitystore API 命名空間以及下列相關的命名空間保持不變。

- CLI 命令
 - [aws configure sso](#)
 - [identitystore](#)
 - [sso](#)
 - [sso-admin](#)
 - [sso-oidc](#)
- 包含 AWSSSO和 字AWSIdentitySync首的[受管政策](#)
- 包含 sso和 [的服務端點](#) identitystore
- 包含字首 AWS::SSO 的 [CloudFormation](#) 資源
- 包含 [的服務連結角色](#) AWSServiceRoleForSSO
- 包含 sso和 URLs singlesignon
- 包含 singlesignon 的文件 URL

透過 IAM Identity Center 開始使用

以下概述如何開始使用 IAM Identity Center。

1. 啟用 IAM Identity Center

當您[啟用 IAM Identity Center](#)時，您可以在兩種類型的 IAM Identity Center 執行個體之間進行選擇。這些類型包括：[組織執行個體](#)（建議）和[帳戶執行個體](#)。若要進一步了解這些執行個體類型的不同功能，請參閱[IAM Identity Center 的組織和帳戶執行個體](#)。

Note

啟用 IAM Identity Center 後，您可以執行下列其中一項操作來登入和開啟 [IAM Identity Center 主控台](#)：

- 組織執行個體 - 在管理帳戶中 AWS 使用具有管理許可的登入資料登入。
- 帳戶執行個體 - 在啟用 IAM Identity Center AWS 帳戶 的 中使用具有管理許可的 AWS 登入資料登入。

2. 將您的身分來源連接至 IAM Identity Center

在 IAM Identity Center 主控台中，確認您要使用的身分來源。如需身分來源，請參閱下列內容：

- 外部身分提供者 - 如果您有現有的身分提供者來管理人力資源使用者，您可以將其連線至 IAM Identity Center。如需如何設定常用身分提供者以搭配 IAM Identity Center 使用的詳細資訊，請參閱[IAM Identity Center 身分來源教學課程](#)。
- Active Directory - 如果您使用 Active Directory 來管理人力資源使用者，您可以將其連線至 IAM Identity Center。如需詳細資訊，請參閱[使用 Active Directory 做為身分來源](#)。
- IAM Identity Center - 或者，您可以[直接在 IAM Identity Center 中建立和管理使用者和群組](#)。

Note

目前，您必須使用外部身分提供者做為身分來源，以利用 IAM Identity Center 的多區域設定。如需此設定優點的詳細資訊，請參閱[跨多個使用 IAM Identity Center AWS 區域](#)。

3. 設定的使用者存取權 AWS 帳戶（僅限組織執行個體）

如果您使用的是 IAM Identity Center 的組織執行個體，您可以使用[許可集](#)授予使用者對 AWS 帳戶和資源的存取權，將使用者[或群組存取權指派給 AWS 帳戶](#)。

4. 設定使用者存取應用程式

使用 IAM Identity Center，您可以授予使用者存取兩種類型的應用程式：

a. [AWS 受管應用程式](#)

- 您可以搭配 Amazon Q Business AWS CLI 和 Amazon Redshift 等 AWS 受管應用程式使用 IAM Identity Center。如需詳細資訊，請參閱[AWS 受管應用程式及將 AWS CLI 與 IAM Identity Center 整合](#)。

b. [客戶受管應用程式](#)

- 您可以將下列任一類型的客戶受管應用程式與 IAM Identity Center 整合：
 - [IAM Identity Center 目錄中列出的應用程式](#)
 - [您的自訂應用程式](#)
- 設定應用程式後，您可以將[存取權指派給使用者](#)。

5. 為您的使用者提供 AWS 存取入口網站的登入指示

AWS 存取入口網站是一種 Web 入口網站，可讓您的使用者無縫存取其所有指派的應用程式 AWS 帳戶，或同時存取兩者。IAM Identity Center 中的新使用者必須先啟用其使用者憑證，才能登入 AWS 存取入口網站。

如需有關如何登入 AWS 存取入口網站的資訊，請參閱AWS 登入 《使用者指南》中的[登入 AWS 存取入口網站](#)。若要了解 AWS 存取入口網站的登入程序，請參閱[登入 AWS 存取入口網站](#)。

IAM Identity Center 先決條件和考量事項

您可以使用 IAM Identity Center 僅存取 AWS 受管應用程式、AWS 帳戶 僅存取受管應用程式，或同時存取兩者。如果您使用 IAM 聯合來管理對 的存取 AWS 帳戶，則可以在使用 IAM Identity Center 進行應用程式存取時繼續這樣做。

啟用 IAM Identity Center 之前，請考慮下列事項：

- **AWS 區域**

您必須先在 IAM Identity Center 每個執行個體的單一 [支援](#) 區域中啟用 IAM Identity Center。如果您想要在存取 AWS 帳戶時使用 IAM Identity Center 進行單一登入，則該區域必須可供組織中的所有使用者存取。如果您計劃使用 IAM Identity Center 進行應用程式存取，請注意，某些 AWS 受管應用程式，例如 Amazon SageMaker AI，只能在其支援的區域中操作。此外，大多數 AWS 受管應用程式都需要在與應用程式相同的區域中使用 IAM Identity Center。這可以透過將它們在同一區域中聯合

放置，或在支援時，將 IAM Identity Center 執行個體複寫到 AWS 受管應用程式的所需部署區域來實現。如需詳細資訊，請參閱[選擇的考量事項 AWS 區域](#)。

- 僅限應用程式存取

您只能使用現有身分提供者，將 IAM Identity Center 用於使用者存取應用程式，例如 Kiro。如需詳細資訊，請參閱[使用 IAM Identity Center 僅供使用者存取應用程式](#)。

 Note

應用程式資源的存取由應用程式擁有者獨立管理。

- IAM 角色的配額

IAM Identity Center 會建立 IAM 角色，以授予使用者帳戶資源的許可。如需詳細資訊，請參閱[IAM Identity Center 建立的 IAM 角色](#)。

- IAM Identity Center 和 AWS Organizations

AWS Organizations 建議與 IAM Identity Center 搭配使用，但非必要。如果您尚未設定組織，則不需要。如果您已經設定 AWS Organizations 並將新增 IAM Identity Center 到您的組織，請確定所有 AWS Organizations 功能都已啟用。如需詳細資訊，請參閱[IAM Identity Center 和 AWS Organizations](#)。

IAM Identity Center Web 介面，包括存取入口網站和 IAM Identity Center 主控台，旨在供人類透過支援的 Web 瀏覽器存取。相容瀏覽器包括 Microsoft Edge、Mozilla Firefox、Google Chrome 和 Apple Safari 的最新版本。不支援使用非瀏覽器型路徑存取這些端點。若要以程式設計方式存取 IAM Identity Center 服務，建議您使用 IAM Identity Center 和 Identity Store APIs 參考指南中提供的文件化 API。

選擇的考量事項 AWS 區域

您可以在 AWS 區域 您選擇的單一支援中啟用 IAM Identity Center，並且可供全球使用者使用。此全域可用性可讓您更輕鬆地設定使用者存取多個 AWS 帳戶 和 應用程式。以下是選擇的重要考量 AWS 區域。

- 使用者的地理位置 – 當您選取地理位置最接近大多數最終使用者的區域時，他們存取 AWS 存取入口網站和 AWS 受管應用程式的延遲會較低，例如 Amazon SageMaker AI。
- 選擇加入區域（預設為停用的區域） – 選擇加入區域是預設為停用 AWS 區域的。若要使用選擇加入區域，您必須啟用該區域。如需詳細資訊，請參閱[在選擇加入區域中管理 IAM Identity Center](#)。

- 將 IAM Identity Center 複寫至其他區域 – 如果您計劃將 IAM Identity Center 複寫至其他區域 AWS 區域，您必須選擇預設啟用的區域。如需詳細資訊，請參閱[跨多個 使用 IAM Identity Center AWS 區域](#)。
- 選擇 AWS 受管應用程式的部署區域 – AWS 受管應用程式只能在可用的 AWS 區域 中操作。許多 AWS 受管應用程式也只能在啟用或複寫 IAM Identity Center 的區域中操作（主要或其他區域）。若要確認您的 IAM Identity Center 執行個體是否支援複寫至其他區域，請參閱[跨多個 使用 IAM Identity Center AWS 區域](#)。如果複寫不是選項，請考慮在您計劃使用 AWS 受管應用程式的區域中啟用 IAM Identity Center。
- 數位主權 – 數位主權法規或公司政策可能強制使用特定 AWS 區域。請洽詢您公司的法務部門。
- 身分來源 – 如果您使用 [Active Directory \(AD\)](#) 中的 [AWS Managed Microsoft AD](#)或自我管理目錄做為身分來源，其主區域必須符合您啟用 IAM Identity Center AWS 區域 的。
- 使用 Amazon Simple Email Service 的跨區域電子郵件 – 在某些區域中，IAM Identity Center 可能會呼叫不同區域中的 [Amazon Simple Email Service \(Amazon SES\)](#) 來傳送電子郵件。在這些跨區域呼叫中，IAM Identity Center 會將特定使用者屬性傳送至其他區域。如需詳細資訊，請參閱[使用 Amazon SES 的跨區域電子郵件](#)。
- AWS Control Tower – 如果您要從中啟用 IAM Identity Center 的組織執行個體 AWS Control Tower，執行個體將在 AWS Control Tower 與登陸區域相同的區域中建立。

主題

- [IAM Identity Center 區域資料儲存和操作](#)
- [切換 AWS 區域](#)
- [停用已啟用 IAM Identity Center AWS 區域 的](#)

IAM Identity Center 區域資料儲存和操作

了解 IAM Identity Center 如何跨 處理資料儲存和操作 AWS 區域。

了解 IAM Identity Center 如何存放資料

當您啟用 IAM Identity Center 時，您在 IAM Identity Center 中設定的所有資料都會存放在您啟用它的區域中。此資料包含目錄組態、許可集、應用程式執行個體，以及 AWS 帳戶 應用程式的使用者指派。如果您使用的是 IAM Identity Center 身分存放區，您在 IAM Identity Center 中建立的所有使用者和群組也會儲存在相同的區域中。如果您將 IAM Identity Center 執行個體複寫至其他區域，IAM Identity Center 會自動將使用者、群組、許可集及其指派，以及其他中繼資料和組態複寫至這些區域。

使用 Amazon SES 的跨區域電子郵件

IAM Identity Center 使用 [Amazon Simple Email Service \(Amazon SES\)](#)，在使用者嘗試使用一次性密碼 (OTP) 作為第二個身分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身分和憑證管理事件傳送，例如當使用者受邀設定初始密碼、驗證電子郵件地址，以及重設密碼時。Amazon SES 可在 IAM Identity Center AWS 區域 支援的子集中使用。

當 Amazon SES 在本機提供時，IAM Identity Center 會呼叫 Amazon SES 本機端點 AWS 區域。當 Amazon SES 無法在本機使用時，IAM Identity Center 會呼叫不同 中的 Amazon SES 端點 AWS 區域，如下表所示。

IAM Identity Center 區域碼	IAM Identity Center 區域名稱	Amazon SES 區域碼	Amazon SES 區域名稱
ap-east-1	亞太地區 (香港)	ap-northeast-2	亞太地區 (首爾)
ap-east-2	亞太區域 (台北)	ap-northeast-1	亞太地區 (東京)
ap-south-2	亞太地區 (海德拉巴)	ap-south-1	亞太地區 (孟買)
ap-southeast-4	亞太地區 (墨爾本)	ap-southeast-2	亞太地區 (悉尼)
ap-southeast-5	亞太地區 (馬來西亞)	ap-southeast-1	亞太地區 (新加坡)
ap-southeast-6	亞太區域 (紐西蘭)	ap-southeast-2	亞太地區 (悉尼)
ap-southeast-7	亞太區域 (泰國)	ap-northeast-3	亞太地區 (大阪)
ca-west-1	加拿大西部 (卡加利)	ca-central-1	加拿大 (中部)
eu-south-2	歐洲 (西班牙)	eu-west-3	Europe (Paris)
eu-central-2	歐洲 (蘇黎世)	eu-central-1	歐洲 (法蘭克福)
mx-central-1	墨西哥 (中部)	us-east-2	美國東部 (俄亥俄)
me-central-1	中東 (阿拉伯聯合大公國)	eu-central-1	歐洲 (法蘭克福)
us-gov-east-1	AWS GovCloud (美國東部)	us-gov-west-1	AWS GovCloud (美國西部)

在這些跨區域呼叫中，IAM Identity Center 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

在選擇加入區域中管理 IAM Identity Center（預設為停用的區域）

根據預設，大多數 AWS 區域 都已啟用所有 AWS 服務中的操作，但如果您想要使用 IAM Identity Center，則必須啟用下列[選擇加入區域](#)：

- 非洲 (開普敦)
- 亞太地區 (香港)
- 亞太區域 (台北)
- 亞太地區 (海德拉巴)
- 亞太地區 (雅加達)
- 亞太地區 (墨爾本)
- 亞太區域 (馬來西亞)
- 亞太區域 (紐西蘭)
- 亞太區域 (泰國)
- 加拿大西部 (卡加利)
- 歐洲 (米蘭)
- 歐洲 (西班牙)
- 歐洲 (蘇黎世)
- 以色列 (特拉維夫)
- 墨西哥 (中部)

- Middle East (Bahrain)
- 中東 (阿拉伯聯合大公國)

如果您在選擇加入區域部署 IAM Identity Center，則必須在您要管理 IAM Identity Center 存取權的所有帳戶中啟用此區域。無論您是否要在該區域中建立資源，所有帳戶都需要此組態。您可以為組織中的目前帳戶啟用區域，您必須在新增帳戶時重複此動作。如需說明，請參閱AWS Organizations 《使用者指南》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 Identity Center。

Note

您的 AWS 成員帳戶必須選擇加入與您的 IAM Identity Center 執行個體所在選擇加入區域相同的區域，以便您可以從存取入口網站 AWS 存取 AWS 成員帳戶。

儲存在選擇加入區域中的中繼資料

當您為選擇加入的管理帳戶啟用 IAM Identity Center 時 AWS 區域，任何成員帳戶的下列 IAM Identity Center 中繼資料都會存放在 區域中。

- 帳戶 ID
- 帳戶名稱
- 帳戶電子郵件
- IAM Identity Center 在成員帳戶中建立的 IAM 角色的 Amazon Resource Name ARNs)

AWS 區域 預設為啟用

下列區域預設為啟用，您可以在這些區域中啟用 IAM Identity Center。

- 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)

- 亞太地區 (孟買)
- 歐洲 (斯德哥爾摩)
- 亞太地區 (首爾)
- 亞太地區 (東京)
- 歐洲 (愛爾蘭)
- 歐洲 (法蘭克福)
- 歐洲 (倫敦)
- 亞太地區 (新加坡)
- 亞太地區 (雪梨)
- 加拿大 (中部)
- 亞太地區 (大阪)

切換 AWS 區域

建議您將 IAM Identity Center 安裝在您想要讓使用者保持可用的區域中，而不是您可能需要停用的區域。如需詳細資訊，請參閱[選擇的考量事項 AWS 區域](#)。

您只能透過[刪除目前的 IAM Identity Center 執行個體，並在另一個區域中建立執行個體來切換 IAM Identity Center 區域](#)。如果您已使用現有的 IAM Identity Center 執行個體啟用 AWS 受管應用程式，請在刪除 IAM Identity Center 之前停用應用程式。如需停用 AWS 受管應用程式的指示，請參閱[停用 AWS 受管應用程式](#)。

Note

如果您正在考慮切換 IAM Identity Center 區域，以在另一個區域中啟用 AWS 受管應用程式的部署，請考慮改為將 IAM Identity Center 執行個體複製至該區域。如需詳細資訊，請參閱[跨多個使用 IAM Identity Center AWS 區域](#)。

新區域中的組態考量事項

您必須在新的 IAM Identity Center 執行個體中重新建立使用者、群組、許可集、應用程式和指派。您可以使用 IAM Identity Center 帳戶和應用程式指派 [APIs](#) 來取得組態的快照，然後使用該快照在新區域中重建組態。切換到不同的區域也會變更[AWS 存取入口網站](#)的 URL，這可讓您的使用者透過單一登入

存取其 AWS 帳戶 和 應用程式。您可能還需要透過新執行個體的管理主控台重新建立一些 IAM Identity Center 組態。

停用已啟用 IAM Identity Center AWS 區域 的

如果您停用已安裝 IAM Identity Center AWS 區域 的，IAM Identity Center 也會停用。在 區域中停用 IAM Identity Center 之後，該區域中的使用者將無法單一登入存取 AWS 帳戶 和 應用程式。

若要在[選擇加入 AWS 區域](#)中重新啟用 IAM Identity Center，您必須重新啟用區域。由於 IAM Identity Center 必須重新處理所有暫停的事件，重新啟用 IAM Identity Center 可能需要一些時間。

Note

IAM Identity Center 只能管理 AWS 帳戶 在 中啟用的 存取權 AWS 區域。若要管理組織中所有帳戶的存取權，請在 中的管理帳戶中啟用 IAM Identity Center AWS 區域，該帳戶會自動啟用以與 IAM Identity Center 搭配使用。

如需啟用和停用的詳細資訊 AWS 區域，請參閱《AWS 一般參考》中的[管理 AWS 區域](#)。

使用 IAM Identity Center 僅供使用者存取應用程式

您可以使用 IAM Identity Center 來使用者存取應用程式，例如 Kiro AWS 帳戶或兩者。您可以連接現有的身分提供者，並從目錄同步使用者和群組，或[直接在 IAM Identity Center 中建立和管理使用者](#)。如需如何將現有身分提供者連線至 IAM Identity Center 的資訊，請參閱 [IAM Identity Center 身分來源教學課程](#)。

已使用 IAM 存取 AWS 帳戶？

您不需要對目前的 AWS 帳戶 工作流程進行任何變更，即可使用 IAM Identity Center 存取 AWS 受管應用程式。如果您使用[聯合身分搭配 IAM](#)進行 AWS 帳戶 存取，您的使用者可以繼續以他們一直擁有 AWS 帳戶 的相同方式存取，而且您可以繼續使用現有的工作流程來管理該存取。

IAM Identity Center 建立的 IAM 角色

當您將使用者指派給 AWS 帳戶時，IAM Identity Center 會建立 IAM 角色，以授予使用者 資源的許可。

當您指派許可集時，IAM Identity Center 會在每個帳戶中建立對應的 IAM Identity Center 控制 IAM 角色，並將許可集中指定的政策連接到這些角色。IAM Identity Center 會管理角色，並允許您定義的授權

使用者使用 AWS 存取入口網站 或 擔任角色 AWS CLI。當您修改許可集時，IAM Identity Center 會確保相應地更新對應的 IAM 政策和角色。將 IAM Identity Center 執行個體複寫至其他區域不會影響現有的 IAM 角色，也不會建立新的 IAM 角色。

Note

許可集不會用來授予應用程式許可。

如果您已在 中設定 IAM 角色 AWS 帳戶，建議您檢查您的帳戶是否接近 IAM 角色的配額。每個帳戶 IAM 角色的預設配額為 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，請考慮請求增加配額。否則，當您將許可集佈建至超過 IAM 角色配額的帳戶時，可能會遇到 IAM Identity Center 的問題。如需如何請求提高配額的詳細資訊，請參閱《Service Quotas 使用者指南》中的 [請求提高配額](#)。

Note

如果您在已使用 IAM Identity Center 的帳戶中檢閱 IAM 角色，您可能會注意到以 開頭的角色名稱“AWSReservedSSO_”。這些是 IAM Identity Center 服務在帳戶中建立的角色，它們來自將許可集指派給帳戶。

IAM Identity Center 和 AWS Organizations

AWS Organizations 建議與 IAM Identity Center 搭配使用，但非必要。如果您尚未設定組織，則不需要。當您啟用 IAM Identity Center 時，您可以選擇是否要使用 啟用服務 AWS Organizations。當您設定組織時，AWS 帳戶 設定組織的 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其他 都是成員帳戶。管理帳戶會建立管理成員帳戶的組織資源、組織單位和政策。管理帳戶會將許可委派給成員帳戶。

Note

我們建議您使用 啟用 IAM Identity Center AWS Organizations，這會建立 IAM Identity Center 的組織執行個體。我們建議使用組織執行個體的最佳實務，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 [IAM Identity Center 的組織執行個體](#)。

如果您已經設定 AWS Organizations 並將新增 IAM Identity Center 到您的組織，請確定所有 AWS Organizations 功能都已啟用。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 的組織執行個體，您必須 AWS 管理主控台 以具有管理登入資料的使用者或根使用者身分登入您的 AWS Organizations 管理帳戶（除非沒有其他管理使用者，否則不建議使用）來登入。如需詳細資訊，請參閱 AWS Organizations 《使用者指南》中的[建立和管理 AWS 組織](#)。

使用 AWS Organizations 成員帳戶的管理登入資料登入時，您可以啟用 IAM Identity Center 的帳戶執行個體。帳戶執行個體的功能有限，且繫結至單一 AWS 帳戶。

IAM Identity Center 的組織和帳戶執行個體

執行個體是 IAM Identity Center 的單一部署。IAM Identity Center 有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（建議）

您在 AWS Organizations 管理帳戶中啟用的 IAM Identity Center 執行個體。組織執行個體支援 IAM Identity Center 的所有功能。我們建議您部署組織執行個體，而不是帳戶執行個體，以將管理點的數量降至最低。

- 帳戶執行個體

繫結至單一 的 IAM Identity Center 執行個體 AWS 帳戶，且僅在啟用該身分中心的 AWS 帳戶和 AWS 區域中可見。針對更簡單的單一帳戶案例使用帳戶執行個體。您可以從下列其中一項啟用帳戶執行個體：

- 不是由 管理 AWS 帳戶 的 AWS Organizations
- 中的成員帳戶 AWS Organizations

AWS 帳戶 可啟用 IAM Identity Center 的類型

若要啟用 IAM Identity Center，請根據您要建立的執行個體類型，AWS 管理主控台 使用下列其中一個登入資料登入：

- 您的 AWS Organizations 管理帳戶（建議）– 建立 IAM Identity Center [的組織執行個體](#)時需要。將組織執行個體用於整個組織的多帳戶許可和應用程式指派。

- 您的 AWS Organizations 成員帳戶 – 用來建立 IAM Identity Center [的帳戶執行個體](#)，以在該成員帳戶中啟用應用程式指派。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 – 用來建立 IAM Identity Center [的組織執行個體](#)或[帳戶執行個體](#)。獨立 AWS 帳戶不是由 管理 AWS Organizations。您只能將 IAM Identity Center 的一個執行個體與獨立建立關聯，AWS 帳戶 並使用該執行個體在該獨立內進行應用程式指派 AWS 帳戶。

使用下表來比較執行個體類型所提供的功能：

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 中的執行個體 AWS 帳戶
管理使用者	✔ 是	✔ 是	✔ 是
AWS 存取受管 AWS 應用程式的單一登入 存取入口網站	✔ 是	✔ 是	✔ 是
OAuth 2.0 (OIDC) 客 戶受管應用程式	✔ 是	✔ 是	✔ 是
多帳戶許可	✔ 是	✘ 否	✘ 否
AWS 存取 時單一登入 的存取入口網站 AWS 帳戶	✔ 是	✘ 否	✘ 否
SAML 2.0 客戶受管應 用程式	✔ 是	✘ 否	✘ 否
委派管理員可以管理 執行個體	✔ 是	✘ 否	✘ 否
使用客戶管理的 KMS 金鑰進行靜態加密	✔ 是	✘ 否	✘ 否
將 IAM Identity Center 複寫至其他區域	✔ 是	✘ 否	✘ 否

如需 AWS 受管應用程式和 IAM Identity Center 的詳細資訊，請參閱 [AWS 可與 IAM Identity Center 搭配使用的 受管應用程式](#)。

主題

- [IAM Identity Center 的組織執行個體](#)
- [IAM Identity Center 的帳戶執行個體](#)。
- [刪除您的 IAM Identity Center 執行個體](#)

IAM Identity Center 的組織執行個體

搭配 啟用 IAM Identity Center 時 AWS Organizations，您要建立 IAM Identity Center 的組織執行個體。您必須在管理帳戶中啟用組織執行個體，之後即可透過單一組織執行個體集中管理使用者與群組的存取權限。每個管理帳戶只能有一個組織執行個體 AWS Organizations。

如果您在 2023 年 11 月 15 日之前啟用 IAM Identity Center，則您有一個 IAM Identity Center 的組織執行個體。

若要啟用 IAM Identity Center 的組織執行個體，請參閱 [啟用 IAM Identity Center 的執行個體](#)。

何時使用組織執行個體

組織執行個體是啟用 IAM Identity Center 的主要方法，通常建議使用組織執行個體。組織執行個體提供下列優點：

- 支援 IAM Identity Center 的所有功能 – 包括管理 AWS 帳戶 組織中多個 的許可、指派客戶受管應用程式的存取權，以及多區域複寫。
- 減少管理點的數量 – 組織執行個體具有單一管理點，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。
- 建立帳戶執行個體的集中控制 – 只要您尚未將 IAM Identity Center 執行個體部署到選擇加入區域（預設為停用）AWS 區域 中的組織，就可以控制您組織中的成員帳戶是否可以建立帳戶執行個體。

如需啟用 IAM Identity Center 組織執行個體的說明，請參閱 [啟用 IAM Identity Center 的執行個體](#)。

IAM Identity Center 的帳戶執行個體。

透過 IAM Identity Center 的帳戶執行個體，您可以部署支援的 AWS 受管應用程式和以 OIDC 為基礎的客戶受管應用程式。帳戶執行個體支援在單一 中隔離部署應用程式 AWS 帳戶，利用 IAM Identity Center 人力資源身分和存取入口網站功能。

帳戶執行個體繫結至單一 AWS 帳戶，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權 AWS 區域。每個限制一個帳戶執行個體 AWS 帳戶。您可以從下列其中一項建立帳戶執行個體：中的成員帳戶 AWS Organizations 或非 AWS 帳戶管理的獨立帳戶 AWS Organizations。

如需啟用 IAM Identity Center 帳戶執行個體的說明，請參閱[啟用 IAM Identity Center 的執行個體](#)並選擇帳戶索引標籤。

何時使用 帳戶執行個體

在大多數情況下，建議使用[組織執行個體](#)。只有在下列其中一個案例適用時，才使用帳戶執行個體：

- 您想要執行受支援 AWS 受管應用程式的暫時試用，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 Identity Center，但您想要支援一或多個 AWS 受管應用程式。
- 您有 IAM Identity Center 的組織執行個體，但您想要將支援的 AWS 受管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。
- 您無法控制營運所在的 AWS 組織。例如，第三方會控制管理您 AWS 的組織 AWS 帳戶。

Important

如果您計劃使用 IAM Identity Center 支援多個帳戶中的應用程式，請使用組織執行個體。帳戶執行個體不支援此使用案例。

AWS 支援帳戶執行個體的 受管應用程式

請參閱[AWS 可與 IAM Identity Center 搭配使用的 受管應用程式](#)以了解哪些 AWS 受管應用程式支援 IAM Identity Center 的帳戶執行個體。使用 AWS 受管應用程式驗證帳戶執行個體建立的可用性。

成員帳戶的可用性限制

若要在 AWS Organizations 成員帳戶中部署 IAM Identity Center 的帳戶執行個體，下列其中一個條件必須為 true：

- 您的組織中沒有 IAM Identity Center 的組織執行個體。
- 您的組織中有 IAM Identity Center 的組織執行個體，且執行個體管理員允許建立 IAM Identity Center 的帳戶執行個體（適用於 2023 年 11 月 15 日之後建立的組織執行個體）。

- 您的組織中有 IAM Identity Center 的組織執行個體，而執行個體管理員則由組織中的成員帳戶手動啟用帳戶執行個體的建立（適用於 2023 年 11 月 15 日之前建立的組織執行個體）。如需說明，請參閱[允許在成員帳戶中建立帳戶執行個體](#)。

符合上述其中一個條件後，下列所有條件都必須為 true：

- 您的管理員尚未建立[服務控制政策](#)，以防止成員帳戶建立帳戶執行個體。
- 無論為何，您在此相同帳戶中還沒有 IAM Identity Center 的執行個體 AWS 區域。
- 您正在可使用 IAM Identity Center AWS 區域的中工作。如需區域的詳細資訊，請參閱[IAM Identity Center 區域資料儲存和操作](#)。

帳戶執行個體考量事項

帳戶執行個體是專為特殊使用案例所設計，並提供組織執行個體可用的功能子集。在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許可集，因此不支援的存取 AWS 帳戶。
- 您無法將帳戶執行個體轉換或合併至組織執行個體。
- 僅選取[AWS 受管應用程式](#)支援帳戶執行個體。
- 將帳戶執行個體用於隔離的使用者，這些使用者只會在單一帳戶中使用應用程式，並在使用的應用程式的生命週期內使用。
- 連接到帳戶執行個體的應用程式必須保持連接到帳戶執行個體，直到您刪除應用程式及其資源為止。
- 帳戶執行個體必須保留在建立該執行個體 AWS 帳戶的中。

允許在成員帳戶中建立帳戶執行個體

如果您在 2023 年 11 月 15 日之前啟用 IAM Identity Center，您有一個 IAM Identity Center [的組織執行個體](#)，可讓成員帳戶建立預設停用的帳戶執行個體。您可以在 IAM Identity Center 主控台中啟用帳戶執行個體功能，以選擇您的成員帳戶是否可以建立帳戶執行個體。

啟用由組織中成員帳戶建立帳戶執行個體

Important

為成員帳戶啟用 IAM Identity Center 的帳戶執行個體是一次性操作。這表示此操作無法反轉。啟用後，您可以透過建立服務控制政策 (SCP) 來限制帳戶執行個體的建立。如需說明，請參閱[使用服務控制政策來控制帳戶執行個體的建立](#)。

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定，然後選擇管理索引標籤。
3. 在 IAM Identity Center 的帳戶執行個體區段中，選擇啟用 IAM Identity Center 的帳戶執行個體。
4. 在啟用 IAM Identity Center 帳戶執行個體對話方塊中，選擇啟用，確認您想要允許組織中的成員帳戶建立帳戶執行個體。

使用服務控制政策來控制帳戶執行個體的建立

成員帳戶建立帳戶執行個體的能力取決於您何時啟用 IAM Identity Center：

- 2023 年 11 月之前 – 您必須[允許在成員帳戶中建立帳戶執行個體](#)，這是無法反轉的動作。
- 2023 年 11 月 15 日之後 – 根據預設，成員帳戶可以建立帳戶執行個體。

在任何一種情況下，您都可以使用服務控制政策 SCPs) 來：

- 防止所有成員帳戶建立帳戶執行個體。
- 僅允許特定成員帳戶建立帳戶執行個體。

防止帳戶執行個體

使用下列程序產生 SCP，以防止成員帳戶建立 IAM Identity Center 的帳戶執行個體。

1. 開啟 [IAM Identity Center 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. 在連接 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 並選擇前往 SCP 儀表板按鈕。系統會將您導向至 [AWS Organizations 主控台](#) 來建立 SCP，或將其做為陳述

式連接到現有的 SCP。SCPs是 的一項功能 AWS Organizations。如需連接 SCP 的說明，請參閱《使用者指南》中的[連接和分離服務控制政策](#)。AWS Organizations

限制帳戶執行個體

除#<ALLOWED-ACCOUNT-ID>#預留位置中明確列出的帳戶執行個體 AWS 帳戶 外，此政策不會阻止建立所有帳戶執行個體，而是拒絕嘗試為所有帳戶建立 IAM Identity Center 的帳戶執行個體。

Example：拒絕政策以限制帳戶執行個體建立

JSON

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

- 將 **【#<ALLOWED-ACCOUNT-ID>#】** 取代為您想要允許 建立 IAM Identity Center 帳戶執行個體的實際 AWS 帳戶 ID。
- 您可以列出陣列格式的多個允許帳戶 IDs：**【"111122223333"#"444455556666"】**。
- 將此政策連接至您的組織 SCP，以強制執行對 IAM Identity Center 帳戶執行個體建立的集中控制。

如需連接 SCP 的指示，請參閱《使用者指南》中的[連接和分離服務控制政策](#)。AWS Organizations

刪除您的 IAM Identity Center 執行個體

刪除 IAM Identity Center 執行個體時，會刪除該執行個體中的所有資料，且無法復原。下表說明根據在 IAM Identity Center 中設定的目錄類型刪除哪些資料。

刪除哪些資料	連線目錄 -、AWS Managed Microsoft AD AD Connector 或外部身分提供者	IAM Identity Center 身分存放區
您已為設定的所有許可集 AWS 帳戶	☑是	☑是
您在 IAM Identity Center 中設定的所有應用程式	☑是	☑是
您已為 AWS 帳戶和應用程式設定的所有使用者指派	☑是	☑是
目錄或存放區中的所有使用者和群組	無	☑是

如果您將 IAM Identity Center 執行個體複寫到其他區域，您必須先移除這些區域，才能刪除執行個體。

使用下列程序刪除您的 IAM Identity Center 執行個體。

刪除您的 IAM Identity Center 執行個體

1. 開啟 [IAM Identity Center 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 Identity Center 組態區段中，選擇刪除。
5. 在刪除 IAM Identity Center 組態對話方塊中，選取每個核取方塊以確認您了解您的資料將被刪除。在文字方塊中輸入 IAM Identity Center 執行個體，然後選擇確認。

啟用 IAM Identity Center

當您啟用 IAM Identity Center 時，您可以選擇要啟用的 AWS IAM Identity Center 執行個體類型。服務執行個體是您 AWS 環境中服務的單一部署。IAM Identity Center 有兩種類型的執行個體：組織執行個體和帳戶執行個體。您可以啟用的執行個體類型取決於您登入的帳戶類型。

下列清單識別您可以為每種類型啟用的 IAM Identity Center 執行個體類型 AWS 帳戶：

- 您的 AWS Organizations 管理帳戶（建議）– 建立 IAM Identity Center [的組織執行個體](#)時需要。將組織執行個體用於整個組織的多帳戶許可和應用程式指派。您可以將此執行個體類型複寫至其他區域，以在選擇 AWS 應用程式部署區域時增強帳戶存取和彈性的彈性。
- 您的 AWS Organizations 成員帳戶 – 用來建立 IAM Identity Center [的帳戶執行個體](#)，以在該成員帳戶中啟用應用程式指派。組織中可以存在一或多個具有成員層級執行個體的帳戶。
- 獨立 – AWS 帳戶用來建立 IAM Identity Center [的組織執行個體](#)或[帳戶執行個體](#)。獨立 AWS 帳戶不是由管理 AWS Organizations。您只能將 IAM Identity Center 的一個執行個體與獨立建立關聯，AWS 帳戶並使用該執行個體在該獨立內進行應用程式指派 AWS 帳戶。

Important

組織管理帳戶可以使用服務控制政策，控制[組織成員帳戶是否可以建立 IAM Identity Center 的帳戶執行個體](#)。

如果您使用免費方案帳戶，建立 AWS 組織會自動將您的帳戶升級至付費計劃，並pay-as-you-go計費。您的免費方案點數會立即過期。如需詳細資訊，請參閱 [AWS 免費方案FAQs](#)。

如需不同執行個體類型所提供不同功能的比較，請參閱 [IAM Identity Center 的組織和帳戶執行個體](#)。

啟用 IAM Identity Center 之前，建議您檢閱 [IAM Identity Center 先決條件和考量事項](#)。

啟用 IAM Identity Center 的執行個體

選擇您要啟用之 IAM Identity Center 執行個體類型的索引標籤，無論是組織或帳戶執行個體：

Organization (recommended)

1. 執行下列其中一項操作來登入 AWS 管理主控台。

- 新使用者 AWS (根使用者) – 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者的身分登入。在下一頁中，輸入您的密碼。
- 已使用 AWS 搭配獨立 AWS 帳戶 (IAM 憑證) – 使用您的 IAM 憑證搭配管理許可來登入。
- 已使用 AWS Organizations (IAM 登入資料) – 使用您的管理帳戶登入資料登入。

2. 開啟 [IAM Identity Center 主控台](#)。

3. (選用) 如果您想要使用客戶受管 KMS 金鑰進行靜態加密，而不是使用預設 AWS 的受管金鑰，請在金鑰區段中設定客戶受管金鑰，以加密靜態 IAM Identity Center 資料。如需詳細資訊，請參閱 [在中實作客戶受管 KMS 金鑰 AWS IAM Identity Center](#)。

 Important

只有在您已設定使用 KMS 客戶受管金鑰的必要許可時，才執行此步驟。如果沒有適當的許可，此步驟可能會失敗或中斷 IAM Identity Center 管理和 AWS 受管應用程式。

4. 在啟用 IAM Identity Center 下，選擇啟用。
5. 在使用 啟用 IAM Identity Center AWS Organizations 頁面上，檢閱資訊，然後選取啟用以完成程序。

 Note

AWS Organizations 只能在單一區域中啟用 IAM Identity Center AWS。啟用 IAM Identity Center 之後，如果您需要在其中變更啟用 IAM Identity Center 的區域，則必須[刪除](#)目前的執行個體，並在其他區域中建立執行個體。

啟用組織執行個體之後，建議您執行下列步驟以完成環境設定：

- 確認您使用的是您選擇的身分來源。如果您已有指派的身分來源，您可以繼續使用。如需詳細資訊，請參閱[在 IAM Identity Center 中確認您的身分來源](#)。
- 將成員帳戶註冊為委派管理員。如需詳細資訊，請參閱[委派的管理](#)。
- IAM Identity Center 為您提供 AWS 資源的存取入口網站。如果您使用新一代防火牆 (NGFW) 或安全 Web Gateway (SWG) 等 Web 內容篩選解決方案來篩選特定 AWS 網域或 URL 端點的存取，請參閱[更新防火牆和閘道以允許存取 AWS 存取入口網站](#)。

Account

1. 執行下列其中一項操作來登入 AWS 管理主控台。
 - 新使用者 AWS (根使用者) – 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者的身分登入。在下一頁中，輸入您的密碼。
 - 已使用 AWS (IAM 登入資料) – 使用具有管理許可的 IAM 登入資料登入。
 - 已使用 AWS Organizations (IAM 登入資料) – 使用您的成員帳戶管理登入資料登入。
2. 開啟 [IAM Identity Center 主控台](#)。
3. 如果您是初次使用 AWS 或具有獨立 AWS 帳戶，請在啟用 IAM Identity Center 下，選擇啟用。

您會看到使用 啟用 IAM Identity Center AWS Organizations 頁面。我們建議使用此選項，但並非必要。

選取連結以啟用 IAM Identity Center 的帳戶執行個體。

4. 如果您是 AWS Organizations 成員帳戶的管理員，請在啟用 IAM Identity Center 的帳戶執行個體下，選取啟用帳戶執行個體。
5. 在啟用 IAM Identity Center 帳戶執行個體頁面上，檢閱資訊並選擇性地新增要與此帳戶執行個體建立關聯的標籤。然後選取啟用以完成程序。

Note

如果 AWS 您的帳戶是組織的成員，則您啟用 IAM Identity Center 帳戶執行個體的能力可能會有限制。

- 如果您的組織在 2023 年 11 月 15 日之前啟用 IAM Identity Center，成員帳戶建立帳戶執行個體的功能預設為停用，且必須由組織的管理帳戶啟用。
- 如果您的組織在 2023 年 11 月 15 日之後啟用 IAM Identity Center，則預設會啟用成員帳戶建立帳戶執行個體的功能。不過，服務控制政策可用來防止在組織內建立 IAM Identity Center 的帳戶執行個體。

如需詳細資訊，請參閱[the section called “允許在成員帳戶中建立帳戶執行個體”](#)及[the section called “建立帳戶執行個體 SCPs”](#)。

在 IAM Identity Center 中確認您的身分來源

IAM Identity Center 中的身分來源會定義使用者和群組的管理位置。啟用 IAM Identity Center 之後，請確認您使用的是您選擇的身分來源。如果您已有指派的身分來源，您可以繼續使用它。

如果您已經在 Active Directory 或外部 IdP 中管理使用者和群組，我們建議您在啟用 IAM Identity Center 並選擇身分來源時，考慮連接此身分來源。這應該在預設 Identity Center 目錄中建立任何使用者和群組並進行任何指派之前完成。

如果您已在 IAM Identity Center 中管理某個身分來源中的使用者和群組，變更為不同的身分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[變更身分來源的考量事項](#)。

確認您的身分來源

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在儀表板頁面的建議設定步驟區段下方，選擇確認您的身分來源。您也可以選擇設定並選擇身分來源索引標籤來存取此頁面。
3. 如果您想要保留指派的身分來源，則不會有任何動作。如果您想要變更，請選擇動作，然後選擇變更身分來源。

您可以選擇下列其中一項做為您的身分來源：

Identity Center 目錄

當您第一次啟用 IAM Identity Center 時，會自動將 Identity Center 目錄設定為您的預設身分來源。如果您尚未使用其他外部身分提供者，您可以開始建立使用者和群組，並將他們的存取層級指派給您的 AWS 帳戶 和應用程式。如需使用此身分來源的教學課程，請參閱 [使用預設 IAM Identity Center 目錄設定使用者存取權](#)。

Active Directory

如果您已經在使用 Directory Service 或 中的自我管理目錄管理 AWS Managed Microsoft AD 目錄中的使用者和群組 Active Directory (AD)，我們建議您在啟用 IAM Identity Center 時連接該目錄。請勿在預設 Identity Center 目錄中建立任何使用者和群組。IAM Identity Center 使用 AWS Directory Service 提供的連線，將 Active Directory 中來源目錄的使用者、群組和成員資格資訊同步到 IAM Identity Center 身分存放區。如需詳細資訊，請參閱[Microsoft AD 目錄](#)。

Note

IAM Identity Center 不支援以 SAMBA4-based Simple AD 做為身分來源。

外部身分提供者

對於外部身分提供者 (IdPs)，例如 Okta 或 Microsoft Entra ID，您可以使用 IAM Identity Center 透過安全聲明標記語言 (SAML) 2.0 標準來驗證來自 IdPs 身分。SAML 通訊協定不提供查詢 IdP 來了解使用者和群組的方法。您可以將這些使用者和群組佈建到 IAM Identity Center，讓 IAM Identity Center 知道這些使用者和群組。如果您的 IdP 支援 SCIM，您可以使用跨網域身管理 (SCIM) 2.0 版通訊協定，從 IdP 執行使用者和群組資訊自動佈建（同步）到 IAM Identity Center。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。

如需設定身分來源的詳細說明，請參閱 [IAM Identity Center 身分來源教學課程](#)。

Note

如果您打算使用外部身分提供者，請注意，外部 IdP 而非 IAM Identity Center 會管理多重要素驗證 (MFA) 設定。外部身分提供者不支援使用 IAM Identity Center 中的 MFA。如需詳細資訊，請參閱 [MFA 提示使用者](#)。

Note

如果您打算將 IAM Identity Center 複寫到其他區域，則需要設定外部身分提供者。如需包括先決條件的詳細資訊，請參閱 [跨多個使用 IAM Identity Center AWS 區域](#)。

更新防火牆和閘道以允許存取 AWS 存取入口網站

AWS 存取入口網站可讓使用者單一登入存取所有您 AWS 帳戶 和最常用的雲端應用程式，例如 Office 365、Concur、Salesforce 等。您只需選擇入口網站中的 AWS 帳戶 或 應用程式圖示，即可快速啟動多個應用程式。

 Note

AWS 受管應用程式與 IAM Identity Center 整合，並將其用於身分驗證和目錄服務，但可能不會使用 AWS 存取入口網站進行應用程式存取。

如果您使用新一代防火牆 (NGFW) 或安全 Web Gateway (SWG) 等 Web 內容篩選解決方案來篩選特定 AWS 網域或 URL 端點的存取，則必須允許列出與 AWS 存取入口網站相關聯的網域和 URL 端點。

下列清單提供 IPv4 和雙堆疊網域，以及要新增至 Web 內容篩選解決方案允許清單的 URL 端點。

IPv4 允許清單

- *[Directory ID or alias].awsapps.com*
- *[Identity Center instance ID].[Region].portal.amazonaws.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]*.prod.pr.panorama.console.api.aws/panoramamaroute
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

雙堆疊允許清單

- *[Identity Center instance ID].portal.[Region].app.aws*
- *.aws.dev
- *.awsstatic.com

- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

合併允許清單 (IPv4 + 具有回溯相容性的雙堆疊)

- *[Directory ID or alias]*.awsapps.com
- *[Identity Center instance ID]*.*[Region]*.portal.amazonaws.com
- *[Identity Centers instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- oidc.*[Region]*.api.aws
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- sso.*[Region]*.api.aws
- *.sso-portal.*[Region]*.amazonaws.com
- portal.sso.*[Region]*.api.aws
- *[Region]*.prod.pr.panorama.console.api.aws/panoramamaroute
- *[Region]*.signin.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com

- `signin.aws.amazon.com`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`
- `cdn.us-east-1.threat-mitigation.aws.amazon.com`
- `us-east-1.threat-mitigation.aws.amazon.com`
- `amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com`

允許列出網域和 URL 端點的考量事項

除了 AWS 存取入口網站的允許清單要求之外，您使用的其他服務和應用程式可能需要網域的允許清單。

- 若要從存取入口網站 AWS 存取 AWS 帳戶 AWS 管理主控台、和 IAM Identity Center 主控台，您必須允許列出其他網域。如需 AWS 管理主控台 網域清單，請參閱AWS 管理主控台 《入門指南》中的[故障診斷](#)。
- 若要從 AWS 存取入口網站存取 AWS 受管應用程式，您必須允許列出其各自的網域。如需指引，請參閱個別的服務文件。
- 如果您使用外部軟體，例如外部 IdPs (例如 Okta和 Microsoft Entra ID)，則需要將其網域包含在允許清單中。

IAM Identity Center 身分來源教學課程

您可以將 AWS Organizations 管理帳戶中的現有身分來源連線至 [IAM Identity Center 的組織執行個體](#)。如果您沒有現有的身分提供者，您可以直接在預設的 IAM Identity Center 目錄中建立和管理使用者。每個組織可以有一個身分來源。

本節中的教學課程說明如何使用常用的身分來源設定 IAM Identity Center 的組織執行個體、建立管理使用者，以及您是否使用 IAM Identity Center 管理存取 AWS 帳戶、建立和設定許可集。如果您只將 IAM Identity Center 用於應用程式存取，則不需要使用許可集。

這些教學課程不會說明如何設定 IAM Identity Center 的帳戶執行個體。您可以使用帳戶執行個體將使用者和群組指派給應用程式，但無法使用此執行個體類型來管理的使用者存取權 AWS 帳戶。如需詳細資訊，請參閱[IAM Identity Center 的帳戶執行個體](#)。

Note

在開始任何這些教學課程之前，請啟用 IAM Identity Center。如需詳細資訊，請參閱[啟用 IAM Identity Center](#)。

主題

- [使用 Active Directory 做為身分來源](#)
- [Setting up SCIM provisioning between CyberArk and IAM Identity Center](#)
- [使用 和 IAM Identity Center 設定 SAML Google Workspace 和 SCIM](#)
- [使用 IAM Identity Center 與您的 JumpCloud 目錄平台連線](#)
- [使用 和 IAM Identity Center 設定 SAML Microsoft Entra ID 和 SCIM](#)
- [使用 和 IAM Identity Center 設定 SAML Okta 和 SCIM](#)
- [在 OneLogin 和 IAM Identity Center 之間設定 SCIM 佈建](#)
- [搭配 IAM Identity Center 使用 Ping Identity 產品](#)
- [使用預設 IAM Identity Center 目錄設定使用者存取權](#)
- [教學課程影片](#)

使用 Active Directory 做為身分來源

如果您使用 Directory Service 或 Active Directory (AD) 中的自我管理目錄來管理 AWS Managed Microsoft AD 目錄中的使用者，您可以變更 IAM Identity Center 身分來源，以使用這些使用者。建議您在啟用 IAM Identity Center 並選擇身分來源時，考慮連接此身分來源。在預設 Identity Center 目錄中建立任何使用者和群組之前執行此操作，可協助您避免稍後變更身分來源時所需的其他組態。

若要使用 Active Directory 做為您的身分來源，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，則必須在設定 AWS Managed Microsoft AD 目錄 AWS 區域的相同中啟用 IAM Identity Center。IAM Identity Center 會將指派資料存放在與目錄相同的區域中。若要管理 IAM Identity Center，您可能需要切換到已設定 IAM Identity Center 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。
- 使用管理帳戶中的 Active Directory：

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 AWS Managed Microsoft AD 一次只能連接一個 AD Connector 目錄或中的一個目錄。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 中的目錄 AWS Managed Microsoft AD 連接至 IAM Identity Center](#)
- [將 Active Directory 中的自我管理目錄連接到 IAM Identity Center](#)
- 使用位於委派管理員帳戶中的 Active Directory：

如果您計劃啟用 IAM Identity Center 委派管理員，並使用 Active Directory 作為 IAM Identity Center 身分來源，則可以使用位於委派管理員帳戶中的 AWS 目錄中設定的現有 AD Connector 或 AWS Managed Microsoft AD 目錄。

如果您決定將 IAM Identity Center 身分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，則目錄必須位於（由擁有）IAM Identity Center 委派管理員成員帳戶中，如果存在的話，則必須位於管理帳戶中。

本教學課程會引導您使用 Active Directory 做為 IAM Identity Center 身分來源的基本設定。

步驟 1：連接 Active Directory 並指定使用者

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至 IAM Identity Center。

 Note

如果您計劃連接 Active Directory 中的 AWS Managed Microsoft AD 目錄或自我管理的目錄，且並未搭配使用 RADIUS MFA AWS Directory Service，請在 IAM Identity Center 中啟用 MFA。

AWS Managed Microsoft AD

1. 檢閱 中的指引[Microsoft AD 目錄](#)。
2. 請遵循 [將 中的目錄 AWS Managed Microsoft AD 連接至 IAM Identity Center](#) 中的步驟。
3. 設定 Active Directory 以同步您要將管理許可授予 IAM Identity Center 的使用者。如需詳細資訊，請參閱[將管理使用者同步至 IAM Identity Center](#)。

Active Directory 中的自我管理目錄

1. 檢閱 中的指引[Microsoft AD 目錄](#)。
2. 請遵循 [將 Active Directory 中的自我管理目錄連接到 IAM Identity Center](#) 中的步驟。
3. 設定 Active Directory 以同步您要將管理許可授予 IAM Identity Center 的使用者。如需詳細資訊，請參閱[將管理使用者同步至 IAM Identity Center](#)。

步驟 2：將管理使用者同步至 IAM Identity Center

將目錄連線至 IAM Identity Center 之後，您可以指定要授予管理許可的使用者，然後將該使用者從目錄同步到 IAM Identity Center。

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，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，然後選擇新增。
6. 在新增的使用者和群組下，執行下列動作：
 - a. 確認已指定您要授予管理許可的使用者。
 - 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清單中的使用者中。
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出現在清單中。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。您將建立管理許可集，並將使用者指派給該許可集，藉此設定此帳戶的管理存取權。如需詳細資訊，請參閱[建立許可集](#)。

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center 支援將使用者資訊從 自動佈建（同步）CyberArk Directory Platform到 IAM Identity Center。此佈建使用 System for Cross-domain Identity Management (SCIM) v2.0 通訊協定。如需詳細資訊，請參閱[搭配外部身分提供者使用 SAML 和 SCIM 聯合身分](#)。

在您開始部署 SCIM 之前，建議您先檢閱 [使用自動佈建的考量事項](#)。然後繼續檢閱下一節中的其他考量事項。

主題

- [先決條件](#)
- [SCIM 考量事項](#)
- [步驟 1：在 IAM Identity Center 中啟用佈建](#)
- [步驟 2：在 中設定佈建 CyberArk](#)
- [（選用）步驟 3：在 中設定使用者屬性CyberArk以進行 IAM Identity Center 中的存取控制 \(ABAC\)](#)
- [（選用）傳遞屬性以進行存取控制](#)

先決條件

您將需要下列項目才能開始使用：

- CyberArk 訂閱或免費試用。若要註冊免費試用，請造訪 [CyberArk](#)。
- 啟用 IAM Identity Center 的帳戶 ([免費](#))。如需詳細資訊，請參閱[啟用 IAM Identity Center](#)。

- 從CyberArk您的帳戶到 IAM Identity Center 的 SAML 連線，如 [CyberArkIAM Identity Center 文件](#) 所述。
- 將 IAM Identity Center 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 考量事項

以下是對 CyberArk IAM Identity Center 使用聯合時的考量：

- 只有應用程式佈建區段中映射的角色才會同步到 IAM Identity Center。
- 佈建指令碼僅支援預設狀態，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「工作電話」。
- 如果 IAM Identity Center CyberArk 應用程式中的角色映射已變更，則預期下列行為：
 - 如果角色名稱已變更 - 不會變更 IAM Identity Center 中的群組名稱。
 - 如果群組名稱變更 - 新的群組將在 IAM Identity Center 中建立，則舊群組會保留，但不會有任何成員。
- 您可以從 CyberArk IAM Identity Center 應用程式設定使用者同步和取消佈建行為，確保您為組織設定正確的行為。以下是您擁有的選項：
 - 以相同的委託人名稱覆寫（或不覆寫）Identity Center 目錄中的使用者。
 - 從CyberArk角色中移除使用者時，從 IAM Identity Center 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 Identity Center 中啟用佈建

在此第一個步驟中，您可以使用 IAM Identity Center 主控台來啟用自動佈建。

在 IAM Identity Center 中啟用自動佈建

1. 完成先決條件後，請開啟 [IAM Identity Center 主控台](#)。
2. 在左側導覽窗格中選擇設定。
3. 在設定頁面上，找到自動佈建資訊方塊，然後選擇啟用。這會立即在 IAM Identity Center 中啟用自動佈建，並顯示必要的 SCIM 端點和存取字符資訊。
4. 在傳入自動佈建對話方塊中，複製 SCIM 端點和存取字符。稍後在 IdP 中設定佈建時，您需要將這些項目貼入。

- a. SCIM 端點 - 例如，`https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-4444-55555555/scim/v2`
- b. 存取字符 - 選擇顯示字符以複製值。

 Warning

這是您唯一可以取得 SCIM 端點和存取權杖的時間。在繼續之前，請務必複製這些值。您將在本教學稍後輸入這些值，以在 IdP 中設定自動佈建。

5. 選擇關閉。

現在您已在 IAM Identity Center 主控台中設定佈建，您需要使用 CyberArk IAM Identity Center 應用程式完成其餘任務。這些步驟會在下列程序中說明。

步驟 2：在 中設定佈建 CyberArk

在 CyberArk IAM Identity Center 應用程式中使用下列程序，以使用 IAM Identity Center 啟用佈建。此程序假設您已將 CyberArk IAM Identity Center 應用程式新增至 Web 應用程式下的 CyberArk 管理員主控台。如果您尚未這麼做，請參閱 [先決條件](#)，然後完成此程序來設定 SCIM 佈建。

在 中設定佈建 CyberArk

1. 開啟您在為 CyberArk 設定 SAML 時新增的 IAM Identity Center 應用程式 CyberArk (應用程式 > Web 應用程式)。請參閱 [先決條件](#)。
2. 選擇 IAM Identity Center 應用程式，然後前往佈建區段。
3. 勾選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 Identity Center 複製 SCIM 端點值。將該值貼到 SCIM 服務 URL 欄位中，在 CyberArk IAM Identity Center 應用程式中，將授權類型設定為授權標頭。
5. 將標頭類型設定為承載字符。
6. 從先前的程序中，您複製了 IAM Identity Center 中的存取字符值。將該值貼到 IAM Identity Center CyberArk 應用程式的承載字符欄位。
7. 按一下驗證以測試和套用組態。
8. 在同步選項下，選擇您要傳出佈建從中 CyberArk 運作的正確行為。您可以選擇覆寫 (或不覆寫) 具有類似主體名稱的現有 IAM Identity Center 使用者，以及取消佈建行為。

9. 在角色映射下，設定從CyberArk角色到目的地群組下 IAM Identity Center 群組的名稱欄位下的映射。
10. 完成後，請按一下底部的儲存。
11. 若要確認使用者已成功同步至 IAM Identity Center，請返回 IAM Identity Center 主控台並選擇使用者。來自的同步使用者CyberArk會出現在使用者頁面上。這些使用者現在可以指派給帳戶，並且可以在 IAM Identity Center 中連線。

(選用) 步驟 3：在 中設定使用者屬性CyberArk以進行 IAM Identity Center 中的存取控制 (ABAC)

如果您選擇CyberArk設定 IAM Identity Center 的屬性來管理對 AWS 資源的存取，這是 的選用程序。您在 中定義的屬性CyberArk會在 SAML 聲明中傳遞至 IAM Identity Center。然後，您可以在 IAM Identity Center 中建立許可集，以根據您從 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[存取控制的屬性](#)此功能。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 中設定使用者屬性CyberArk，以在 IAM Identity Center 中進行存取控制

1. 開啟您在設定 SAML for CyberArk CyberArk(應用程式 > Web 應用程式) 時安裝的 IAM Identity Center 應用程式。
2. 前往 SAML 回應選項。
3. 在屬性下，依照下列邏輯將相關屬性新增至資料表：
 - a. 屬性名稱是來自的原始屬性名稱CyberArk。
 - b. 屬性值是在 SAML 聲明中傳送至 IAM Identity Center 的屬性名稱。
4. 選擇儲存。

(選用) 傳遞屬性以進行存取控制

您可以選擇性地使用 IAM Identity Center 中的 [存取控制的屬性](#) 功能，傳遞 Name 屬性設為的 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》中的在 [中傳遞工作階段標籤 AWS STS](#)。

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，請為每個標籤加入個別的 `Attribute` 元素。

使用 和 IAM Identity Center 設定 SAML Google Workspace 和 SCIM

如果您的組織正在使用 Google Workspace，您可以將來自 的使用者整合 Google Workspace 到 IAM Identity Center，讓他們能夠存取 AWS 資源。您可以將 IAM Identity Center 身分來源從預設 IAM Identity Center 身分來源變更為，以達成此整合 Google Workspace。

Note

Google Workspace 目前不支援 AWS IAM Identity Center 應用程式中的 SAML 多個宣告使用服務 (ACS) URLs。需要此 SAML 功能才能充分利用 IAM Identity Center 中的 [多區域支援](#)。如果您打算將 IAM Identity Center 複寫到其他區域，請注意，使用單一 ACS URL 可能會影響這些其他區域中的使用者體驗。您的主要區域會繼續正常運作。我們建議您與 IdP 廠商合作，以啟用此功能。如需使用單一 ACS URL 在其他區域中使用者體驗的詳細資訊，請參閱 [the section called “使用沒有多個 ACS URLs AWS 受管應用程式”](#) 和 [the section called “AWS 帳戶 在沒有多個 ACS URLs 存取彈性”](#)。

來自 的使用者資訊會使用跨網域身分管理 (SCIM) 2.0 通訊協定 Google Workspace 同步至 IAM Identity Center。 [SCIM 設定檔](#) 如需詳細資訊，請參閱 [搭配外部身分提供者使用 SAML 和 SCIM 聯合身分](#)。

您可以使用 Google Workspace IAM Identity Center 的 SCIM 端點和 IAM Identity Center 承載字符，在 中設定此連線。當您設定 SCIM 同步時，您可以在 中建立使用者屬性映射 Google Workspace 至 IAM Identity Center 中具名屬性的映射。此映射符合 IAM Identity Center 和 之間的預期使用者屬性 Google Workspace。若要這樣做，您需要將 設定為 Google Workspace 身分提供者，並與您的 IAM Identity Center 連線。

目標

本教學課程中的步驟可協助您在 Google Workspace 和 之間建立 SAML 連線 AWS。稍後，您將同步使用者 Google Workspace 使用 SCIM。為了驗證一切設定正確，在完成設定步驟後，您將以 Google Workspace 使用者身分登入並驗證對 AWS 資源的存取。請注意，本教學課程是以小型 Google Workspace 目錄測試環境為基礎。本教學課程不包含群組和組織單位等目錄結構。完成本教學課程後，您的使用者將可以使用您的 Google Workspace 登入資料存取 AWS 存取入口網站。

Note

若要註冊免費試用，Google Workspace 請造訪 [Google Workspace](#) Google's 網站。
如果您尚未啟用 IAM Identity Center，請參閱 [啟用 IAM Identity Center](#)。

考量事項

- 在 Google Workspace 和 IAM Identity Center 之間設定 SCIM 佈建之前，建議您先檢閱 [使用自動佈建的考量事項](#)。
- 來自 Google Workspace 的 SCIM 自動同步目前僅限於使用者佈建。目前不支援自動群組佈建。您可以使用 AWS CLI Identity Store [create-group](#) 命令或 AWS Identity and Access Management (IAM) API [CreateGroup](#) 手動建立群組。或者，您可以使用 [ssosync](#) 將 Google Workspace 使用者和群組同步至 IAM Identity Center。
- 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 使用者每個資料屬性只有一個值，例如電子郵件地址或電話號碼。具有多個值的任何使用者都將無法同步。如果使用者在其屬性中有多個值，請在嘗試在 IAM Identity Center 中佈建使用者之前移除重複的屬性。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」，所以即使使用者的電話號碼是家用電話或行動電話，也請使用「工作電話」屬性來存放使用者的電話號碼。
- 如果使用者在 IAM Identity Center 中已停用，但在 中仍處於作用中狀態，則屬性仍會同步 Google Workspace。
- 如果 Identity Center 目錄中現有的使用者具有相同的使用者名稱和電子郵件，則會使用來自 的 SCIM 覆寫和同步該使用者 Google Workspace。
- 變更您的身分來源時，還有其他考量。如需詳細資訊，請參閱 [the section called “從 IAM Identity Center 變更為外部 IdP”](#)。

步驟 1：Google Workspace：設定 SAML 應用程式

1. 使用具有超級管理員權限的帳戶登入您的 Google Admin 主控台。

2. 在Google管理員主控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，然後從清單中選擇 Amazon Web Services (SAML) 應用程式。
5. 在Google身分提供者詳細資訊 - Amazon Web Services 頁面上，您可以執行下列其中一項操作：
 - a. 下載 IdP 中繼資料。
 - b. 複製 SSO URL、實體 ID URL 和憑證資訊。

您將需要步驟 2 中的 XML 檔案或 URL 資訊。

6. 在 Google Admin 主控台中移至下一個步驟之前，請將此頁面保持開啟並移至 IAM Identity Center 主控台。

步驟 2：IAM Identity Center 和 Google Workspace：變更 IAM Identity Center 身分來源並Google Workspace設定為 SAML 身分提供者

1. 使用具有管理許可的角色登入 [IAM Identity Center 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，然後選擇變更身分來源。
 - 如果您尚未啟用 IAM Identity Center，請參閱 [啟用 IAM Identity Center](#) 以取得詳細資訊。第一次啟用和存取 IAM Identity Center 之後，您將會抵達儀表板，您可以在其中選取選擇您的身分來源。
4. 在選擇身分來源頁面上，選取外部身分提供者，然後選擇下一步。
5. 設定外部身分提供者頁面隨即開啟。若要完成此頁面和步驟 1 中的Google Workspace頁面，您需要完成下列項目：
 - 在 IAM Identity Center 主控台的身分提供者中繼資料區段下，您將需要執行下列其中一項操作：
 - i. 在 IAM Identity Center 主控台中上傳 Google SAML 中繼資料作為 IdP SAML 中繼資料。
 - ii. 將 Google SSO URL 複製並貼到 IdP 登入 URL 欄位、Google將發行者 URL 貼到 IdP 發行者 URL 欄位，並將Google憑證上傳為 IdP 憑證。

6. 在 IAM Identity Center 主控台的 Identity Provider 中繼資料區段中提供 Google 中繼資料之後，請複製 IAM Identity Assertion Consumer Service (ACS) URL 和 IAM Identity Center 發行者 URL。在下一個步驟中，您將需要在 Google Admin 主控台中提供這些 URLs。
7. 使用 IAM Identity Center 主控台保持頁面開啟，並返回 Google Admin 主控台。您應該位於 Amazon Web Services - 服務提供者詳細資訊頁面。選取繼續。
8. 在服務提供者詳細資訊頁面上，輸入 ACS URL 和實體 ID 值。您在上一個步驟中複製了這些值，它們可以在 IAM Identity Center 主控台中找到。
 - 將 IAM Identity Center Assertion Consumer Service (ACS) URL 貼入 ACS URL 欄位
 - 將 IAM Identity Center 發行者 URL 貼入實體 ID 欄位。
9. 在服務供應商詳細資訊頁面上，完成名稱 ID 下方的欄位，如下所示：
 - 針對名稱 ID 格式，選取 EMAIL
 - 針對名稱 ID，選取基本資料 > 主要電子郵件
10. 選擇繼續。
11. 在屬性映射頁面的屬性下，選擇新增 MAPPING，然後在 Google 目錄屬性下設定這些欄位：
 - 針對 `https://aws.amazon.com/SAML/Attributes/RoleSessionName` 應用程式屬性，從 Google Directory 屬性中選取基本資訊、主要電子郵件欄位。
 - 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 Identity Center 主控台，然後選擇下一步。在檢閱和確認頁面上，檢閱資訊，然後在提供的空格中輸入 ACCEPT。選擇變更身分來源。

您現在可以在 中啟用 Amazon Web Services 應用程式，Google Workspace 以便將使用者佈建至 IAM Identity Center。

步驟 3：Google Workspace：啟用應用程式

1. 返回 Google 管理員主控台和您的 AWS IAM Identity Center 應用程式，您可以在應用程式和 Web 和行動應用程式下找到。
2. 在使用者存取權旁的使用者存取面板中，選擇向下箭頭展開使用者存取權，以顯示服務狀態面板。
3. 在服務狀態面板中，為所有人選擇 ON，然後選擇儲存。

 Note

為了協助維護最低權限原則，我們建議您在完成本教學課程後，將每個人的服務狀態變更為 OFF。只有需要存取 AWS 的使用者才能啟用服務。您可以使用 Google Workspace 群組或組織單位，讓使用者存取使用者的特定子集。

步驟 4：IAM Identity Center：設定 IAM Identity Center 自動佈建

1. 返回 IAM Identity Center 主控台。
2. 在設定頁面上，找到自動佈建資訊方塊，然後選擇啟用。這會立即在 IAM Identity Center 中啟用自動佈建，並顯示必要的 SCIM 端點和存取字符資訊。
3. 在傳入自動佈建對話方塊中，複製下列選項的每個值。在此教學課程的步驟 5 中，您將輸入這些值，以在 中設定自動佈建 Google Workspace。
 - a. SCIM 端點 - 例如，
 - IPv4 `https://scim.Region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - 雙堆疊 `https://scim.Region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. 存取字符 - 選擇顯示字符以複製值。

 Warning

這是您唯一可以取得 SCIM 端點和存取權杖的時間。在繼續之前，請務必複製這些值。

4. 選擇關閉。

現在您已在 IAM Identity Center 主控台中設定佈建，在下一個步驟中，您將在 中設定自動佈建 Google Workspace。

步驟 5：Google Workspace：設定自動佈建

1. 返回Google管理員主控台和您的 AWS IAM Identity Center 應用程式，您可以在應用程式和 Web 和行動應用程式下找到。在自動佈建區段中，選擇設定自動佈建。
2. 在先前的程序中，您會在 IAM Identity Center 主控台中複製存取字符值。將該值貼到存取字符欄位中，然後選擇繼續。此外，在先前的程序中，您會在 IAM Identity Center 主控台中複製 SCIM 端點值。將該值貼入端點 URL 欄位，然後選擇繼續。
3. 確認所有強制性 IAM Identity Center 屬性（標記為 * 的屬性）都對應至Google Cloud Directory屬性。如果沒有，請選擇向下箭頭並對應至適當的屬性。選擇繼續。
4. 在佈建範圍區段中，您可以選擇具有Google Workspace目錄的群組，以提供 Amazon Web Services 應用程式的存取權。略過此步驟，然後選取繼續。
5. 在取消佈建區段中，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，您可以指定取消佈建開始之前的時間量：
 - 24 小時內
 - 一天後
 - 七天後
 - 30 天後

每種情況都有時間設定，用於暫停帳戶存取的時間，以及刪除帳戶的時間。

Tip

刪除使用者帳戶之前，請務必設定比暫停使用者帳戶更長的時間。

6. 選擇完成。您會返回 Amazon Web Services 應用程式頁面。
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

如果使用者未開啟 IAM Identity Center，則會停用啟用滑桿。選擇使用者存取並 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 Identity Center，請返回 IAM Identity Center 主控台並選擇 使用者。使用者 頁面列出您Google Workspace目錄中由 SCIM 建立的使用者。如果使用者尚未列

出，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，它在幾分鐘內完成。請務必每隔幾分鐘重新整理瀏覽器視窗。

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

恭喜您！

您已成功在 Google Workspace 和 之間設定 SAML 連線，AWS 並已驗證自動佈建是否正常運作。您現在可以將這些使用者指派給 IAM Identity Center 中的帳戶和應用程式。在本教學課程中，在下一個步驟中，我們將其中一個使用者授予管理帳戶的管理許可，以指定為 IAM Identity Center 管理員。

傳遞存取控制的屬性 - 選用

您可以選擇性地使用 IAM Identity Center 中的 [存取控制的屬性](#) 功能，傳遞 Name 屬性設為的 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》中的在 [中傳遞工作階段標籤 AWS STS](#)。

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，請為每個標籤加入個別的 Attribute 元素。

將存取權指派給 AWS 帳戶

下列步驟僅需要授予 AWS 帳戶 的存取權。這些步驟不需要授予 AWS 應用程式存取權。

Note

若要完成此步驟，您需要 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱[IAM Identity Center 的組織和帳戶執行個體](#)。

步驟 1：IAM Identity Center：授予 Google Workspace 使用者帳戶存取權

1. 返回 IAM Identity Center 主控台。在 IAM Identity Center 導覽窗格中的多帳戶許可下，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及其下的帳戶。選取管理帳戶的核取方塊，然後選取指派使用者或群組。
3. 此時會顯示指派使用者和群組工作流程。它包含三個步驟：
 - a. 針對步驟 1：選取使用者和群組，選擇將執行管理員任務功能的使用者。然後選擇下一步。
 - b. 針對步驟 2：選取許可集選擇建立許可集，以開啟新標籤，逐步引導您完成建立許可集所涉及的三個子步驟。
 - i. 對於步驟 1：選取許可集類型完成下列項目：
 - 在許可集類型中，選擇預先定義的許可集。
 - 在預先定義許可集的政策中，選擇 AdministratorAccess。
 - 選擇下一步。
 - ii. 針對步驟 2：指定許可集詳細資訊，保留預設設定，然後選擇下一步。

預設設定會建立名為 *AdministratorAccess* 的許可集，並將工作階段持續時間設定為一小時。
 - iii. 針對步驟 3：檢閱和建立，確認許可集類型使用 AWS 受管政策 AdministratorAccess。選擇建立。在許可集頁面上會出現通知，通知您已建立許可集。您現在可以在 Web 瀏覽器中關閉此索引標籤。
 - iv. 在指派使用者和群組瀏覽器索引標籤上，您仍在步驟 2：選取您從中開始建立許可集工作流程的許可集。
 - v. 在許可集區域中，選擇重新整理按鈕。您建立的 *AdministratorAccess* 許可集會出現清單中。選取該許可集的核取方塊，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許可集，然後選擇提交。

頁面會以 AWS 帳戶 正在設定 的訊息進行更新。等待程序完成。

您會返回 AWS 帳戶 頁面。通知訊息會通知您 AWS 帳戶，您的 已重新佈建，並已套用更新的許可集。當使用者登入時，他們可以選擇 *AdministratorAccess* 角色。

Note

來自的 SCIM 自動同步 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 為 Google Workspace 使用者建立群組 AWS 管理主控台。佈建使用者之後，您可以使用 AWS CLI Identity Store [create-group](#) 命令或 IAM API [CreateGroup](#) 建立群組。

步驟 2：Google Workspace：確認 Google Workspace 使用者存取 AWS 資源

1. Google 使用測試使用者帳戶登入。若要了解如何將使用者新增至 Google Workspace，請參閱 [Google Workspace 文件](#)。
2. 選取 Google apps 啟動器（鬆餅）圖示。
3. 捲動至自訂應用程式所在的 Google Workspace 應用程式清單底部。Amazon Web Services 應用程式隨即顯示。
4. 選取 Amazon Web Services 應用程式。您已登入 AWS 存取入口網站，可以看到 AWS 帳戶 圖示。展開該圖示以查看使用者可以存取 AWS 帳戶 的清單。在本教學課程中，您只使用單一帳戶，因此展開圖示只會顯示一個帳戶。
5. 選取帳戶以顯示使用者可用的許可集。在本教學課程中，您已建立 AdministratorAccess 許可集。
6. 許可集旁的是該許可集可用的存取類型的連結。當您建立許可集時，您指定同時啟用管理主控台和程式設計存取，因此這兩個選項都存在。選取管理主控台以開啟 AWS 管理主控台。
7. 使用者已登入 主控台。

後續步驟

現在您已 Google Workspace 在 IAM Identity Center 中將設定為身分提供者和佈建使用者，您可以：

- 使用 AWS CLI Identity Store [create-group](#) 命令或 IAM API [CreateGroup](#) 為您的使用者建立群組。

群組在將存取權指派給 AWS 帳戶 和 應用程式時非常有用。您可以將許可授予群組，而不是個別指派每個使用者。稍後，當您從群組新增或移除使用者時，使用者會動態取得或失去您指派給群組的帳戶和應用程式的存取權。

- 根據任務函數設定許可，請參閱[建立許可集](#)。

許可集定義使用者和群組對 的存取層級 AWS 帳戶。許可集存放在 IAM Identity Center 中，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 Identity Center 管理員，您偶爾需要用較新的 IdP 憑證取代較舊的 IdP 憑證。例如，當憑證上的過期日期接近時，您可能需要取代 IdP 憑證。使用較新的憑證取代較舊憑證的程序稱為憑證輪換。請務必檢閱如何[管理的 SAML 憑證](#) Google Workspace。

疑難排解

如需使用 進行一般 SCIM 和 SAML 故障診斷 Google Workspace，請參閱下列章節：

- [特定使用者無法從外部 SCIM 供應商同步到 IAM Identity Center](#)
- [IAM Identity Center 建立的 SAML 聲明內容相關問題](#)
- [使用外部身分提供者佈建使用者或群組時發生重複的使用者或群組錯誤](#)
- 如需 Google Workspace 故障診斷，請參閱 [Google Workspace 文件](#)。

下列資源可協助您在使用 時進行故障診斷 AWS：

- [AWS re:Post](#) - 尋找FAQs和其他資源的連結，以協助您疑難排解問題。
- [AWS 支援](#) - 取得技術支援

使用 IAM Identity Center 與您的JumpCloud目錄平台連線

IAM Identity Center 支援將使用者資訊從 JumpCloud Directory Platform 自動佈建（同步）到 IAM Identity Center。此佈建使用[安全性聲明標記語言 \(SAML\) 2.0](#) 通訊協定。如需詳細資訊，請參閱[搭配外部身分提供者使用 SAML 和 SCIM 聯合身分](#)。

您可以使用 IAM Identity Center SCIM 端點和存取權杖JumpCloud在 中設定此連線。當您設定 SCIM 同步時，您可以在 中建立使用者屬性映射JumpCloud至 IAM Identity Center 中具名屬性的映射。這會導致 IAM Identity Center 和 之間的預期屬性相符JumpCloud。

本指南以 2021 年 6 月JumpCloud的 為基礎。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 設定使用者身分驗證的注意事項。

下列步驟會逐步解說如何使用 SCIM 通訊協定，將使用者和群組從 自動佈建JumpCloud至 IAM Identity Center。

Note

在您開始部署 SCIM 之前，建議您先檢閱 [使用自動佈建的考量事項](#)。然後繼續檢閱下一節的其他考量事項。

主題

- [先決條件](#)
- [SCIM 考量事項](#)
- [步驟 1：在 IAM Identity Center 中啟用佈建](#)
- [步驟 2：在 中設定佈建 JumpCloud](#)
- [\(選用\) 步驟 3：在 中設定使用者屬性JumpCloud，以在 IAM Identity Center 中進行存取控制](#)
- [\(選用\) 傳遞屬性以進行存取控制](#)

先決條件

您將需要下列項目才能開始使用：

- JumpCloud 訂閱或免費試用。若要註冊免費試用，請造訪 [JumpCloud](#)。
- 啟用 IAM Identity Center 的帳戶 ([免費](#))。如需詳細資訊，請參閱[啟用 IAM Identity Center](#)。
- 從JumpCloud您的帳戶到 IAM Identity Center 的 SAML 連線，如 [JumpCloudIAM Identity Center 的文件](#)中所述。
- 如果您將 IAM Identity Center 複製到其他區域，則必須更新身分提供者組態，以啟用受 AWS 管應用程式和 AWS 帳戶 來自這些區域的存取。如需詳細資訊，請參閱[the section called “步驟 3：更新外部 IdP 設定”](#)。如需其他詳細資訊，請參閱 JumpCloud 文件。

- 將 IAM Identity Center 連接器與您要允許存取 AWS 帳戶的群組建立關聯。

SCIM 考量事項

以下是對 JumpCloud IAM Identity Center 使用聯合時的考量事項。

- 只有與 中的 AWS 單一登入連接器相關聯的群組 JumpCloud 才會與 SCIM 同步。
- 只能同步一個電話號碼屬性，預設值為「工作電話」。
- JumpCloud 目錄中的使用者必須設定名字和姓氏，才能透過 SCIM 同步至 IAM Identity Center。
- 如果使用者在 IAM Identity Center 中已停用，但仍在 中啟用，則屬性仍會同步 JumpCloud。
- 您可以選擇僅啟用使用者資訊的 SCIM 同步，方法是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」。

步驟 1：在 IAM Identity Center 中啟用佈建

在此第一個步驟中，您可以使用 IAM Identity Center 主控台來啟用自動佈建。

在 IAM Identity Center 中啟用自動佈建

1. 完成先決條件後，請開啟 [IAM Identity Center 主控台](#)。
2. 在左側導覽窗格中選擇設定。
3. 在設定頁面上，找到自動佈建資訊方塊，然後選擇啟用。這會立即在 IAM Identity Center 中啟用自動佈建，並顯示必要的 SCIM 端點和存取字符資訊。
4. 在傳入自動佈建對話方塊中，複製 SCIM 端點和存取字符。稍後在 IdP 中設定佈建時，您需要將這些項目貼入。
 - a. SCIM 端點 - 例如，`https://scim.us-east-2.amazonaws.com/11111111-2222-3333-444-55555555/scim/v2`
 - b. 存取字符 - 選擇顯示字符以複製值。

Warning

這是您唯一可以取得 SCIM 端點和存取權杖的時間。在繼續之前，請務必複製這些值。您將在本教學課程稍後輸入這些值，以在 IdP 中設定自動佈建。

5. 選擇關閉。

現在您已在 IAM Identity Center 主控台中設定佈建，您需要使用 JumpCloud IAM Identity Center 連接器完成其餘任務。這些步驟會在下列程序中說明。

步驟 2：在 中設定佈建 JumpCloud

在 JumpCloud IAM Identity Center 連接器中使用下列程序，以使用 IAM Identity Center 啟用佈建。此程序假設您已將 JumpCloud IAM Identity Center 連接器新增至 JumpCloud 管理員入口網站和群組。如果您尚未這麼做，請參閱 [先決條件](#)，然後完成此程序以設定 SCIM 佈建。

在 中設定佈建 JumpCloud

1. 開啟您在設定 SAML for JumpCloud JumpCloud(使用者身分驗證 > IAM Identity Center) 時安裝的 IAM Identity Center 連接器。請參閱 [先決條件](#)。
2. 選擇 IAM Identity Center 連接器，然後選擇第三個索引標籤 Identity Management。
3. 如果您希望群組進行 SCIM 同步，請勾選在此應用程式中啟用使用者群組和群組成員資格的管理方塊。
4. 按一下設定。
5. 在先前的程序中，您會在 IAM Identity Center 中複製 SCIM 端點值。將該值貼到 JumpCloud IAM Identity Center 連接器的基本 URL 欄位中。
6. 從上一個程序中，您複製了 IAM Identity Center 中的存取字符值。將該值貼到 JumpCloud IAM Identity Center 連接器的字符金鑰欄位中。
7. 按一下啟用以套用組態。
8. 請確定已啟用單一登入旁的綠色指標。
9. 移至第四個索引標籤 使用者群組，並檢查您要使用 SCIM 佈建的群組。
10. 完成後，請按一下底部的儲存。
11. 若要確認使用者已成功同步至 IAM Identity Center，請返回 IAM Identity Center 主控台並選擇使用者。來自 的同步使用者 JumpCloud 會出現在使用者頁面上。這些使用者現在可以指派給 IAM Identity Center 內的帳戶。

(選用) 步驟 3：在 中設定使用者屬性 JumpCloud，以在 IAM Identity Center 中進行存取控制

JumpCloud 如果您選擇設定 IAM Identity Center 的屬性來管理對 AWS 資源的存取，這是 的選用程序。您在 中定義的屬性 JumpCloud 會在 SAML 聲明中傳遞至 IAM Identity Center。然後，您可以在 IAM Identity Center 中建立許可集，以根據您從 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[存取控制功能的屬性](#)。如需如何執行此操作的詳細資訊，請參閱[啟用和設定存取控制的屬性](#)。

在 中設定使用者屬性JumpCloud，以在 IAM Identity Center 中進行存取控制

1. 開啟您在為 JumpCloud 設定 SAML 時安裝的 IAM Identity Center 連接器 JumpCloud(使用者身分驗證 > IAM Identity Center)。
2. 選擇 IAM Identity Center 連接器。然後，選擇第二個索引標籤 IAM Identity Center。
3. 在此索引標籤底部，您有使用者屬性映射，選擇新增屬性，然後執行下列動作：您必須對要新增的每個屬性執行這些步驟，以便在 IAM Identity Center 中用於存取控制。
 - a. 在服務提供屬性名稱欄位中，輸入 **AttributeName** 以您在 IAM Identity Center 中預期的屬性名稱`https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`。取代。例如 `https://aws.amazon.com/SAML/Attributes/AccessControl:Email`。
 - b. 在JumpCloud屬性名稱欄位中，從您的JumpCloud目錄中選擇使用者屬性。例如，電子郵件（工作）。
4. 選擇儲存。

（選用）傳遞屬性以進行存取控制

您可以選擇性地使用 IAM Identity Center 中的 [存取控制的屬性](#) 功能，傳遞 Name 屬性設為的 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》中的在 [中傳遞工作階段標籤 AWS STS](#)。

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，請為每個標籤加入個別的Attribute元素。

使用 和 IAM Identity Center 設定 SAML Microsoft Entra ID 和 SCIM

AWS IAM Identity Center 支援與[安全性聲明標記語言 \(SAML\) 2.0](#) 整合，以及使用跨網域身分管理 (SCIM) 2.0 通訊協定，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) 到 IAM Identity Center。 [SCIM 設定檔](#)如需詳細資訊，請參閱[搭配外部身分提供者使用 SAML 和 SCIM 聯合身分](#)。

目標

在本教學課程中，您將設定測試實驗室，並在 和 IAM Identity Center 之間設定 SAML 連線和 SCIM Microsoft Entra ID 佈建。在初始準備步驟期間，您會在 Microsoft Entra ID 和 IAM Identity Center 中建立測試使用者 (Nikki Wolf)，以雙向測試 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)，以驗證 中的新屬性 Microsoft Entra ID 是否如預期同步至 IAM Identity Center。

先決條件

您必須先設定下列項目，才能開始使用本教學課程：

- Microsoft Entra ID 租戶。如需詳細資訊，請參閱[快速入門：在文件中設定租用戶](#)。Microsoft
- 已啟用 AWS IAM Identity Center 的帳戶。如需詳細資訊，請參閱 AWS IAM Identity Center 《使用者指南》中的[啟用 IAM Identity Center](#)。

考量事項

以下是有關 的重要考量 Microsoft Entra ID，這可能會影響您計劃使用 SCIM v2 通訊協定在生產環境中使用 IAM Identity Center 實作[自動佈建](#)的方式。

自動佈建

在您開始部署 SCIM 之前，建議您先檢閱 [使用自動佈建的考量事項](#)。

存取控制的屬性

存取控制的屬性會用於 許可政策，以決定身分來源中誰可以存取您的 AWS 資源。如果從 中的使用者移除屬性 Microsoft Entra ID，則不會從 IAM Identity Center 中的對應使用者移除該屬性。這是 中的已知限制 Microsoft Entra ID。如果屬性在使用者上變更為不同的 (非空白) 值，則該變更會同步至 IAM Identity Center。

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。只有屬於明確指派群組的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使用者或群組的群組成員（直接指派的群組成員的使用者或群組）。如需詳細資訊，請參閱 Microsoft 文件中的以[指派為基礎的範圍](#)。或者，您可以使用 [IAM Identity Center 可設定的 AD 同步](#)，將Active Directory群組與IAM Identity Center 整合。

動態群組

Microsoft Entra ID 使用者佈建服務可以在[動態群組](#)中讀取和佈建使用者。如需使用動態群組時顯示使用者和群組結構的範例，以及它們在 IAM Identity Center 中的顯示方式，請參閱下文。這些使用者和群組是透過 SCIM 從 佈建Microsoft Entra ID至 IAM Identity Center

例如，如果動態群組的Microsoft Entra ID結構如下：

1. 群組 A 具有成員 ua1、ua2
2. 群組 B 與成員 ub1
3. 群組 C 與成員 uc1
4. 群組 K 具有包含群組 A、B、C 成員的規則
5. 群組 L 具有包含成員群組 B 和 C 的規則

使用者和群組資訊透過 SCIM 從 佈建Microsoft Entra ID至 IAM Identity Center 後，結構將如下所示：

1. 群組 A 具有成員 ua1、ua2
2. 群組 B 與成員 ub1
3. 群組 C 與成員 uc1
4. 群組 K 具有成員 ua1、ua2、ub1、uc1
5. 群組 L 與成員 ub1、uc1

當您使用動態群組設定自動佈建時，請謹記下列考量。

- 動態群組可以包含巢狀群組。不過，Microsoft Entra ID佈建服務不會壓平巢狀群組。例如，如果您的動態群組有下列Microsoft Entra ID結構：
 - 群組 A 是群組 B 的父項。
 - 群組 A 以成員身分擁有 ua1。
 - B 群組以成員身分擁有 ub1。

包含群組 A 的動態群組只會包含群組 A 的直接成員（即 ua1）。它不會遞迴地包含群組 B 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 文件中的[預覽限制](#)。

步驟 1：準備您的 Microsoft 租用戶

在此步驟中，您將逐步了解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 Microsoft Entra ID 的測試使用者。

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，您會在 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 SAML 連線 AWS。

1. 至少以雲端應用程式管理員身分登入 [Microsoft Entra 管理中心](#)。
2. 導覽至身分 > 應用程式 > 企業應用程式，然後選擇新應用程式。
3. 在瀏覽 Microsoft Entra Gallery 頁面上，**AWS IAM Identity Center**在搜尋方塊中輸入。
4. AWS IAM Identity Center 從結果中選取。
5. 選擇建立。

Step 1.2 >

步驟 1.2：在 中建立測試使用者 Microsoft Entra ID

Nikki Wolf 是您將在此程序中建立 Microsoft Entra ID 的測試使用者名稱。

1. 在 [Microsoft Entra 管理中心](#) 主控台中，導覽至身分 > 使用者 > 所有使用者。
2. 選取新使用者，然後在畫面頂端選擇建立新使用者。
3. 在使用者主體名稱中，輸入 **NikkiWolf**，然後選取您偏好的網域和延伸。例如，NikkiWolf@*example.org*。
4. 在顯示名稱中，輸入 **NikkiWolf**。
5. 在密碼中，輸入高強度密碼或選取眼睛圖示以顯示自動產生的密碼，然後複製或寫下顯示的值。
6. 選擇屬性，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：在將許可指派給 Nikki 之前，先測試 Nikki 的體驗 AWS IAM Identity Center

在此程序中，您將驗證 Nikki 可以成功登入其 Microsoft [My Account 入口網站](#)的內容。

1. 在相同的瀏覽器中，開啟新標籤，前往[我的帳戶入口網站](#)登入頁面，然後輸入 Nikki 的完整電子郵件地址。例如，NikkiWolf@*example.org*。
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. 在必要動作頁面上，選擇稍後請求以略過其他安全方法的提示。
4. 在我的帳戶頁面的左側導覽窗格中，選擇我的應用程式。請注意，除了增益集之外，目前不會顯示任何應用程式。您將新增應用程式，該AWS IAM Identity Center應用程式將在稍後的步驟中顯示在這裡。

Step 1.4

步驟 1.4：在 中將許可指派給 Nikki Microsoft Entra ID

現在您已驗證 Nikki 可以成功存取我的帳戶入口網站，請使用此程序將她的使用者指派給AWS IAM Identity Center應用程式。

1. 在 [Microsoft Entra 管理中心](#)主控台中，導覽至身分 > 應用程式 > 企業應用程式，然後從AWS IAM Identity Center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)。您可以忽略訊息，指出群組無法進行指派。本教學課程不會使用群組進行指派。
4. 在新增指派頁面的使用者下，選擇未選取。
5. 選取 NikkiWolf，然後選擇選取。
6. 在 Add Assignment (新增指派) 頁面上，選擇 Assign (指派)。NikkiWolf 現在會出現在指派給AWS IAM Identity Center應用程式的使用者清單中。

步驟 2：準備 AWS 您的帳戶

在此步驟中，您將逐步說明如何使用 IAM Identity Center 來設定存取許可（透過許可集）、手動建立對應的 Nikki Wolf 使用者，以及指派必要的許可給她以管理 資源 AWS。

Step 2.1 >

步驟 2.1：在 中建立 RegionalAdmin 許可集 IAM Identity Center

此許可集將用於授予 Nikki 從 中的 AWS 帳戶頁面管理區域所需的必要帳戶許可 AWS 管理主控台。預設會拒絕檢視或管理 Nikki 帳戶任何其他資訊的所有其他許可。

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在多帳戶許可下，選擇許可集。
3. 選擇 Create permission set (建立許可集合)。
4. 在選取許可集類型頁面上，選取自訂許可集，然後選擇下一步。
5. 選取內嵌政策以展開政策，然後使用下列步驟為許可集建立政策：
 - a. 選擇新增陳述式以建立政策陳述式。
 - b. 在編輯陳述式下，從清單中選擇帳戶，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. 在指定許可集詳細資訊頁面的許可集名稱下，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)。您應該會在許可集清單中看到 RegionalAdmin。

Step 2.2 >

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

由於 SAML 通訊協定不提供查詢 IdP (Microsoft Entra ID) 和自動在 IAM Identity Center 中在此處建立使用者的機制，請使用下列程序在 IAM Identity Center 中手動建立使用者，以鏡射 中 Nikki Wolfs 使用者的核心屬性Microsoft Entra ID。

1. 開啟 [IAM Identity Center 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. 針對使用者名稱和電子郵件地址 – 輸入您在建立Microsoft Entra ID使用者時所使用的相同 **NikkiWolf@*yourcompanydomain.extension***。例如，NikkiWolf@*example.org*。
 - b. 確認電子郵件地址 – 重新輸入上一個步驟的電子郵件地址
 - 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，然後選擇新增使用者。
4. 請選擇 Close (關閉)。

Step 2.3

步驟 2.3：將 Nikki 指派給 中的 RegionalAdmin 許可集 IAM Identity Center

您可以在此處找到 Nikki 將在 AWS 帳戶 其中管理區域的，然後指派她成功存取 AWS 存取入口網站所需的必要許可。

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在多帳戶許可下，選擇 AWS 帳戶。

3. 選取您要授予 Nikki 存取權以管理區域的帳戶名稱 (例如##) 旁的核取方塊，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 旁的方塊，然後選擇下一步。
5. Example

<caption>On the 選取許可集 page, choose the RegionalAdmin permission set created in Step 2.1, and then choose 下一頁.</caption>
6. 在檢閱和提交頁面上，檢閱您的選擇，然後選擇提交。

步驟 3：設定和測試 SAML 連線

在此步驟中，您會使用 中的 AWS IAM Identity Center 企業應用程式 Microsoft Entra ID 以及 IAM Identity Center 中的外部 IdP 設定來設定 SAML 連線。

Step 3.1 >

步驟 3.1：從 IAM Identity Center 收集所需的服務供應商中繼資料

在此步驟中，您將從 IAM Identity Center 主控台中啟動變更身分來源精靈，並擷取下一個步驟 Microsoft Entra ID 中設定與連線時需要輸入的中繼資料檔案和 AWS 特定登入 URL。

1. 在 [IAM Identity Center 主控台](#) 中，選擇設定。
2. 在設定頁面上，選擇身分來源索引標籤，然後選擇動作 > 變更身分來源。
3. 在選擇身分來源頁面上，選取外部身分提供者，然後選擇下一步。
4. 在設定外部身分提供者頁面的服務提供者中繼資料下，選擇預設 IPv4 或雙堆疊。您可以在完成身分來源變更後下載服務提供者中繼資料檔案。
5. 在相同區段中，找到 AWS 存取入口網站登入 URL 值並將其複製。在下一個步驟中出現提示時，您將需要輸入此值。
6. 保持開啟此頁面，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程序。

Step 3.2 >

步驟 3.2：在 中設定 AWS IAM Identity Center 企業應用程式 Microsoft Entra ID

此程序會使用您在最後一個步驟中取得的中繼資料檔案和登入 URL 中的值，在 Microsoft 端建立一半的 SAML 連線。

1. 在 [Microsoft Entra 管理員中心](#) 主控台中，導覽至身分 > 應用程式 > 企業應用程式，然後選擇 AWS IAM Identity Center。
2. 在左側，選擇 2. 設定單一登入。
3. 在使用 SAML 設定單一登入頁面上，選擇 SAML。然後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，確認識別符和回覆 URL（聲明消費者服務 URL）值現在都指向中的端點 AWS。
 - 識別符 - 這是來自 IAM Identity Center 的發行者 URL。無論您使用 IPv4-only 或雙堆疊端點，都適用相同的值。
 - 回覆 URL（聲明消費者服務 URL）- 此處的值包含來自 IAM Identity Center 所有已啟用區域的 IPv4-only 和雙堆疊端點。您可以使用主要區域的 ACS URL 做為預設 URL，以便在使用者從啟動 Amazon Web Services 應用程式時重新導向至主要區域 Microsoft Entra ID。如需 ACS URLs 的詳細資訊，請參閱 [主要和其他中的 ACS 端點 AWS 區域](#)。
 - （選用）如果您將 IAM Identity Center 複寫到其他區域，您也可以在中 Microsoft Entra ID 為每個其他區域的 AWS 存取入口網站建立書籤應用程式。這可讓您的使用者從存取其他區域中的 AWS 存取入口網站 Microsoft Entra ID。請務必授予使用者存取中書籤應用程式的許可 Microsoft Entra ID。如需詳細資訊，請參閱 [Microsoft Entra ID 文件](#)。如果您計劃稍後將 IAM Identity Center 複寫到其他區域，請造訪 [Microsoft Entra ID 用於存取其他區域的組態](#) 以取得指引，了解如何在此初始設定後啟用其他區域的存取權。
5. 在登入 URL（選用）下，貼上您在上一個步驟（**Step 3.1**）中複製的 AWS 存取入口網站登入 URL 值，選擇儲存，然後選擇 X 關閉視窗。
6. 如果系統提示您使用測試單一登入 AWS IAM Identity Center，請選擇否 我稍後會測試。您將在後續步驟中執行此驗證。
7. 在使用 SAML 設定單一登入頁面上，在聯合中繼資料 XML 旁的 SAML 憑證區段中，選擇下載以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 Identity Center 主控台內的變更身分來源精靈，以完成 SAML 連線的第二部分 AWS。

1. 返回您在 IAM Identity Center 主控台 **Step 3.1** 中保持開啟狀態的瀏覽器工作階段。
2. 在設定外部身分提供者頁面的身分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 Microsoft Entra ID 中從中下載的身分提供者中繼資料檔案，然後選擇開啟。
3. 選擇下一步。
4. 在您閱讀免責聲明並準備好繼續之後，請輸入 **ACCEPT**。
5. 選擇變更身分來源以套用您的變更。

Step 3.4 >

步驟 3.4：測試 Nikki 是否已重新導向至 AWS 存取入口網站

在此程序中，您將使用 Nikki 的登入資料登入 Microsoft 的 My Account 入口網站，以測試 SAML 連線。驗證後，您將選取 AWS IAM Identity Center 應用程式，將 Nikki 重新導向至 AWS 存取入口網站。

1. 前往 [我的帳戶入口網站](#) 登入頁面，然後輸入 Nikki 的完整電子郵件地址。例如，**NikkiWolf@example.org**。
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窗格中，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其他身分驗證。
5. 在 Microsoft 的登入頁面上，選擇您的 NikkiWolf 登入資料。如果提示再次進行身分驗證，請再次選擇您的 NikkiWolf 登入資料。這應該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，請檢查以確保您在 中輸入的 AWS 存取入口網站登入 URL 值與您從 複製的值 **Step 3.2** 相符 **Step 3.1**。

6. 確認您的 AWS 帳戶 顯示器。

Tip

如果頁面空白且無 AWS 帳戶 顯示，請確認 Nikki 已成功指派給 RegionalAdmin 許可集（請參閱 **Step 2.3**）。

Step 3.5

步驟 3.5：測試 Nikki 管理她的存取層級 AWS 帳戶

在此步驟中，您將檢查以判斷 Nikki 管理她區域設定的存取層級 AWS 帳戶。Nikki 應該只有夠的管理員權限，才能從帳戶頁面管理區域。

1. 在 AWS 存取入口網站中，選擇帳戶索引標籤以顯示帳戶清單。隨即顯示與您定義許可集之任何帳戶相關聯的帳戶名稱、帳戶 IDs 和電子郵件地址。
2. 選擇您套用許可集的帳戶名稱（例如##）（請參閱 **Step 2.3**）。這將擴展 Nikki 可以從中選擇以管理其帳戶的許可集清單。
3. 在 RegionalAdmin 旁邊，選擇 管理主控台以擔任您在 RegionalAdmin 許可集中定義的角色。這會將您重新導向至 AWS 管理主控台 首頁。
4. 在主控台的右上角，選擇您的帳戶名稱，然後選擇帳戶。這將帶您前往帳戶頁面。請注意，此頁面的所有其他區段會顯示訊息，指出您沒有檢視或修改這些設定的必要許可。
5. 在帳戶頁面上，向下捲動至AWS 區域區段。選取資料表中任何可用區域的核取方塊。請注意，Nikki 確實具備必要許可，可如預期啟用或停用其帳戶的 區域清單。

做得很好！

步驟 1 到 3 可協助您成功實作和測試 SAML 連線。現在，為了完成教學課程，建議您繼續進行步驟 4 以實作自動佈建。

步驟 4：設定和測試您的 SCIM 同步

在此步驟中，您將使用 SCIM v2.0 通訊協定，將使用者資訊從 [自動佈建](#)（同步）Microsoft Entra ID到 IAM Identity Center。您可以使用 Microsoft Entra ID IAM Identity Center 的 SCIM 端點和 IAM Identity Center 自動建立的承載字符，在 中設定此連線。

當您設定 SCIM 同步時，您會在 中建立使用者屬性映射Microsoft Entra ID至 IAM Identity Center 中具名屬性的映射。這會導致 IAM Identity Center 和 之間的預期屬性相符Microsoft Entra ID。

下列步驟說明如何使用 中的 IAM Identity Center 應用程式，將主要位於 中的使用者自動佈建Microsoft Entra ID至 IAM Identity CenterMicrosoft Entra ID。

Step 4.1 >

步驟 4.1：在 中建立第二個測試使用者 Microsoft Entra ID

基於測試目的，您將在 中建立新的使用者 (Richard Roe)Microsoft Entra ID。稍後，在您設定 SCIM 同步後，您將測試此使用者 and 所有相關屬性是否已成功同步至 IAM Identity Center。

1. 在 [Microsoft Entra 管理中心](#) 主控台中，導覽至身分 > 使用者 > 所有使用者。
2. 選取新使用者，然後在畫面頂端選擇建立新使用者。
3. 在使用者主體名稱中，輸入 **RichRoe**，然後選取您偏好的網域和延伸。例如，RichRoe@*example.org*。
4. 在顯示名稱中，輸入 **RichRoe**。
5. 在密碼中，輸入高強度密碼或選取眼睛圖示以顯示自動產生的密碼，然後複製或寫下顯示的值。
6. 選擇屬性，然後提供下列值：
 - 名字 - 輸入 **Richard**
 - 姓氏 - 輸入 **Roe**
 - 任務標題 - 輸入 **Marketing Lead**
 - 部門 - 輸入 **Sales**
 - 員工 ID - 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 Identity Center 中啟用自動佈建

在此程序中，您將使用 IAM Identity Center 主控台來啟用將來自 的使用者和群組自動佈建Microsoft Entra ID至 IAM Identity Center。

1. 開啟 [IAM Identity Center 主控台](#)，然後在左側導覽窗格中選擇設定。
2. 在設定頁面的身分來源索引標籤下，請注意佈建方法設定為手動。
3. 找到自動佈建資訊方塊，然後選擇啟用。這會立即在 IAM Identity Center 中啟用自動佈建，並顯示必要的 SCIM 端點和存取字符資訊。
4. 在傳入自動佈建對話方塊中，複製下列選項的每個值。在 中設定佈建時，您需要在下一個步驟中貼上這些項目Microsoft Entra ID。

- a. SCIM 端點 - 例如，
 - IPv4 : `https://scim.aws-region.amazonaws.com/1111111111-2222-3333-4444-5555555555/scim/v2`
 - 雙堆疊 : `https://scim.aws-region.api.aws/1111111111-2222-3333-4444-5555555555/scim/v2`
- b. 存取字符 - 選擇顯示字符以複製值。

 Warning

這是您唯一可以取得 SCIM 端點和存取權杖的時間。在繼續之前，請務必複製這些值。

5. 選擇關閉。
6. 在身分來源索引標籤下，請注意佈建方法現在設定為 SCIM。

Step 4.3 >

步驟 4.3：在 中設定自動佈建 Microsoft Entra ID

現在您已備妥 RichRoe 測試使用者，並已在 IAM Identity Center 中啟用 SCIM，您可以繼續在 中設定 SCIM 同步設定 Microsoft Entra ID。

1. 在 [Microsoft Entra 管理中心](#) 主控台中，導覽至身分 > 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. 在管理員登入資料下，在租戶 URL 中，貼上您稍早在 中複製的 SCIM 端點 URL 值 **Step 4.2**。在私密字符中，貼上存取字符值。
5. 選擇 Test Connection (測試連接)。您應該會看到訊息，指出測試的登入資料已成功授權啟用佈建。
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. 在新增指派頁面的使用者下，選擇未選取。

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：確認同步已發生

在本節中，您將確認 Richard 的使用者已成功佈建，且所有屬性都會顯示在 IAM Identity Center 中。

1. 在 [IAM Identity Center 主控台](#) 中，選擇使用者。
2. 在使用者頁面上，您應該會顯示您的 RichRoe 使用者。請注意，在建立者資料欄中，值設定為 SCIM。
3. 在設定檔下選擇 RichRoe，確認已從 複製下列屬性 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 Identity Center 中建立，您可以將其指派給任何許可集，以便控制他對 AWS 資源的存取層級。例如，您可以將 RichRoe 指派給先前用來授予 Nikki 管理區域（請參閱 **Step 2.3**）的許可 **RegionalAdmin** 集，然後使用 測試他的存取層級 **Step 3.5**。

恭喜您！

您已成功設定 Microsoft 和 之間的 SAML 連線，AWS 並已驗證自動佈建正在讓一切保持同步。現在，您可以套用所學到的知識，以更順暢地設定您的生產環境。

步驟 5：設定 ABAC - 選用

現在您已成功設定 SAML 和 SCIM，您可以選擇設定屬性型存取控制 (ABAC)。ABAC 是一種授權策略，可根據屬性定義許可。

透過 Microsoft Entra ID，您可以使用下列兩種方法之一來設定 ABAC 以搭配 IAM Identity Center 使用。

Configure user attributes in Microsoft Entra ID for access control in IAM Identity Center

在 中設定使用者屬性Microsoft Entra ID，以在 IAM Identity Center 中進行存取控制

在下列程序中，您將決定 IAM Identity Center Microsoft Entra ID應使用哪些屬性來管理對 AWS 資源的存取。定義後，會透過 SAML 聲明將這些屬性Microsoft Entra ID傳送至 IAM Identity Center。然後，您需要在 IAM Identity Center [建立許可集](#)中，根據您從傳遞的屬性來管理存取權Microsoft Entra ID。

開始此程序之前，您必須先啟用[存取控制的屬性](#)此功能。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 管理中心](#)主控台中，導覽至身分 > 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. 在屬性和宣告區段中，選擇編輯。
4. 在屬性和宣告頁面上，執行下列動作：
 - a. 選擇新增宣告
 - b. 對於名稱，輸入 `AccessControl:AttributeName`。以您在 IAM Identity Center 中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，請使用下拉式清單選擇Microsoft Entra ID使用者屬性。例如 `user.department`。
5. 針對您需要傳送至 SAML 聲明中的 IAM Identity Center 的每個屬性，重複上述步驟。
6. 選擇儲存。

Configure ABAC using IAM Identity Center

使用 IAM Identity Center 設定 ABAC

透過此方法，您可以使用 IAM Identity Center 中的 [存取控制的屬性](#) 功能來傳遞 Name 屬性設為的 Attribute 元素 `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`。您可以使用此元素，在 SAML 聲明中將屬性傳遞為工作階段標籤。如需工作階段標籤的詳細資訊，請參閱《IAM 使用者指南》中的在 [中傳遞工作階段標籤 AWS STS](#)。

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，若要傳遞標籤鍵值對 `Department=billing`，請使用下列屬性：

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

如果您需要新增多個屬性，請為每個標籤加入個別的 Attribute 元素。

將存取權指派給 AWS 帳戶

下列步驟只需要將存取權授予 AWS 帳戶 即可。授予 AWS 應用程式存取權不需要這些步驟。

Note

若要完成此步驟，您需要 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱 [IAM Identity Center 的組織和帳戶執行個體](#)。

步驟 1：IAM Identity Center：授予 Microsoft Entra ID 使用者帳戶存取權

1. 返回 IAM Identity Center 主控台。在 IAM Identity Center 導覽窗格中的多帳戶許可下，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及其下的帳戶。選取管理帳戶的核取方塊，然後選取指派使用者或群組。

3. 此時會顯示指派使用者和群組工作流程。它包含三個步驟：

- a. 針對步驟 1：選取使用者和群組，選擇將執行管理員任務功能的使用者。然後選擇下一步。
- b. 針對步驟 2：選取許可集選擇建立許可集，以開啟新標籤，引導您完成建立許可集所涉及的三個子步驟。
 - i. 針對步驟 1：選取許可集類型完成下列項目：
 - 在許可集類型中，選擇預先定義的許可集。
 - 在預先定義許可集的政策中，選擇 `AdministratorAccess`。

選擇下一步。

- ii. 對於步驟 2：指定許可集詳細資訊，保留預設設定，然後選擇下一步。

預設設定會建立名為 `AdministratorAccess` 的許可集，並將工作階段持續時間設定為一小時。

- iii. 對於步驟 3：檢閱和建立，確認許可集類型使用 AWS 受管政策 `AdministratorAccess`。選擇建立。在許可集頁面上會出現通知，通知您已建立許可集。您現在可以在 Web 瀏覽器中關閉此索引標籤。
- iv. 在指派使用者和群組瀏覽器索引標籤上，您仍在步驟 2：選取您從中開始建立許可集工作流程的許可集。
- v. 在許可集區域中，選擇重新整理按鈕。您建立的 `AdministratorAccess` 許可集會出現在清單中。選取該許可集的核取方塊，然後選擇下一步。
- c. 針對步驟 3：檢閱並提交檢閱選取的使用者和許可集，然後選擇提交。

頁面會以 AWS 帳戶 正在設定 的訊息進行更新。等待程序完成。

您會返回 AWS 帳戶 頁面。通知訊息會通知您 AWS 帳戶，您的 已重新佈建，並已套用更新的許可集。當使用者登入時，他們可以選擇 `AdministratorAccess` 角色。

步驟 2：Microsoft Entra ID：確認 Microsoft Entra ID 使用者存取 AWS 資源

1. 返回 Microsoft Entra ID 主控台並導覽至您的 IAM Identity Center SAML 型登入應用程式。
2. 選取使用者和群組，然後選取新增使用者或群組。您將在此教學課程中建立的使用者新增至 Microsoft Entra ID 應用程式。透過新增使用者，您將允許他們登入 AWS。搜尋您在步驟 4 建立的使用者。如果您遵循此步驟，則會是 **RichardRoe**。

- 如需示範，請參閱[使用 聯合現有的 IAM Identity Center 執行個體 Microsoft Entra ID](#)

Microsoft Entra ID 存取 IAM Identity Center 其他區域的組態 - 選用

如果您將 IAM Identity Center 複寫至其他區域，則必須更新身分提供者組態，以啟用受 AWS 管應用程式的存取，以及 AWS 帳戶 透過其他區域存取。下列步驟會引導您完成程序。如需有關此主題的詳細資訊，包括先決條件，請參閱 [跨多個 使用 IAM Identity Center AWS 區域](#)。

1. 從 IAM Identity Center 主控台擷取其他區域的 ACS URLs，如 中所述[主要和其他 中的 ACS 端點 AWS 區域](#)。
2. 在 [Microsoft Entra 管理員中心](#)主控台中，導覽至身分 > 應用程式 > 企業應用程式，然後選擇 AWS IAM Identity Center。
3. 在左側，選擇 2。設定單一登入。
4. 在基本 SAML 組態頁面的回覆 URL（聲明消費者服務 URL）區段下，為每個新增區域的 ACS URL 選擇新增回覆 URL。您可以保留主要區域的 ACS URL 作為預設 URL，以便在使用者從 啟動 AWS IAM Identity Center 應用程式時，持續重新導向至主要區域Microsoft Entra ID。
5. 新增 ACS URLs完成後，請儲存AWS IAM Identity Center應用程式。
6. 您可以在 中Microsoft Entra ID為每個額外區域的 AWS 存取入口網站建立書籤應用程式。這可讓您的使用者從 存取其他區域中的 AWS 存取入口網站Microsoft Entra ID。請務必授予使用者存取 中書籤應用程式的許可Microsoft Entra ID。如需詳細資訊，請參閱 [Microsoft Entra ID 文件](#)。
7. 確認您可以在每個其他區域中登入 AWS 存取入口網站。導覽至[AWS 存取入口網站 URLs](#)或從 啟動書籤應用程式Microsoft Entra ID。

疑難排解

如需使用 進行一般 SCIM 和 SAML 疑難排解Microsoft Entra ID，請參閱下列章節：

- [與 Microsoft Entra ID和 IAM Identity Center 的同步問題](#)
- [特定使用者無法從外部 SCIM 供應商同步到 IAM Identity Center](#)
- [IAM Identity Center 建立的 SAML 聲明內容相關問題](#)
- [使用外部身分提供者佈建使用者或群組時發生重複的使用者或群組錯誤](#)
- [其他資源](#)

與 Microsoft Entra ID 和 IAM Identity Center 的同步問題

如果您遇到 Microsoft Entra ID 使用者未同步至 IAM Identity Center 的問題，這可能是因為在將新使用者新增至 IAM Identity Center 時，IAM Identity Center 已標記的語法問題。您可以檢查 Microsoft Entra ID 稽核日誌是否有失敗的事件來確認這一點，例如 'Export'。此事件的狀態原因將指出：

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

您也可以檢查 AWS CloudTrail 失敗的事件。這可以透過使用下列篩選條件在 CloudTrail 的事件歷史記錄主控台中搜尋來完成：

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

CloudTrail 事件中的錯誤會陳述下列項目：

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

最後，此例外狀況表示從傳遞的其中一個值 Microsoft Entra ID 包含比預期更多的值。解決方案是檢閱中使用者的屬性 Microsoft Entra ID，確保沒有包含重複值。重複值的一個常見範例是為行動、工作和傳真等聯絡號碼提供多個值。雖然個別的值，但它們都會在單一父屬性 phoneNumbers 下傳遞至 IAM Identity Center。

如需一般 SCIM 故障診斷秘訣，請參閱[故障診斷](#)。

Microsoft Entra ID 訪客帳戶同步

如果您想要將 Microsoft Entra ID 訪客使用者同步至 IAM Identity Center，請參閱下列程序。

Microsoft Entra ID 訪客使用者的電子郵件與 Microsoft Entra ID 使用者不同。此差異會導致嘗試將 Microsoft Entra ID 訪客使用者與 IAM Identity Center 同步時發生問題。例如，請參閱下列訪客使用者的電子郵件地址：

```
exampleuser_domain.com#EXT#@domain.onmicrosoft.com.
```

IAM Identity Center 不預期電子郵件地址包含 **#EXT#@domain** 格式。

1. 登入 [Microsoft Entra 管理中心](#)，導覽至身分 > 應用程式 > 企業應用程式，然後選擇 AWS IAM Identity Center
2. 導覽至左側窗格中的單一登入索引標籤。

3. 選取使用者屬性和宣告旁顯示的編輯。
4. 選取必要宣告後方的唯一使用者識別符（名稱 ID）。
5. 您將為您的Microsoft Entra ID使用者和訪客使用者建立兩個宣告條件：
 - a. 對於Microsoft Entra ID使用者，為來源屬性設為 `user.userprincipalname` 的成員建立使用者類型。
 - b. 對於Microsoft Entra ID訪客使用者，請為外部訪客建立使用者類型，並將來源屬性設為 `user.mail`。
 - c. 選取儲存並重試以Microsoft Entra ID訪客使用者身分登入。

其他資源

- 如需一般 SCIM 疑難排解秘訣，請參閱 [對 IAM Identity Center 問題進行故障診斷](#)。
- 如需Microsoft Entra ID故障診斷，請參閱 [Microsoft 文件](#)。
- 若要進一步了解多個的聯合 AWS 帳戶，請參閱[AWS 帳戶 使用 保護Azure Active Directory Federation](#)。

下列資源可協助您在使用時進行故障診斷 AWS：

- [AWS re:Post](#) - 尋找FAQs和其他資源的連結，協助您疑難排解問題。
- [AWS 支援](#) - 取得技術支援

使用 和 IAM Identity Center 設定 SAML Okta和 SCIM

您可以使用跨網域身分管理 (SCIM) 2.0 通訊協定，自動將使用者和群組資訊從 佈建或同步Okta到 IAM Identity Center。 [SCIM 設定檔](#)如需詳細資訊，請參閱[搭配外部身分提供者使用 SAML 和 SCIM 聯合身分](#)。

若要在 中設定此連線Okta，您可以使用 IAM Identity Center 的 SCIM 端點和 IAM Identity Center 自動建立的承載字符。當您設定 SCIM 同步時，您可以在 中建立使用者屬性映射Okta至 IAM Identity Center 中具名屬性的映射。此映射符合 IAM Identity Center 與Okta您的帳戶之間的預期使用者屬性。

Okta 透過 SCIM 連線至 IAM Identity Center 時，支援下列佈建功能：

- 建立使用者 – 在 中指派給 IAM Identity Center 應用程式的使用者Okta會在 IAM Identity Center 中佈建。

- 更新使用者屬性 – 在 中指派給 IAM Identity Center 應用程式之使用者的屬性變更Okta會在 IAM Identity Center 中更新。
- 停用使用者 – 從 中的 IAM Identity Center 應用程式取消指派的使用者Okta會在 IAM Identity Center 中停用。
- 群組推送 – 中的群組 Okta (及其成員) 會同步至 IAM Identity Center。

Note

為了將 Okta和 IAM Identity Center 的管理開銷降至最低，建議您指派和推送群組，而不是個別使用者。

- 匯入使用者 – 使用者可以從 IAM Identity Center 匯入 Okta。

目標

在本教學課程中，您將逐步解說如何設定與 IAM Identity Center 的 SAML Okta 連線。稍後，您將使用 SCIM Okta從 同步使用者。在此案例中，您會在 中管理所有使用者和群組Okta。使用者透過 Okta 入口網站登入。若要驗證一切設定正確，在完成設定步驟後，您將以 Okta使用者身分登入並驗證對 AWS 資源的存取。

透過 SAML Okta連線至 IAM Identity Center 時，支援下列功能：

- IdP 啟動的 SAML 登入 – 使用者透過Okta入口網站登入並存取 IAM Identity Center。
- SP 啟動的 SAML 登入 – 使用者存取 AWS 存取入口網站，這會重新導向他們透過Okta入口網站登入。

Note

您可以註冊已安裝 [IAM Identity Center 應用程式](#)Okta的帳戶 Okta's ([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類似功能，以啟用傳出佈建。設定從 Okta到 IAM Identity Center 的 SCIM 時，可能需要這些功能。

如果您尚未啟用 IAM Identity Center，請參閱 [啟用 IAM Identity Center](#)。

考量事項

- 在 Okta和 IAM Identity Center 之間設定 SCIM 佈建之前，建議您先檢閱 [使用自動佈建的考量事項](#)。

- 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使用者每個資料屬性只有一個值，例如電子郵件地址或電話號碼。具有多個值的任何使用者都將無法同步。如果使用者在其屬性中有多個值，請在嘗試在 IAM Identity Center 中佈建使用者之前移除重複的屬性。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」，所以即使使用者的電話號碼是家用電話或行動電話，也請使用「工作電話」屬性來存放使用者的電話號碼。
- Okta 搭配 IAM Identity Center 使用時，IAM Identity Center 通常會在 中設定為應用程式Okta。這可讓您將 IAM Identity Center 的多個執行個體設定為多個應用程式，以支援在 的單一執行個體內存取多個 AWS OrganizationsOkta。
- 不支援權利和角色屬性，且無法與 IAM Identity Center 同步。
- 目前不支援對指派和Okta群組推送使用相同的群組。若要在 Okta和 IAM Identity Center 之間維持一致的群組成員資格，請建立個別的群組，並將其設定為將群組推送至 IAM Identity Center。
- 如果您將 IAM Identity Center 複寫至其他區域，則必須更新身分提供者組態，以啟用受 AWS 管應用程式的存取，以及 AWS 帳戶 透過其他區域存取。如需包括先決條件的詳細資訊，請參閱 [跨多個 使用 IAM Identity Center AWS 區域](#)。Okta 特定步驟說明於 [Okta 用於存取其他區域的組態](#)

步驟 1：Okta：從Okta您的帳戶取得 SAML 中繼資料

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 Identity Center 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。新的瀏覽器索引標籤隨即開啟，顯示 XML 檔案的文件樹狀目錄。選取從 <md:EntityDescriptor>到 的所有 XML，</md:EntityDescriptor>並將其複製到文字檔案。
6. 將文字檔案儲存為 metadata.xml。

保持Okta admin dashboard開啟狀態，您將在後續步驟中繼續使用此主控台。

步驟 2：IAM Identity Center：將 Okta設定為 IAM Identity Center 的身分來源

1. 以具有管理權限的使用者身分開啟 [IAM Identity Center 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，然後選擇變更身分來源。
4. 在選擇身分來源下，選取外部身分提供者，然後選擇下一步。
5. 在設定外部身分提供者下，執行下列動作：
 - a. 在服務提供者中繼資料下，將下列項目複製到文字檔案，以便於存取：
 - IAM Identity Center Assertion Consumer Service (ACS) URL – 您可以選擇IPv4-only 和雙堆疊 ACS URLs。此外，如果您的 IAM Identity Center 執行個體在多個區域中啟用，則每個額外的區域都有自己的IPv4-only 和雙堆疊 ACS URLs。如需 ACS URLs 的詳細資訊，請參閱 [主要和其他 中的 ACS 端點 AWS 區域](#)。
 - IAM Identity Center 發行者 URL

您稍後在本教學課程中將需要這些值。

- b. 在身分提供者中繼資料下，於 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metadata.xml的檔案。
 - c. 選擇下一步。
6. 在您閱讀免責聲明並準備好繼續之後，請輸入 ACCEPT。
7. 選擇變更身分來源。

保持 AWS 主控台開啟，您將在下一個步驟中繼續使用此主控台。

8. 返回 Okta admin dashboard，然後選取 AWS IAM Identity Center 應用程式的登入索引標籤，然後選取編輯。
9. 在進階登入設定下，輸入下列項目：
 - 針對 ACS URL，輸入您為 IAM Identity Center Assertion Consumer Service (ACS) URL 複製的值(s)。您可以使用主要區域的 ACS URL 做為預設 URL，以便在使用者從 啟動 Amazon Web Services 應用程式時重新導向至主要區域Okta。
 - (選用) 如果您將 IAM Identity Center 複寫到其他區域，您也可以在中Okta為每個其他區域的 AWS 存取入口網站建立書籤應用程式。這可讓您的使用者從 存取其他區域中的 AWS 存取入口網站Okta。請務必授予使用者存取 中書籤應用程式的許可Okta。如需詳細資訊，請參閱 [Okta 文件](#)。如果您計劃稍後將 IAM Identity Center 複寫到其他區域，請造訪 [Okta 用於存取其他區域的組態](#) 以取得指引，了解如何在此初始設定後啟用其他區域的存取權。
 - 針對發行者 URL，輸入您為 IAM Identity Center 發行者 URL 複製的值
 - 對於應用程式使用者名稱格式，從功能表中選取其中一個選項。

確保您選擇的值對每個使用者都是唯一的。在此教學課程中，選取 Okta 使用者名稱

10. 選擇儲存。

您現在可以將使用者從 佈建Okta至 IAM Identity Center。保持Okta admin dashboard開啟狀態，並返回 IAM Identity Center 主控台進行下一個步驟。

步驟 3：IAM Identity Center 和 Okta：佈建Okta使用者

1. 在設定頁面上的 IAM Identity Center 主控台中，找到自動佈建資訊方塊，然後選擇啟用。這會在 IAM Identity Center 中啟用自動佈建，並顯示必要的 SCIM 端點和存取字符資訊。
2. 在傳入自動佈建對話方塊中，複製下列選項的每個值：

- a. SCIM 端點 - 端點格式取決於您的組態：

- IPv4：`https://scim.us-east-2.amazonaws.com/111111111-2222-3333-4444-55555555/scim/v2`
- 雙堆疊：`https://scim.us-east-2.api.aws/111111111-2222-3333-444-55555555/scim/v2`

- b. 存取字符 - 選擇顯示字符以複製值。

Warning

這是您唯一可以取得 SCIM 端點和存取權杖的時間。在繼續之前，請務必複製這些值。您將在本教學課程Okta稍後輸入這些值來設定自動佈建。

3. 選擇關閉。
4. 返回 Okta admin dashboard並導覽至 IAM Identity Center 應用程式。
5. 在 IAM Identity Center 應用程式頁面上，選擇佈建索引標籤，然後在設定下的左側導覽中，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自動佈建。
7. Okta 使用您在此步驟中稍早複製 AWS IAM Identity Center 的 SCIM 佈建值來設定：
 - a. 在基本 URL 欄位中，輸入 SCIM 端點值。
 - b. 在 API Token 欄位中，輸入 Access Token 值。
8. 選擇測試 API 登入資料來驗證輸入的登入資料是否有效。

訊息AWS IAM Identity Center 已成功驗證！隨即顯示。

9. 選擇儲存。系統會將您移至設定區段，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。在此教學課程中，選取所有選項。
11. 選擇儲存。

您現在可以從 同步您的使用者Okta與 IAM Identity Center。

步驟 4：Okta：將來自 的使用者Okta與 IAM Identity Center 同步

根據預設，不會將群組或使用者指派給您的 Okta IAM Identity Center 應用程式。佈建群組會佈建屬於群組成員的使用者。完成下列步驟，以與 同步群組和使用者 AWS IAM Identity Center。

1. 在 Okta IAM Identity Center 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 Identity Center 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。
 - 選擇您要存取 IAM Identity Center 應用程式Okta的使用者。選擇指派，選擇儲存並返回，然後選擇完成。

這會開始將使用者佈建至 IAM Identity Center 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 Identity Center 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。

這會開始將群組中的使用者佈建至 IAM Identity Center 的程序。

Note

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

2. 選擇推送群組索引標籤。選擇您要與 IAM Identity Center 同步的 Okta 群組。選擇儲存。

群組及其成員推送至 IAM Identity Center 後，群組狀態會變更為作用中。

3. 返回指派索引標籤。
4. 若要將個別 Okta 使用者新增至 IAM Identity Center，請使用下列步驟：
 - a. 在指派頁面中，選擇指派，然後選擇指派給人員。
 - b. 選擇您要存取 IAM Identity Center 應用程式 Okta 的使用者。選擇指派，選擇儲存並返回，然後選擇完成。

這會開始將個別使用者佈建至 IAM Identity Center 的程序。

Note

您也可以從的應用程式頁面，將使用者和群組指派給 AWS IAM Identity Center 應用程式 Okta admin dashboard。若要這樣做，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。

5. 返回 IAM Identity Center 主控台。在左側導覽中，選取使用者，您應該會看到使用者填入 Okta 的使用者清單。

恭喜您！

您已成功在 Okta 和 之間設定 SAML 連線，AWS 並已驗證自動佈建是否正常運作。您現在可以將這些使用者指派給 IAM Identity Center 中的帳戶和應用程式。在本教學課程中，在下一個步驟中，我們將其中一個使用者授予管理帳戶的管理許可，以指定為 IAM Identity Center 管理員。

傳遞存取控制的屬性 - 選用

您可以選擇性地使用 IAM Identity Center 中的 [存取控制的屬性](#) 功能，傳遞 Name 屬性設為的 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》中的在 [中傳遞工作階段標籤 AWS STS](#)。

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，請為每個標籤加入個別的Attribute元素。

將存取權指派給 AWS 帳戶

下列步驟僅需要授予 AWS 帳戶 的存取權。授予 AWS 應用程式存取權不需要這些步驟。

Note

若要完成此步驟，您需要 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱[IAM Identity Center 的組織和帳戶執行個體](#)。

步驟 1：IAM Identity Center：授予Okta使用者帳戶存取權

1. 在 IAM Identity Center 導覽窗格中的多帳戶許可下，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及其下的帳戶。選取管理帳戶的核取方塊，然後選取指派使用者或群組。
3. 此時會顯示指派使用者和群組工作流程。它包含三個步驟：
 - a. 針對步驟 1：選取使用者和群組，選擇將執行管理員任務功能的使用者。然後選擇下一步。
 - b. 針對步驟 2：選取許可集，選擇建立許可集以開啟新索引標籤，引導您完成建立許可集所涉及的三個子步驟。
 - i. 對於步驟 1：選取許可集類型完成下列項目：
 - 在許可集類型中，選擇預先定義的許可集。
 - 在預先定義許可集的政策中，選擇 AdministratorAccess。

選擇下一步。

- ii. 對於步驟 2：指定許可集詳細資訊，保留預設設定，然後選擇下一步。

預設設定會建立名為 *AdministratorAccess* 的許可集，並將工作階段持續時間設定為一小時。

- iii. 針對步驟 3：檢閱和建立，確認許可集類型使用 AWS 受管政策 *AdministratorAccess*。選擇建立。在許可集頁面上，會出現通知，通知您已建立許可集。您現在可以在 Web 瀏覽器中關閉此索引標籤。

在指派使用者和群組瀏覽器索引標籤上，您仍在步驟 2：選取您從中開始建立許可集工作流程的許可集。

在許可集區域中，選擇重新整理按鈕。您建立的 *AdministratorAccess* 許可集會出現在清單中。選取該許可集的核取方塊，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許可集，然後選擇提交。

頁面會以 AWS 帳戶 正在設定 的訊息進行更新。等待程序完成。

您會返回 AWS 帳戶 頁面。通知訊息會通知您 AWS 帳戶，您的 已重新佈建並套用更新的許可集。當使用者登入時，他們可以選擇 *AdministratorAccess* 角色。

步驟 2：Okta：確認Okta使用者存取 AWS 資源

1. 使用測試帳戶登入 Okta dashboard。
2. 在我的應用程式下，選取 AWS IAM Identity Center 圖示。
3. 您應該會看到 AWS 帳戶 圖示。展開該圖示以查看使用者可以存取 AWS 帳戶 的清單。在本教學課程中，您只使用單一帳戶，因此展開圖示只會顯示一個帳戶。
4. 選取帳戶以顯示使用者可用的許可集。在本教學課程中，您已建立 *AdministratorAccess* 許可集。
5. 許可集旁邊是該許可集可用存取類型的連結。當您建立許可集時，您會指定對 AWS 管理主控台和 程式設計存取的存取權。選取管理主控台以開啟 AWS 管理主控台。
6. 使用者已登入 AWS 管理主控台。

您也可以使用 AWS 存取入口網站。這會將您重新導向至透過Okta入口網站登入，然後再帶您前往 AWS 存取入口網站。此路徑遵循 SP 起始的 SAML 登入流程。

Okta 存取 IAM Identity Center 其他區域的組態 - 選用

如果您將 IAM Identity Center 複寫至其他區域，則必須更新身分提供者組態，以啟用受 AWS 管應用程式的存取，以及 AWS 帳戶 透過其他區域存取。下列步驟會引導您完成程序。如需有關此主題的詳細資訊，包括先決條件，請參閱 [跨多個 使用 IAM Identity Center AWS 區域](#)。

1. 從 IAM Identity Center 主控台擷取其他區域的 ACS URLs，如 中所述[主要和其他 中的 ACS 端點 AWS 區域](#)。
2. 在Okta管理員儀表板的導覽窗格中，選擇應用程式，然後在展開的清單中再次選擇應用程式。
3. 選擇 AWS IAM Identity Center 應用程式。
4. 選擇 Sign On (登入) 標籤。
5. 在進階登入設定和其他可請求URLs 下，為每個額外區域的 ACS URL 選擇新增另一個 URL，然後將 ACS URL 貼到文字欄位中。
6. 新增 ACS URLs 完成後，請儲存AWS IAM Identity Center應用程式。
7. 您可以在 中Okta為每個額外區域的 AWS 存取入口網站建立書籤應用程式。這可讓您的使用者從 存取其他區域中的 AWS 存取入口網站Okta。請務必授予使用者存取 中書籤應用程式的許可 Okta。如需詳細資訊，請參閱 [Okta 文件](#)。
8. 確認您可以在每個額外的區域中登入 AWS 存取入口網站。導覽至[AWS 存取入口網站 URLs](#)或從啟動書籤應用程式Okta。

後續步驟

現在您已Okta在 IAM Identity Center 中將 設定為身分提供者和佈建使用者，您可以：

- 授予 的存取權 AWS 帳戶，請參閱 [將使用者或群組存取權指派給 AWS 帳戶](#)。
- 授予雲端應用程式的存取權，請參閱 [在 IAM Identity Center 主控台中指派使用者對應用程式的存取權](#)。
- 根據任務函數設定許可，請參閱[建立許可集](#)。

疑難排解

如需使用 進行一般 SCIM 和 SAML 故障診斷Okta，請參閱下列章節：

- [重新佈建從 IAM Identity Center 刪除的使用者和群組](#)
- [中的自動佈建錯誤 Okta](#)

- [特定使用者無法從外部 SCIM 供應商同步到 IAM Identity Center](#)
- [IAM Identity Center 建立的 SAML 聲明內容相關問題](#)
- [使用外部身分提供者佈建使用者或群組時發生重複的使用者或群組錯誤](#)
- [其他資源](#)

重新佈建從 IAM Identity Center 刪除的使用者和群組

- 如果您在 中嘗試變更曾同步的使用者或群組，然後從 IAM Identity Center 刪除Okta，您可能會在 Okta主控台中收到下列錯誤訊息：
 - 自動將使用者 *Jane Doe* 推送至應用程式 AWS IAM Identity Center 失敗：嘗試推送 *jane_doe@example.com* 的設定檔更新時發生錯誤：未傳回使用者 *xxxxx-xxxxxx-xxxxx-xxxxxx*
 - 連結的群組遺失 AWS IAM Identity Center。變更連結的群組以繼續推送群組成員資格。
- 您也可以 在 Okta 的 Systems Logs 中，針對同步和刪除的 IAM Identity Center 使用者或群組收到下列錯誤訊息：
 - Okta 錯誤：Eventfailed application.provision.user.push_profile：未傳回使用者 *xxxxx-xxxxxx-xxxxx-xxxxxx*
 - Okta 錯誤：application.provision.group_push.mapping.update.or.delete.failed.with.error：缺少連結的群組 AWS IAM Identity Center。變更連結的群組以繼續推送群組成員資格。

Warning

如果您已使用 SCIM 同步和 IAM Identity Center，則應從 刪除使用者Okta和群組，Okta而不是從 IAM Identity Center 刪除。

對已刪除的 IAM Identity Center 使用者進行故障診斷

若要解決已刪除 IAM Identity Center 使用者的此問題，必須從 刪除使用者Okta。如有必要，這些使用者也需要在 中重新建立Okta。在 中重新建立使用者時Okta，也會透過 SCIM 將其重新佈建至 IAM Identity Center。如需刪除使用者的詳細資訊，請參閱 [Okta 文件](#)。

 Note

如果您需要移除Okta使用者對 IAM Identity Center 的存取權，您應該先將其從群組推送中移除，然後在 中移除其指派群組Okta。這可確保從 IAM Identity Center 中的關聯群組成員資格中移除使用者。如需群組推送疑難排解的詳細資訊，請參閱 [Okta 文件](#)。

對已刪除的 IAM Identity Center 群組進行故障診斷

若要解決已刪除 IAM Identity Center 群組的問題，必須從 Okta 刪除該群組。如有必要，這些群組也需要使用群組推送在 Okta 中重新建立。在 Okta 中重新建立使用者時，也會透過 SCIM 將其重新佈建至 IAM Identity Center。如需刪除群組的詳細資訊，請參閱 [Okta 文件](#)。

中的自動佈建錯誤 Okta

如果您在 中收到下列錯誤訊息Okta：

使用者 Jane Doe 至應用程式的自動佈建 AWS IAM Identity Center 失敗：找不到相符的使用者

如需詳細資訊，請參閱 [Okta 文件](#)。

其他資源

- 如需一般 SCIM 疑難排解秘訣，請參閱 [對 IAM Identity Center 問題進行故障診斷](#)。

下列資源可協助您在使用 時進行故障診斷 AWS：

- [AWS re:Post](#) - 尋找FAQs和其他資源的連結，協助您疑難排解問題。
- [AWS 支援](#) - 取得技術支援

在 OneLogin和 IAM Identity Center 之間設定 SCIM 佈建

IAM Identity Center 支援使用跨網域身分管理 (SCIM) 2.0 版通訊協定，將使用者和群組資訊從 自動佈建（同步）OneLogin到 IAM Identity Center。如需詳細資訊，請參閱[搭配外部身分提供者使用 SAML 和 SCIM 聯合身分](#)。

 Note

OneLogin 目前不支援 AWS IAM Identity Center 應用程式中的 SAML 多聲明使用服務 (ACS) URLs。需要此 SAML 功能才能充分利用 IAM Identity Center 中的[多區域支援](#)。如果您打算將 IAM Identity Center 複寫到其他區域，請注意，使用單一 ACS URL 可能會影響這些其他區域中的使用者體驗。您的主要區域會繼續正常運作。我們建議您與 IdP 廠商合作，以啟用此功能。如需使用單一 ACS URL 在其他區域中使用使用者體驗的詳細資訊，請參閱 [the section called “使用沒有多個 ACS URLs AWS 受管應用程式”](#)和 [the section called “AWS 帳戶 在沒有多個 ACS URLs存取彈性”](#)。

您可以使用 IAM Identity Center 的 SCIM 端點和 IAM Identity Center 自動建立的承載字符OneLogin，在 中設定此連線。當您設定 SCIM 同步時，您可以在 中建立使用者屬性映射OneLogin至 IAM Identity Center 中具名屬性的映射。這會導致 IAM Identity Center 和 之間的預期屬性相符OneLogin。

下列步驟會逐步解說如何使用 SCIM 通訊協定，將使用者和群組從 自動佈建OneLogin至 IAM Identity Center。

 Note

在您開始部署 SCIM 之前，建議您先檢閱 [使用自動佈建的考量事項](#)。

主題

- [先決條件](#)
- [步驟 1：在 IAM Identity Center 中啟用佈建](#)
- [步驟 2：在 中設定佈建 OneLogin](#)
- [\(選用\) 步驟 3：在 中設定使用者屬性OneLogin，以在 IAM Identity Center 中進行存取控制](#)
- [\(選用\) 傳遞屬性以進行存取控制](#)
- [疑難排解](#)

先決條件

您將需要下列項目才能開始使用：

- OneLogin 帳戶。如果您沒有現有的 帳戶，您可能可以從 [OneLogin網站](#)取得免費試用或開發人員帳戶。

- 啟用 IAM Identity Center 的帳戶 ([免費](#))。如需詳細資訊，請參閱[啟用 IAM Identity Center](#)。
- 從OneLogin您的帳戶到 IAM Identity Center 的 SAML 連線。如需詳細資訊，請參閱 AWS 合作夥伴網路部落格上的在 [OneLogin和 之間啟用單一登入 AWS](#)。

步驟 1：在 IAM Identity Center 中啟用佈建

在此第一個步驟中，您可以使用 IAM Identity Center 主控台來啟用自動佈建。

在 IAM Identity Center 中啟用自動佈建

1. 完成先決條件後，請開啟 [IAM Identity Center 主控台](#)。
2. 在左側導覽窗格中選擇設定。
3. 在設定頁面上，找到自動佈建資訊方塊，然後選擇啟用。這會立即在 IAM Identity Center 中啟用自動佈建，並顯示必要的 SCIM 端點和存取字符資訊。
4. 在傳入自動佈建對話方塊中，複製 SCIM 端點和存取字符。稍後在 IdP 中設定佈建時，您需要將這些項目貼入。
 - a. SCIM 端點 - 例如，`https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-444-55555555/scim/v2`
 - b. 存取字符 - 選擇顯示字符以複製值。

Warning

這是您唯一可以取得 SCIM 端點和存取權杖的時間。在繼續之前，請務必複製這些值。您將在本教學稍後輸入這些值，以設定 IdP 中的自動佈建。

5. 選擇關閉。

您現在已在 IAM Identity Center 主控台中設定佈建。現在，您需要使用OneLogin管理員主控台執行剩餘的任務，如下列程序所述。

步驟 2：在 中設定佈建 OneLogin

在OneLogin管理員主控台中使用下列程序，以啟用 IAM Identity Center 與 IAM Identity Center 應用程式之間的整合。此程序假設您已在 中設定 AWS 單一登入應用程式OneLogin以進行 SAML 身分驗證。如果您尚未建立此 SAML 連線，請在繼續之前執行此操作，然後返回這裡以完成 SCIM 佈建程序。如

需使用 設定 SAML 的詳細資訊OneLogin，請參閱 合作夥伴網路部落格上的 AWS 在 [OneLogin和 之間啟用單一登入 AWS](#)。

在 中設定佈建 OneLogin

1. 登入 OneLogin，然後導覽至應用程式 > 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，以與 IAM Identity Center 建立 SAML 連線。選擇它，然後從導覽窗格中選擇組態。
3. 在先前的程序中，您會在 IAM Identity Center 中複製 SCIM 端點值。將該值貼到 中的 SCIM 基礎 URL 欄位OneLogin。此外，在先前的程序中，您複製了 IAM Identity Center 中的存取字符值。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組態。
5. 在導覽窗格中，選擇 Provisioning (佈建)。
6. 選取啟用佈建、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. 在導覽窗格中，選擇使用者。
8. 按一下更多動作，然後選擇同步登入。您應該會收到使用 AWS 單一登入同步使用者的訊息。
9. 再次按一下更多動作，然後選擇重新套用權利映射。您應該會收到正在重新套用映射的訊息。
10. 此時，佈建程序應開始。若要確認，請導覽至活動 > 事件，並監控進度。成功的佈建事件以及錯誤都應該出現在事件串流中。
11. 若要確認您的使用者和群組皆已成功同步至 IAM Identity Center，請返回 IAM Identity Center 主控台並選擇使用者。來自 的同步使用者OneLogin會出現在使用者頁面上。您也可以群組頁面上檢視同步的群組。
12. 若要自動將使用者變更同步至 IAM Identity Center，請導覽至佈建頁面，找到需要管理員核准才能執行此動作區段，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OneLogin，以在 IAM Identity Center 中進行存取控制

OneLogin 如果您選擇設定要在 IAM Identity Center 中用來管理 AWS 資源存取的屬性，這是 的選用程序。您在 中定義的屬性OneLogin會在 SAML 聲明中傳遞至 IAM Identity Center。然後，您將在 IAM Identity Center 中建立許可集，以根據您從 傳遞的屬性來管理存取權OneLogin。

開始此程序之前，您必須先啟用[存取控制的屬性](#)此功能。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 中設定使用者屬性OneLogin，以在 IAM Identity Center 中控制存取控制

1. 登入 OneLogin，然後導覽至應用程式 > 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，以與 IAM Identity Center 建立 SAML 連線。選擇它，然後從導覽窗格中選擇參數。
3. 在必要參數區段中，針對您要在 IAM Identity Center 中使用的每個屬性執行下列動作：
 - a. 選擇 +。
 - b. 在欄位名稱中，輸入 `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`，並以您在 IAM Identity Center 中預期的屬性名稱 **AttributeName** 取代。例如 `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`。
 - c. 在旗標下，勾選包含在 SAML 聲明中的核取方塊，然後選擇儲存。
 - d. 在值欄位中，使用下拉式清單選擇 OneLogin 使用者屬性。例如，Department。
4. 選擇儲存。

（選用）傳遞屬性以進行存取控制

您可以選擇性地使用 IAM Identity Center 中的 [存取控制的屬性](#) 功能，傳遞 Name 屬性設為的 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》中的在 [中傳遞工作階段標籤 AWS STS](#)。

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，請為每個標籤加入個別的 Attribute 元素。

疑難排解

以下可協助您針對使用 設定自動佈建時可能遇到的一些常見問題進行疑難排解 OneLogin。

群組不會佈建至 IAM Identity Center

根據預設，群組可能不會從 佈建OneLogin至 IAM Identity Center。請確定您已在 中為 IAM Identity Center 應用程式啟用群組佈建OneLogin。若要這樣做，請登入OneLogin管理員主控台，並檢查以確保在 IAM Identity Center 應用程式 (IAM Identity Center 應用程式 > 參數 > 群組) 的屬性下選取包含在使用者佈建選項。如需如何在 中建立群組的詳細資訊OneLogin，包括如何在 SCIM 中同步OneLogin角色為群組，請參閱 [OneLogin網站](#)。

即使所有設定都正確，也不會從 同步OneLogin到 IAM Identity Center

除了上述有關管理員核准的備註之外，您將需要重新套用權利映射，許多組態變更才會生效。這可在應用程式 > 應用程式 > IAM Identity Center 應用程式 > 更多動作中找到。您可以在活動 > 事件下查看 中大多數動作的詳細資訊和日誌，OneLogin包括同步事件。

我已在 中刪除或停用群組OneLogin，但仍會出現在 IAM Identity Center 中

OneLogin 目前不支援群組的 SCIM DELETE 操作，這表示群組會持續存在於 IAM Identity Center 中。因此，您必須直接從 IAM Identity Center 移除群組，以確保移除該群組 IAM Identity Center 中的任何對應許可。

我刪除了 IAM Identity Center 中的群組，但未先從 刪除該群組OneLogin，現在發生使用者/群組同步問題

若要修正這種情況，請先確定您在 中沒有任何備援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。接著，刪除 IAM Identity Center 中任何不需要的群組。最後，在 中OneLogin重新整理權利 (IAM Identity Center 應用程式 > 佈建 > 權限)，然後重新套用權利映射 (IAM Identity Center 應用程式 > 更多動作)。若要避免未來發生此問題，請先進行變更以停止在 中佈建群組OneLogin，然後從 IAM Identity Center 刪除群組。

搭配 IAM Identity Center 使用 Ping Identity 產品

下列Ping Identity產品已透過 IAM Identity Center 進行測試。

主題

- [PingFederate](#)
- [PingOne](#)

PingFederate

IAM Identity Center 支援透過（以下稱「Ping」）從PingFederate產品自動佈建 Ping Identity（同步）使用者和群組資訊至 IAM Identity Center。此佈建使用 System for Cross-domain Identity Management (SCIM) v2.0 通訊協定。如需詳細資訊，請參閱[搭配外部身分提供者使用 SAML 和 SCIM 聯合身分](#)。

您可以使用 IAM Identity Center SCIM 端點和存取權杖PingFederate在 中設定此連線。當您設定 SCIM 同步時，您會在 中建立使用者屬性映射PingFederate至 IAM Identity Center 中具名屬性的映射。這會導致 IAM Identity Center 和 之間的預期屬性相符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。Ping 如需如何為其他版本的設定佈建至 IAM Identity Center 的詳細資訊，請聯絡 PingFederate。

下列步驟會逐步解說如何使用 SCIM 通訊協定，將使用者和群組從 自動佈建PingFederate至 IAM Identity Center。

Note

在您開始部署 SCIM 之前，建議您先檢閱 [使用自動佈建的考量事項](#)。然後繼續檢閱下一節的其他考量事項。

主題

- [先決條件](#)
- [考量事項](#)
- [步驟 1：在 IAM Identity Center 中啟用佈建](#)
- [步驟 2：在 中設定佈建 PingFederate](#)
- [（選用）步驟 3：在 PingFederate 中設定使用者屬性，以便在 IAM Identity Center 中進行存取控制](#)
- [（選用）傳遞屬性以進行存取控制](#)
- [疑難排解](#)

先決條件

您需要下列項目才能開始使用：

- 運作中的PingFederate伺服器。如果您沒有現有的PingFederate伺服器，您可能可以從 [Ping Identity](#) 網站取得免費試用或開發人員帳戶。該試驗包括授權和軟體下載以及相關文件。
- 安裝在PingFederate伺服器上的 PingFederate IAM Identity Center Connector 軟體副本。如需如何取得此軟體的詳細資訊，請參閱 Ping Identity 網站上的 [IAM Identity Center Connector](#)。
- 啟用 IAM Identity Center 的帳戶 ([免費](#))。如需詳細資訊，請參閱[啟用 IAM Identity Center](#)。
- 從PingFederate執行個體到 IAM Identity Center 的 SAML 連線。如需如何設定此連線的說明，請參閱 PingFederate 文件。總之，建議路徑是使用 IAM Identity Center Connector 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 Identity Center 之間交換 SAML 中繼資料。
- 如果您將 IAM Identity Center 複製到其他區域，則必須更新身分提供者組態，以啟用受 AWS 管應用程式和 AWS 帳戶 來自這些區域的存取。如需詳細資訊，請參閱[the section called “步驟 3：更新外部 IdP 設定”](#)。如需其他詳細資訊，請參閱 PingFederate 文件。

考量事項

以下是有關的重要考量PingFederate，這可能會影響您使用 IAM Identity Center 實作佈建的方式。

- 如果從在 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，則不會從 IAM Identity Center 中的對應使用者移除該屬性。這是PingFederate's佈建器實作的已知限制。如果屬性變更為使用者上的不同（非空白）值，則該變更會同步至 IAM Identity Center。

步驟 1：在 IAM Identity Center 中啟用佈建

在此第一個步驟中，您可以使用 IAM Identity Center 主控台來啟用自動佈建。

在 IAM Identity Center 中啟用自動佈建

1. 完成先決條件後，請開啟 [IAM Identity Center 主控台](#)。
2. 在左側導覽窗格中選擇設定。
3. 在設定頁面上，找到自動佈建資訊方塊，然後選擇啟用。這會立即在 IAM Identity Center 中啟用自動佈建，並顯示必要的 SCIM 端點和存取字符資訊。
4. 在傳入自動佈建對話方塊中，複製 SCIM 端點和存取字符。稍後在 IdP 中設定佈建時，您需要將這些項目貼入。
 - a. SCIM 端點 - 例如，`https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-444-55555555/scim/v2`

- b. 存取字符 - 選擇顯示字符以複製值。

Warning

這是您唯一可以取得 SCIM 端點和存取權杖的時間。在繼續之前，請務必複製這些值。您將在本教學課程稍後輸入這些值，以在 IdP 中設定自動佈建。

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 管理主控台完成其餘任務。，步驟如下列程序所述。

步驟 2：在 中設定佈建 PingFederate

在 PingFederate 管理主控台中使用下列程序來啟用 IAM Identity Center 與 IAM Identity Center Connector 之間的整合。此程序假設您已安裝 IAM Identity Center Connector 軟體。如果您尚未這麼做，請參閱 [先決條件](#)，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傳出 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 `pf.provisioner.mode` 的設定修改為 OFF（這是預設值）以外的值，如果目前正在執行，則重新啟動伺服器。例如，STANDALONE 如果您目前沒有的高可用性組態，您可以選擇使用 PingFederate。

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 Identity Center 建立 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。如果沒有，您必須先完成這些步驟，才能繼續。
5. 選取傳出佈建核取方塊，選擇 IAM Identity Center Cloud Connector 做為類型，然後按一下儲存。如果 IAM Identity Center Cloud Connector 未顯示為選項，請確定您已安裝 IAM Identity Center Connector 並重新啟動 PingFederate 伺服器。

6. 重複按一下下一步，直到您抵達傳出佈建頁面，然後按一下設定佈建按鈕。
7. 在先前的程序中，您會在 IAM Identity Center 中複製 SCIM 端點值。將該值貼到 PingFederate 主控台的 SCIM URL 欄位。此外，在先前的程序中，您複製了 IAM Identity Center 中的存取字符值。將該值貼到 PingFederate 主控台的存取字符欄位。按一下 Save (儲存)。
8. 在頻道組態 (設定頻道) 頁面上，按一下建立。
9. 輸入此新佈建頻道的頻道名稱 (例如 **AWSIAMIdentityCenterchannel**)，然後按一下下一步。
10. 在來源頁面上，選擇您要用於連線至 IAM Identity Center 的作用中資料存放區，然後按一下下一步。

 Note

如果您尚未設定資料來源，您現在必須這麼做。如需如何在 中選擇和設定資料來源的資訊，請參閱Ping產品文件PingFederate。

11. 在來源設定頁面上，確認安裝的所有值都正確，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，然後按一下下一步。例如，如果使用 Active Directory 做為 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，指定單一群組，其中包含您要佈建至 IAM Identity Center 的所有使用者。如果沒有這類單一群組，請在 AD 中建立該群組，返回此設定，然後輸入對應的 DN。
 - c. 指定是否搜尋子群組 (巢狀搜尋) 和任何必要的 LDAP 篩選條件。
 - d. 在群組 > 群組 DN 中，指定單一群組，其中包含您要佈建至 IAM Identity Center 的所有群組。在許多情況下，這可能會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條件值。
13. 在屬性映射頁面上，確保下列事項，然後按一下下一步：
 - a. userName 欄位必須對應至格式化為電子郵件的屬性 (user@domain.com)。它還必須符合使用者用來登入 Ping 的值。此值會在聯合身分驗證期間填入 SAML nameId宣告中，並用於比對 IAM Identity Center 中的使用者。例如，使用 Active Directory 時，您可以選擇將指定UserPrincipalName為 userName。
 - b. 尾碼為 * 的其他欄位必須映射至使用者非 Null 的屬性。
14. 在啟用與摘要頁面上，將頻道狀態設定為作用中，讓同步在儲存組態後立即開始。
15. 確認頁面上的所有組態值都正確，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 `provisioner.log` 檔案，預設位於您 PingFederate 伺服器上的 `pingfederate-<version>/pingfederate/log` 目錄中。
18. 若要確認使用者和群組已成功同步至 IAM Identity Center，請返回 IAM Identity Center 主控台並選擇使用者。來自的同步使用者 PingFederate 會出現在使用者頁面上。您也可以群組頁面上檢視同步的群組。

(選用) 步驟 3：在 PingFederate 中設定使用者屬性，以便在 IAM Identity Center 中進行存取控制

PingFederate 如果您選擇設定要在 IAM Identity Center 中用來管理 AWS 資源存取的屬性，這是的選用程序。您在 中定義的屬性 PingFederate 會在 SAML 聲明中傳遞至 IAM Identity Center。然後，您將在 IAM Identity Center 中建立許可集，以根據您從傳遞的屬性來管理存取權 PingFederate。

開始此程序之前，您必須先啟用 [存取控制的屬性](#) 此功能。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 中設定使用者屬性 PingFederate，以在 IAM Identity Center 中進行存取控制

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 Identity Center 建立 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。然後按一下設定瀏覽器 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，輸入 `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`，**AttributeName** 以您在 IAM Identity Center 中預期的屬性名稱取代。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. 在身分驗證來源映射頁面上，選擇使用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(資料存放區)和值(資料存放區屬性)`https://aws.amazon.com/SAML/Attributes/AccessControl:Department`。

Note

如果您尚未設定資料來源，則需要現在這麼做。如需如何在 中選擇和設定資料來源的資訊，請參閱Ping產品文件PingFederate。

10. 重複按一下下一步，直到您抵達啟用與摘要頁面，然後按一下儲存。

(選用) 傳遞屬性以進行存取控制

您可以選擇性地使用 IAM Identity Center 中的 [存取控制的屬性](#) 功能，傳遞 Name 屬性設為的 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》中的在 [中傳遞工作階段標籤 AWS STS](#)。

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，請為每個標籤加入個別的 Attribute 元素。

疑難排解

如需使用 進行一般 SCIM 和 SAML 疑難排解PingFederate，請參閱下列章節：

- [特定使用者無法從外部 SCIM 供應商同步到 IAM Identity Center](#)
- [IAM Identity Center 建立的 SAML 聲明內容相關問題](#)
- [使用外部身分提供者佈建使用者或群組時發生重複的使用者或群組錯誤](#)
- 如需的詳細資訊PingFederate，請參閱 [PingFederate 文件](#)。

下列資源可協助您在使用時進行故障診斷 AWS：

- [AWS re:Post](#) - 尋找FAQs和其他資源的連結，以協助您疑難排解問題。
- [AWS 支援](#) - 取得技術支援

PingOne

IAM Identity Center 支援透過（以下稱「Ping」）從PingOne產品自動佈建 Ping Identity（同步）使用者資訊至 IAM Identity Center。此佈建使用 System for Cross-domain Identity Management (SCIM) v2.0 通訊協定。您可以使用 IAM Identity Center SCIM 端點和存取權杖PingOne在 中設定此連線。當您設定 SCIM 同步時，您可以在 中建立使用者屬性映射PingOne至 IAM Identity Center 中具名屬性的映射。這會導致 IAM Identity Center 和 之間的預期屬性相符PingOne。

下列步驟會逐步解說如何使用 SCIM 通訊協定，將使用者從 自動佈建PingOne至 IAM Identity Center。

Note

在您開始部署 SCIM 之前，建議您先檢閱 [使用自動佈建的考量事項](#)。然後繼續檢閱下一節的其他考量事項。

主題

- [先決條件](#)
- [考量事項](#)
- [步驟 1：在 IAM Identity Center 中啟用佈建](#)
- [步驟 2：在 中設定佈建 PingOne](#)
- [（選用）步驟 3：在 中設定使用者屬性PingOne，以在 IAM Identity Center 中進行存取控制](#)
- [（選用）傳遞屬性以進行存取控制](#)
- [疑難排解](#)

先決條件

您需要下列項目才能開始使用：

- PingOne 訂閱或免費試用，同時具備聯合身分驗證和佈建功能。如需如何取得免費試用的詳細資訊，請參閱 [Ping Identity](#) 網站。

- 啟用 IAM Identity Center 的帳戶 ([免費](#))。如需詳細資訊，請參閱[啟用 IAM Identity Center](#)。
- PingOne IAM Identity Center 應用程式已新增至您的PingOne管理員入口網站。您可以從 Application Catalog PingOne 取得 IAM Identity Center PingOne 應用程式。如需一般資訊，請參閱 Ping Identity 網站上的[從 Application Catalog 新增應用程式](#)。
- 從PingOne執行個體到 IAM Identity Center 的 SAML 連線。將 PingOne IAM Identity Center 應用程式新增至PingOne管理員入口網站後，您必須使用它來設定從PingOne執行個體到 IAM Identity Center 的 SAML 連線。在兩端使用「下載」和「匯入」中繼資料功能，在 PingOne和 IAM Identity Center 之間交換 SAML 中繼資料。如需如何設定此連線的說明，請參閱 PingOne 文件。
- 如果您將 IAM Identity Center 複寫到其他區域，則必須更新身分提供者組態，以啟用受 AWS 管應用程式和 AWS 帳戶 來自這些區域的存取。如需詳細資訊，請參閱[the section called “步驟 3：更新外部 IdP 設定”](#)。如需其他詳細資訊，請參閱 PingOne 文件。

考量事項

以下是有關的重要考量PingOne，這可能會影響您使用 IAM Identity Center 實作佈建的方式。

- PingOne 不支援透過 SCIM 佈建群組。如需的 SCIM 中群組支援的最新資訊Ping，請聯絡 PingOne。
- 在 PingOne管理員入口網站中停用佈建PingOne之後，使用者可以繼續從 佈建。如果您需要立即終止佈建，請刪除相關的 SCIM 承載字符，和/或在 IAM Identity Center [使用 SCIM 從外部身分提供者佈建使用者和群組](#)中停用。
- 如果從 中設定的資料存放區中移除使用者的屬性PingOne，則不會從 IAM Identity Center 中的對應使用者中移除該屬性。這是PingOne's佈建器實作的已知限制。如果修改屬性，變更會同步至 IAM Identity Center。
- 以下是有關 中 SAML 組態的重要備註PingOne：
 - IAM Identity Center 僅支援 emailAddress NameId 格式。這表示您需要為 中的 SAML_SUBJECT 映射選擇 目錄中唯一的使用者屬性PingOne，而非 Null，並格式化為電子郵件/UPN (例如 user@domain.com)PingOne。Email (Work) 是搭配PingOne內建目錄用於測試組態的合理值。
 - 中PingOne包含 + 字元的電子郵件地址的使用者可能無法登入 IAM Identity Center，並出現錯誤，例如 'SAML_215' 或 'Invalid input'。若要修正此問題，請在 PingOne中選擇屬性映射中 SAML_SUBJECT 映射的進階選項。然後在下拉式功能表urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress中設定要傳送至 SP： 的名稱 ID 格式。

步驟 1：在 IAM Identity Center 中啟用佈建

在此第一個步驟中，您可以使用 IAM Identity Center 主控台來啟用自動佈建。

在 IAM Identity Center 中啟用自動佈建

1. 完成先決條件後，請開啟 [IAM Identity Center 主控台](#)。
2. 在左側導覽窗格中選擇設定。
3. 在設定頁面上，找到自動佈建資訊方塊，然後選擇啟用。這會立即在 IAM Identity Center 中啟用自動佈建，並顯示必要的 SCIM 端點和存取字符資訊。
4. 在傳入自動佈建對話方塊中，複製 SCIM 端點和存取字符。稍後在 IdP 中設定佈建時，您需要將這些項目貼入。
 - a. SCIM 端點 - 例如，`https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-444-55555555/scim/v2`
 - b. 存取字符 - 選擇顯示字符以複製值。

Warning

這是您唯一可以取得 SCIM 端點和存取權杖的時間。在繼續之前，請務必複製這些值。您將在本教學課程稍後輸入這些值，以在 IdP 中設定自動佈建。

5. 選擇關閉。

現在您已在 IAM Identity Center 主控台中設定佈建，您需要使用 PingOne IAM Identity Center 應用程式完成其餘任務。這些步驟會在下列程序中說明。

步驟 2：在 中設定佈建 PingOne

在 PingOne IAM Identity Center 應用程式中使用下列程序，以啟用使用 IAM Identity Center 的佈建。此程序假設您已將 PingOne IAM Identity Center 應用程式新增至 PingOne 管理員入口網站。如果您尚未這麼做，請參閱 [先決條件](#)，然後完成此程序以設定 SCIM 佈建。

在 中設定佈建 PingOne

1. 開啟您在為 PingOne 設定 SAML 時安裝的 IAM Identity Center 應用程式 PingOne(應用程式 > 我的應用程式)。請參閱 [先決條件](#)。
2. 捲動至頁面底部。在使用者佈建下，選擇完整連結以導覽至連線的使用者佈建組態。

3. 在佈建指示頁面上，選擇繼續下一個步驟。
4. 在先前的程序中，您會在 IAM Identity Center 中複製 SCIM 端點值。將該值貼到 IAM Identity Center PingOne 應用程式的 SCIM URL 欄位中。此外，在先前的程序中，您複製了 IAM Identity Center 中的存取字符值。將該值貼到 IAM Identity Center PingOne 應用程式的 ACCESS_TOKEN 欄位。
5. 針對 REMOVE_ACTION，選擇已停用或刪除（如需詳細資訊，請參閱頁面上的說明文字）。
6. 在屬性映射頁面上，依照本頁[考量事項](#)稍早的指導方針，選擇要用於 SAML_SUBJECT (NameId) 聲明的值。然後選擇繼續下一步。
7. 在PingOne應用程式自訂 - IAM Identity Center 頁面上，進行任何所需的自訂變更（選用），然後按一下繼續下一個步驟。
8. 在群組存取頁面上，選擇包含您要啟用以佈建和單一登入 IAM Identity Center 之使用者的群組。選擇繼續至下一步。
9. 捲動至頁面底部，然後選擇完成以開始佈建。
10. 若要確認使用者已成功同步至 IAM Identity Center，請返回 IAM Identity Center 主控台並選擇使用者。來自的同步使用者PingOne會出現在使用者頁面上。這些使用者現在可以指派給 IAM Identity Center 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。如需詳細資訊Ping，請聯絡。

（選用）步驟 3：在 中設定使用者屬性PingOne，以在 IAM Identity Center 中進行存取控制

PingOne 如果您選擇設定 IAM Identity Center 的屬性來管理對 AWS 資源的存取，這是 的選用程序。您在 中定義的屬性PingOne會在 SAML 聲明中傳遞至 IAM Identity Center。然後，您可以在 IAM Identity Center 中建立許可集，以根據您從 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[存取控制的屬性](#)此功能。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 中設定使用者屬性PingOne，以在 IAM Identity Center 中控制存取控制

1. 開啟您在為 PingOne 設定 SAML 時安裝的 IAM Identity Center 應用程式 PingOne(應用程式 > 我的應用程式)。
2. 選擇編輯，然後選擇繼續下一步，直到到達屬性映射頁面。
3. 在屬性映射頁面上，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 Identity Center 中使用的每個屬性執行這些步驟，以進行存取控制。

- a. 在應用程式屬性欄位中，輸入 `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`。以您在 IAM Identity Center 中預期的屬性名稱取代 `AttributeName`。例如 `https://aws.amazon.com/SAML/Attributes/AccessControl:Email`。
 - b. 在 Identity Bridge 屬性或文字值欄位中，從您的 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。

（選用）傳遞屬性以進行存取控制

您可以選擇性地使用 IAM Identity Center 中的 [存取控制的屬性](#) 功能，傳遞 Name 屬性設為的 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》中的在 [中傳遞工作階段標籤 AWS STS](#)。

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，請為每個標籤加入個別的 Attribute 元素。

疑難排解

如需使用 進行一般 SCIM 和 SAML 疑難排解 PingOne，請參閱下列章節：

- [特定使用者無法從外部 SCIM 供應商同步到 IAM Identity Center](#)
- [IAM Identity Center 建立的 SAML 聲明內容相關問題](#)
- [使用外部身分提供者佈建使用者或群組時發生重複的使用者或群組錯誤](#)
- 如需的詳細資訊 PingOne，請參閱 [PingOne 文件](#)。

下列資源可協助您在使用時進行故障診斷 AWS：

- [AWS re:Post](#) - 尋找FAQs和其他資源的連結，以協助您疑難排解問題。
- [AWS 支援](#) - 取得技術支援

使用預設 IAM Identity Center 目錄設定使用者存取權

當您第一次啟用 IAM Identity Center 時，會自動設定 Identity Center 目錄做為您的預設身分來源，因此您不需要選擇身分來源。如果您的組織使用其他身分提供者，例如 Microsoft Active Directory、或 Microsoft Entra ID，Okta請考慮將該身分來源與 IAM Identity Center 整合，而不是使用預設組態。

目標

在本教學課程中，您將使用預設目錄做為身分來源和 IAM Identity Center 組織執行個體，以設定和測試管理使用者。此管理使用者會建立和管理使用者和群組，並使用許可集授予 AWS 存取權。在後續步驟中，您將建立下列項目：

- 名為 *Nikki Wolf* 的管理使用者
- 名為 *Admin ###* 群組
- 名為 *AdminAccess* 的許可集

若要驗證一切是否已正確建立，您將登入並設定管理使用者的密碼。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、建立其他許可集，以及設定應用程式的組織存取權。或者，如果您想要授予使用者存取應用程式的權限，您可以遵循此程序的[步驟 1](#) 並[設定應用程式存取](#)。

先決條件

完成本教學課程需要下列先決條件：

- [啟用 IAM Identity Center](#) 和 具有 [IAM Identity Center 的組織執行個體](#)。
 - 如果您有 IAM Identity Center [的帳戶執行個體](#)，您可以建立使用者和群組，並授予他們存取應用程式的權限。如需詳細資訊，請參閱[應用程式存取](#)。
- 登入 AWS 管理主控台，並以下列任一方式存取 IAM Identity Center 主控台：
 - 新使用者 AWS（根使用者）– 選擇AWS 帳戶 根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者的身分登入。在下一頁中，輸入您的密碼。
 - 已使用 AWS (IAM 登入資料) – 使用具有管理許可的 IAM 登入資料登入。
 - 如需登入的更多說明 AWS 管理主控台，請參閱 [AWS 登入指南](#)。

- 您可以為 IAM Identity Center 使用者設定多重驗證。如需詳細資訊，請參閱[在 IAM Identity Center 中設定 MFA](#)。

步驟 1：新增使用者

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在 IAM Identity Center 導覽窗格中，選擇使用者，然後選取新增使用者。
3. 在指定使用者詳細資訊頁面上，完成下列資訊：

- 使用者名稱 - 在本教學課程中，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，而且您稍後無法變更。

- 密碼 - 選擇使用密碼設定指示（建議）傳送電子郵件給此使用者。

此選項會傳送來自 Amazon Web Services 的電子郵件給使用者，主旨行邀請加入 IAM Identity Center。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已核准的寄件者清單。

- 電子郵件地址 - 輸入您可以接收電子郵件之使用者的電子郵件地址。然後，再次輸入以確認。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。在本教學課程中，輸入 *Nikki*。
 - 姓氏 - 輸入使用者的姓氏。在本教學課程中，輸入 *Wolf*。
 - 顯示名稱 - 預設值為使用者的名字和姓氏。如果您想要變更顯示名稱，您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。
 - 視需要填寫選用資訊。在本教學課程中不會使用它，您可以稍後進行變更。
4. 選擇下一步。將使用者新增至群組頁面隨即出現。我們將建立一個群組來指派管理許可給，而不是直接將它們提供給 *Nikki*。

選擇建立群組

新的瀏覽器索引標籤隨即開啟，顯示建立群組頁面。

- a. 在群組詳細資訊下，在群組名稱中輸入群組的名稱。我們建議使用群組名稱來識別群組的角色。在本教學課程中，輸入 *#####*。
- b. 選擇建立群組

- c. 關閉群組瀏覽器索引標籤以返回新增使用者瀏覽器索引標籤

5. 在群組區域中，選取重新整理按鈕。**#####**群組會出現在清單中。

選取**#####**旁的核取方塊，然後選擇下一步。

6. 在檢閱和新增使用者頁面上，確認下列事項：

- 主要資訊會如您預期般顯示
- 群組會顯示新增至您建立之群組的使用者

如需變更，請選擇 Edit (編輯)。當所有詳細資訊都正確時，請選擇新增使用者。

通知訊息會通知您已新增使用者。

接下來，您將新增**#####**群組的管理許可，以便 *Nikki* 可以存取 資源。

步驟 2：新增管理許可

Important

只有在您啟用 [IAM Identity Center 的組織執行個體](#) 時，才能執行下列步驟。

1. 在 IAM Identity Center 導覽窗格中的多帳戶許可下，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及其下的帳戶。選取管理帳戶的核取方塊，然後選取指派使用者或群組。
3. 此時會顯示指派使用者和群組工作流程。它包含三個步驟：
 - a. 針對步驟 1：選取使用者和群組，選擇您建立的**#####**群組。然後選擇下一步。
 - b. 針對步驟 2：選取許可集選擇建立許可集，以開啟新標籤，逐步引導您完成建立許可集所涉及的三個子步驟。
 - i. 對於步驟 1：選取許可集類型完成下列項目：
 - 在許可集類型中，選擇預先定義的許可集。
 - 在預先定義許可集的政策中，選擇 AdministratorAccess。
 - 選擇下一步。
 - ii. 對於步驟 2：指定許可集詳細資訊，保留預設設定，然後選擇下一步。

預設設定會建立名為 *AdministratorAccess* 的許可集，並將工作階段持續時間設定為一小時。您可以在許可集名稱欄位中輸入新名稱，以變更許可集的名稱。

- iii. 針對步驟 3：檢閱和建立，確認許可集類型使用 AWS 受管政策 *AdministratorAccess*。選擇建立。在許可集頁面上會出現通知，通知您已建立許可集。您現在可以在 Web 瀏覽器中關閉此索引標籤。

在指派使用者和群組瀏覽器索引標籤上，您仍在步驟 2：選取您從中開始建立許可集工作流程的許可集。

在許可集區域中，選擇重新整理按鈕。您建立的 *AdministratorAccess* 許可集會出現在清單中。選取該許可集的核取方塊，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* 許可集，然後選擇提交。

頁面會以 AWS 帳戶 正在設定 的訊息進行更新。等待程序完成。

您會返回 AWS 帳戶 頁面。通知訊息會通知您 AWS 帳戶，您的 已重新佈建並套用更新的許可集。

恭喜您！

您已成功設定第一個使用者、群組和許可集。

在本教學課程的下一部分中，您將使用其管理登入資料登入存取入口網站並設定其密碼，以測試 *Nikki # AWS* 存取。立即登出 主控台。

步驟 3：測試使用者存取許可

現在 *Nikki Wolf* 是您組織中的使用者，他們可以登入並存取根據其許可集授予許可的資源。若要驗證使用者是否已正確設定，在下一個步驟中，您將使用 *Nikki #* 登入資料來登入並設定其密碼。當您在步驟 1 新增使用者 *Nikki Wolf* 時，您選擇讓 *Nikki* 收到包含密碼設定指示的電子郵件。是時候開啟該電子郵件並執行下列動作：

1. 在電子郵件中，選取接受邀請連結以接受邀請。

 Note

電子郵件也包含 **Nikki** #使用者名稱，以及他們將用來登入組織的 AWS 存取入口網站 URL。記錄此資訊以供日後使用。

系統會將您導向新使用者註冊頁面，您可以在其中設定 **Nikki** 的密碼並[註冊其 MFA 裝置](#)。

2. 設定 **Nikki** 的密碼後，您會導覽至登入頁面。輸入 **nikkiw**，然後選擇下一步，然後輸入 **Nikki** 的密碼，然後選擇登入。
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，然後選取帳戶以顯示您可用來存取帳戶中資源的角色。

每個許可集都有兩種您可以使用的管理方法，即角色或存取金鑰。

- 角色，例如 **AdministratorAccess** - 開啟 AWS Console Home。
- 存取金鑰 - 提供您可以搭配 AWS CLI 或 和 AWS SDK 使用的登入資料。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 AWS SDKs 的 IAM Identity Center 使用者憑證](#)。

4. 選擇角色連結以登入 AWS Console Home。

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

後續步驟

現在您已在 IAM Identity Center 中建立管理使用者，您可以：

- [指派應用程式](#)
- [新增其他使用者](#)
- [將使用者指派給帳戶](#)
- [設定其他許可集](#)

 Note

您可以將多個許可集指派給相同的使用者。若要遵循套用最低權限許可的最佳實務，請在建立管理使用者之後建立更嚴格的許可集，並將其指派給相同的使用者。如此一來，您 AWS 帳戶 只可以使用所需的許可來存取，而不是管理許可。

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是針對他們獲指派的 AWS 帳戶、角色和應用程式。

教學課程影片

作為其他資源，您可以使用這些影片教學來進一步了解如何設定外部身分提供者：

- [在 中的外部身分提供者之間遷移 AWS IAM Identity Center](#)
- [使用 聯合現有 AWS IAM Identity Center 執行個體 Microsoft Entra ID](#)

在 IAM Identity Center 中設定您的人力資源

IAM Identity Center 是將您的人力資源使用者連線至 Kiro 和 Amazon Quick 等 AWS 受管應用程式和其他 AWS 資源 AWS 的解決方案。您可以連接現有的身分提供者，並從目錄同步使用者和群組，或直接在 IAM Identity Center 中建立和管理使用者。

已使用 IAM 存取 AWS 帳戶？

您不需要對目前的 AWS 帳戶 工作流程進行任何變更，即可使用 IAM Identity Center 存取 AWS 受管應用程式。如果您使用[聯合身分搭配 IAM](#) 進行 AWS 帳戶 存取，您的使用者可以繼續以他們一直擁有 AWS 帳戶 的相同方式存取，而且您可以繼續使用現有的工作流程來管理該存取。

選擇最適合您組織身分管理策略和現有基礎設施的方法。

主題

- [IAM Identity Center 中的使用者、群組和佈建](#)
- [管理您的身分來源](#)
- [在 Identity Center 目錄中管理使用者](#)

IAM Identity Center 中的使用者、群組和佈建

IAM Identity Center 可讓您控制誰可以登入，以及他們可以存取哪些資源。必須佈建使用者才能登入。然後，您只能將存取權指派給佈建的使用者或群組。了解 IAM Identity Center 中的使用者、群組和佈建。

使用者名稱和電子郵件地址唯一性

IAM Identity Center 要求每個使用者都有唯一的使用者名稱。使用者名稱是使用者的主要識別符。使用者名稱不需要符合使用者的電子郵件地址。IAM Identity Center 要求您使用者的所有使用者名稱和電子郵件地址都是非 NULL 且唯一的。

Groups (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 Identity Center 不支援巢狀群組（群組中的群組）。群組在將存取權指派給 AWS 帳戶 和 應用程式時非常有用。您可以將許可授予群組，而不是個別指派每個使用者。稍後，當您從群組新增或移除使用者時，使用者會動態取得或失去您指派給群組的帳戶和應用程式的存取權。

使用者和群組佈建

佈建是讓使用者和群組資訊可供 IAM Identity Center 和 AWS 受管應用程式或客戶受管應用程式使用的程序。您可以直接在 IAM Identity Center 中建立使用者和群組，或將您的身分來源連線到 IAM Identity Center。透過 IAM Identity Center，您可以指派使用者和群組對連線應用程式 和 的存取權 AWS 帳戶。

IAM Identity Center 中的佈建會根據您使用的身分來源而有所不同。如需詳細資訊，請參閱[管理您的身分來源](#)。

取消佈建使用者和群組

取消佈建是從 IAM Identity Center 移除使用者和群組資訊的程序。

如果您使用 Active Directory 或外部身分提供者搭配 IAM Identity Center，您應該從這些身分來源移除使用者和群組，而不是 IAM Identity Center。如果您的身分來源是 Active Directory 或外部身分提供者，刪除 IAM Identity Center 使用者和群組不會將其完全移除。

如果您需要取消佈建 IAM Identity Center 使用者或群組，應先[將許可集或應用程式的任何指派](#)移除給您要取消佈建的使用者或群組。否則，您會在 IAM Identity Center 中擁有未指派的許可集和應用程式指派。

管理您的身分來源

IAM Identity Center 中的身分來源會定義使用者和群組的管理位置。設定身分來源後，您可以查詢使用者或群組，以授予使用者 AWS 帳戶、應用程式或兩者的單一登入存取權。

每個組織只能有一個身分來源 AWS Organizations。您可以選擇下列其中一項做為您的身分來源：

- [外部身分提供者](#) – 如果您想要管理外部身分提供者 (IdP) 中的使用者，例如 Okta 或 Microsoft Entra ID，請選擇此選項。
- [您的內部部署或 AWS 受管 Active Directory](#) – 如果您想要連接 Active Directory (AD)，請選擇此選項。
- [Identity Center 目錄](#) – 當您第一次啟用 IAM Identity Center 時，除非您選擇不同的身分來源，否則它會自動設定為 Identity Center 目錄做為您的預設身分來源。使用 Identity Center 目錄，您可以建立使用者和群組，並將他們的存取層級指派給您的 AWS 帳戶 和 應用程式。

 Note

IAM Identity Center 不支援以 SAMBA4-based Simple AD 做為身分來源。

主題

- [變更身分來源的考量事項](#)
- [變更您的身分來源](#)
- [IAM Identity Center 中支援的使用者和群組屬性](#)
- [外部身分提供者](#)
- [Microsoft AD 目錄](#)

變更身分來源的考量事項

雖然您可以隨時變更身分來源，但我們建議您考慮此變更如何影響您目前的部署。

如果您已經在一個身分來源中管理使用者和群組，變更為不同的身分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。

變更 IAM Identity Center 的身分來源之前，請先檢閱下列考量，再繼續。如果您想要繼續變更身分來源，請參閱 [變更您的身分來源](#) 以取得詳細資訊。

在 IAM Identity Center 目錄和 Active Directory 之間變更

如果您已在 Active Directory 中管理使用者和群組，我們建議您在啟用 IAM Identity Center 並選擇身分來源時，考慮連接目錄。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，請先執行此操作。

 Important

將 IAM Identity Center 中的身分來源類型變更為 Active Directory 或從 Active Directory 變更時，請注意 Identity Store ID 會變更。這可能會有下列影響：

- 您的預設 AWS 存取入口網站 URL 將會變更。您需要將新的 URL 傳達給人力資源，並更新書籤、Gateway 或防火牆允許清單，以及參考此 URL 的組態。我們建議您在排定的維護時段執行此變更，以將對使用者的干擾降至最低。

- 如果您在 IAM Identity Center 中使用客戶受管 KMS 金鑰進行靜態加密，並且已使用加密內容設定 KMS 金鑰政策，請注意 Identity Store 的加密內容將會變更。例如，在 Identity Store ARN "arn:aws:identitystore::123456789012:identitystore/d-922763e9b3" 中，"d-922763e9b3" 是 Identity Store ID。為避免在此轉換期間發生服務中斷，請暫時修改 KMS 金鑰政策以使用萬用字元模式："arn:aws:identitystore::123456789012:identitystore/*"。

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

- 已移除的指派和已刪除的使用者和群組 – 將您的身分來源變更為 Active Directory 會從 Identity Center 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，在變更為 Active Directory 之後，您必須將使用者和群組從 Active Directory 同步到 Identity Center 目錄，然後重新套用其指派。

如果您選擇不使用 Active Directory，則必須在 Identity Center 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 – 在 Identity Center 目錄中刪除身分時，IAM Identity Center 中也會刪除對應的指派。不過，在 Active Directory 中，刪除身分時（在 Active Directory 中或同步身分中），不會刪除對應的指派。
- APIs 沒有傳出同步 – 如果您使用 Active Directory 做為身分來源，建議您謹慎使用[建立、更新和刪除](#) APIs。IAM Identity Center 不支援傳出同步，因此您的身分來源不會自動更新您使用這些 APIs 對使用者或群組所做的變更。
- 存取入口網站 URL 將會變更 – 在 IAM Identity Center 和 Active Directory 之間變更您的身分來源也會變更 AWS 存取入口網站的 URL。
- 如果在 IAM Identity Center 主控台中使用 Identity Store APIs 刪除或停用使用者，具有作用中工作階段的使用者可以繼續存取整合的應用程式和帳戶。如需身分驗證工作階段持續時間和使用者的資訊，請參閱 [了解 IAM Identity Center 中的身分驗證工作階段](#)。

如需 IAM Identity Center 如何佈建使用者和群組的資訊，請參閱 [Microsoft AD 目錄](#)。

從 IAM Identity Center 變更為外部 IdP

如果您將身分來源從 IAM Identity Center 變更為外部身分提供者 (IdP)，請考慮下列事項：

- 指派和成員資格使用正確的聲明 – 只要新的 IdP 傳送正確的聲明（例如 SAML nameIDs），您的使用者指派、群組指派和群組成員資格就會繼續運作。這些聲明必須符合 IAM Identity Center 中的使用者名稱和群組。
- 無傳出同步 – IAM Identity Center 不支援傳出同步，因此您的外部 IdP 不會自動更新您在 IAM Identity Center 中對使用者和群組所做的變更。
- SCIM 佈建 – 如果您使用 SCIM 佈建，身分提供者中的使用者和群組變更只會在身分提供者將這些變更傳送至 IAM Identity Center 之後，才反映在 IAM Identity Center 中。請參閱 [使用自動佈建的考量事項](#)。
- 回復 – 您可以隨時使用 IAM Identity Center 將身分來源還原為 [從外部 IdP 變更為 IAM Identity Center](#)。
- 現有的使用者工作階段會在工作階段持續時間到期時撤銷 – 一旦您將身分來源變更為外部身分提供者，作用中的使用者工作階段會在主控台中設定的工作階段持續時間上限剩餘時間內保留。例如，如果 AWS 存取入口網站工作階段持續時間設定為 8 小時，且您在第四小時內變更了身分來源，則作用中的使用者工作階段會再保留 4 小時。若要撤銷使用者工作階段，請參閱 [the section called “結束人力使用者的作用中工作階段”](#)。

如果在 IAM Identity Center 主控台中使用 Identity Store APIs 刪除或停用使用者，具有作用中工作階段的使用者可以繼續存取整合的應用程式和帳戶。如需身分驗證工作階段持續時間和使用者的資訊，請參閱 [了解 IAM Identity Center 中的身分驗證工作階段](#)。

Note

刪除使用者之後，您無法從 IAM Identity Center 主控台撤銷使用者工作階段。

如需 IAM Identity Center 如何佈建使用者和群組的資訊，請參閱 [外部身分提供者](#)。

從外部 IdP 變更為 IAM Identity Center

如果您將身分來源從外部身分提供者 (IdP) 變更為 IAM Identity Center，請考慮下列事項：

- IAM Identity Center 會保留您的所有指派。
- 強制重設密碼 – 在 IAM Identity Center 中擁有密碼的使用者可以繼續使用其舊密碼繼續登入。對於位於外部 IdP 且不在 IAM Identity Center 的使用者，管理員必須強制重設密碼。
- 現有的使用者工作階段會在工作階段持續時間到期時撤銷 – 一旦您將身分來源變更為 IAM Identity Center，作用中的使用者工作階段會在主控台中設定的工作階段持續時間上限的剩餘期間內保留。例如，如果 AWS 存取入口網站工作階段持續時間為 8 小時，而且您在第四小時變更了身分來源，

則作用中的使用者工作階段會繼續額外執行 4 小時。若要撤銷使用者工作階段，請參閱 [the section called “結束人力使用者的作用中工作階段”](#)。

如果在 IAM Identity Center 主控台中使用 Identity Store APIs 刪除或停用使用者，具有作用中工作階段的使用者可以繼續存取整合的應用程式和帳戶。如需身分驗證工作階段持續時間和使用者行為的資訊，請參閱 [了解 IAM Identity Center 中的身分驗證工作階段](#)。

Note

刪除使用者之後，您將無法從 IAM Identity Center 主控台撤銷使用者工作階段。

- 多區域支援 – 如果您已將 IAM Identity Center 複寫至其他區域或計劃這樣做，您必須使用外部身分提供者做為身分來源。如需包含其他先決條件的詳細資訊，請參閱 [跨多個 使用 IAM Identity Center AWS 區域](#)。

如需 IAM Identity Center 如何佈建使用者和群組的資訊，請參閱 [在 Identity Center 目錄中管理使用者](#)。

從一個外部 IdP 變更為另一個外部 IdP

如果您已經使用外部 IdP 做為 IAM Identity Center 的身分來源，並變更為不同的外部 IdP，請考慮下列事項：

- 指派和成員資格使用正確的聲明 – IAM Identity Center 會保留所有指派。只要新的 IdP 傳送正確的聲明（例如 SAML nameIDs），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 驗證時，這些聲明必須符合 IAM Identity Center 中的使用者名稱。

- SCIM 佈建 – 如果您使用 SCIM 佈建至 IAM Identity Center，建議您檢閱本指南中的 IdP 特定資訊，以及 IdP 提供的文件，以確保新的供應商在啟用 SCIM 時正確符合使用者和群組。
- 現有的使用者工作階段會在工作階段持續時間到期時撤銷 – 一旦您將身分來源變更為不同的外部身分提供者，作用中的使用者工作階段會在主控台中設定的工作階段持續時間上限的剩餘期間內保留。例如，如果 AWS 存取入口網站工作階段持續時間為 8 小時，而且您在第四小時變更了身分來源，則作用中的使用者工作階段會再保留 4 小時。若要撤銷使用者工作階段，請參閱 [the section called “結束人力使用者的作用中工作階段”](#)。

如果在 IAM Identity Center 主控台中使用 Identity Store APIs 刪除或停用使用者，具有作用中工作階段的使用者可以繼續存取整合的應用程式和帳戶。如需身分驗證工作階段持續時間和使用者行為的資訊，請參閱 [了解 IAM Identity Center 中的身分驗證工作階段](#)。

Note

刪除使用者之後，您無法從 IAM Identity Center 主控台撤銷使用者工作階段。

如需 IAM Identity Center 如何佈建使用者和群組的資訊，請參閱 [外部身分提供者](#)。

在 Active Directory 和外部 IdP 之間變更

如果您將身分來源從外部 IdP 變更為 Active Directory，或從 Active Directory 變更為外部 IdP，請考慮下列事項：

- 刪除使用者、群組和指派 – 從 IAM Identity Center 刪除所有使用者、群組和指派。外部 IdP 或 Active Directory 中不會影響使用者或群組資訊。
- 佈建使用者 – 如果您變更為外部 IdP，則必須設定 IAM Identity Center 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，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。
- 如果在 IAM Identity Center 主控台中使用 Identity Store APIs 刪除或停用使用者，具有作用中工作階段的使用者可以繼續存取整合的應用程式和帳戶。如需身分驗證工作階段持續時間和使用行為的資訊，請參閱 [了解 IAM Identity Center 中的身分驗證工作階段](#)。
- 多區域支援 – 如果您已將 IAM Identity Center 複寫至其他區域或計劃這樣做，您必須使用外部身分提供者做為身分來源。如需包含其他先決條件的詳細資訊，請參閱 [跨多個使用 IAM Identity Center AWS 區域](#)。

如需 IAM Identity Center 如何佈建使用者和群組的資訊，請參閱 [Microsoft AD 目錄](#)。

變更您的身分來源

下列程序說明如何從 IAM Identity Center 提供的目錄（預設 Identity Center 目錄）變更為 Active Directory 或外部身分提供者，或反之亦然。在繼續之前，請檢閱 [變更身分來源的考量事項](#)。若要完成此程序，您需要 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱 [IAM Identity Center 的組織和帳戶執行個體](#)。

⚠ Warning

根據您目前的部署，此變更會移除您在 IAM Identity Center 中設定的任何使用者和群組指派。此變更也會從您的 移除許可集 IAM 角色 AWS 帳戶。因此，您可能需要更新資源政策，並應確保這不會中斷對 AWS KMS 金鑰和 Amazon EKS 叢集的存取。如需詳細資訊，請參閱 [在資源政策、Amazon EKS 叢集組態映射和 AWS KMS 金鑰政策中參考許可集](#)。

發生這種情況時，所有使用者和群組，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。

變更您的身分來源

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤。選擇動作，然後選擇變更身分來源。
4. 在選擇身分來源下，選取您要變更的來源，然後選擇下一步。

如果您要變更為 Active Directory，請從下一頁的選單中選擇可用的目錄。

⚠ Important

在 Active Directory 之間變更您的身分來源會刪除 Identity Center 目錄中的使用者和群組。此變更也會移除您在 IAM Identity Center 中設定的任何指派。

i Note

如果您將 IAM Identity Center 複寫到其他區域，您將無法變更身分來源類型。您只能將目前的外部 IdP 取代為另一個外部 IdP。若要變更身分來源類型，您必須先移除所有其他區域。如需詳細資訊，請參閱[跨多個 使用 IAM Identity Center AWS 區域](#)

如果您要切換到外部身分提供者，建議您遵循中的步驟[如何連線至外部身分提供者](#)。

5. 在您閱讀免責聲明並準備好繼續之後，請輸入 ACCEPT。
6. 選擇變更身分來源。如果您要將身分來源變更為 Active Directory，請繼續下一個步驟。

7. 將身分來源變更為 Active Directory 會帶您前往設定頁面。在設定頁面上，執行下列其中一項操作：
- 選擇開始引導式設定。如需如何完成引導式設定程序的詳細資訊，請參閱 [引導式設定](#)。
 - 在身分來源區段中，選擇動作，然後選擇管理同步以設定您的同步範圍，以及要同步的使用者和群組清單。

IAM Identity Center 中支援的使用者和群組屬性

本指南提供 IAM Identity Center 中 SCIM 屬性支援的參考。它列出 IAM Identity Center 身分存放區中支援 SCIM 規格中的哪些使用者和群組屬性，並識別不支援的特定屬性和子屬性。

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片段，例如 name、email 或 members。IAM Identity Center 透過手動項目和自動 SCIM 佈建支援最常用的屬性。

- 如需跨網域身分管理 (SCIM) 規格的相關資訊，請參閱 <https://tools.ietf.org/html/rfc7642>。
- 如需手動和自動佈建的相關資訊，請參閱 [使用者來自外部 IdP 時的佈建](#)。
- 如需屬性映射的資訊，請參閱 [IAM Identity Center 與外部身分提供者目錄之間的屬性映射](#)。

由於 IAM Identity Center 支援 SCIM 自動佈建使用案例，因此 Identity Center 目錄支援 SCIM 規格中列出的所有相同使用者和群組屬性，但有少數例外。下列各節說明 IAM Identity Center 不支援哪些屬性。

不支援使用者物件

IAM Identity Center 身分存放區支援來自 SCIM 使用者結構描述 (<https://tools.ietf.org/html/rfc7643#section-8.3> : //) 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，但下列項目除外：

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

- 'version' 'meta' 屬性的子屬性

不支援群組物件

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，但下列項目除外：

- 'display' 任何多值屬性的子屬性（例如成員）。

外部身分提供者

使用 IAM Identity Center，您可以透過安全聲明標記語言 (SAML) 2.0 和跨網域身分管理 (SCIM) 通訊協定，從外部身分提供者 (IdPs) 連接現有的人力資源身分。這可讓您的使用者使用其公司登入資料登入 AWS 存取入口網站。然後，他們可以導覽至在外部 IdPs 中託管的指派帳戶、角色和應用程式。

例如，您可以將外部 IdP 例如 Okta 或 Microsoft Entra ID 連接到 IAM Identity Center。然後，您的使用者可以使用現有的 Okta 或 Microsoft Entra ID 登入資料登入 AWS 存取入口網站。若要控制使用者登入後可以執行的動作，您可以將存取許可集中指派給 AWS 組織中所有帳戶和應用程式。此外，開發人員可以使用現有的登入資料登入 AWS Command Line Interface (AWS CLI)，並受益於自動產生短期登入資料和輪換。

如果您在 Active Directory 或 中使用自我管理目錄 AWS Managed Microsoft AD，請參閱 [Microsoft AD 目錄](#)。

Note

SAML 通訊協定不提供查詢 IdP 以了解使用者和群組的方式。因此，您必須將使用者和群組佈建到 IAM Identity Center，讓 IAM Identity Center 知道這些使用者和群組。

使用者來自外部 IdP 時的佈建

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 Identity Center，才能對 AWS 帳戶或應用程式進行任何指派。若要這樣做，您可以[使用 SCIM 從外部身分提供者佈建使用者和群組](#)為使用者和群組設定，或使用[手動佈建](#)。無論您如何佈建使用者，IAM Identity Center 都會將 AWS 管理主控台、命令列界面和應用程式身分驗證重新導向至外部 IdP。然後，IAM Identity Center 會根據您在 IAM Identity Center 中建立的政策授予這些資源的存取權。如需佈建的詳細資訊，請參閱[使用者和群組佈建](#)。

主題

- [如何連線至外部身分提供者](#)
- [如何在 IAM Identity Center 中變更外部身分提供者的中繼資料](#)
- [搭配外部身分提供者使用 SAML 和 SCIM 聯合身分](#)
- [SCIM 設定檔和 SAML 2.0 實作](#)

如何連線至外部身分提供者

支援的外部 IdPs 有不同的先決條件、考量事項和佈建程序。有幾個 step-by-step 教學課程：IdPs

- [CyberArk](#)
- [Google Workspace](#)
- [JumpCloud](#)
- [Microsoft Entra ID](#)
- [Okta](#)
- [OneLogin](#)
- [Ping 身分](#)

如需 IAM Identity Center 支援的外部 IdPs 考量事項的詳細資訊，請參閱 [搭配外部身分提供者使用 SAML 和 SCIM 聯合身分](#)。

下列程序提供與所有外部身分提供者搭配使用的程序的一般概觀。

連線至外部身分提供者

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，然後選擇動作 > 變更身分來源。
4. 在選擇身分來源下，選取外部身分提供者，然後選擇下一步。
5. 在設定外部身分提供者下，執行下列動作：
 - 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，並將其儲存在系統中。外部身分提供者需要 IAM Identity Center SAML 中繼資料檔案。

 Note

您下載的 SAML 中繼資料檔案包含 IPv4-only 和雙堆疊聲明消費者服務 (ACS) URLs。此外，如果您的 IAM Identity Center 複寫到其他區域，中繼資料檔案會包含每個其他區域的 ACS URLs。如果您的外部 IdP 限制了 ACS URLs 的數量，您將需要移除不必要的 ACS URLs。例如，如果您的組織已完全採用雙堆疊端點，且不再使用 IPv4-only 的端點，您可以移除後者。另一種方法是不使用中繼資料檔案，而是將 ACS URLs 複製並貼到外部 IdP 中。

- b. 在身分提供者中繼資料下，選擇選擇檔案，然後找到您從外部身分提供者下載的中繼資料檔案。然後上傳檔案。此中繼資料檔案包含必要的公有 x509 憑證，用於信任從 IdP 傳送的訊息。
- c. 選擇下一步。

 Important

在 Active Directory 之間變更來源會移除所有現有的使用者和群組指派。成功變更來源後，您必須手動重新套用指派。

6. 在您閱讀免責聲明並準備好繼續之後，請輸入 ACCEPT。
7. 選擇變更身分來源。狀態訊息會通知您已成功變更身分來源。

如何在 IAM Identity Center 中變更外部身分提供者的中繼資料

您可以變更先前提供給 IAM Identity Center 的外部身分提供者中繼資料。這些變更會影響使用者透過 IAM Identity Center 登入和存取 AWS 資源的能力。下列程序說明如何更新存放在 IAM Identity Center 中的外部 IdP 中繼資料。若要完成此程序，您需要 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱 [IAM Identity Center 的組織和帳戶執行個體](#)。

變更外部身分提供者的中繼資料

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤。選擇動作，然後選擇管理身分驗證。

4. 在身分提供者中繼資料區段中，選擇編輯 IdP 中繼資料。您可以在此頁面上變更外部 IdP 的 IdP 登入 URL 和 或 IdP 發行者 URL。當您進行所有必要的變更時，請選擇儲存變更。

搭配外部身分提供者使用 SAML 和 SCIM 聯合身分

IAM Identity Center 針對聯合身分實作下列標準型通訊協定：

- 用於使用者身分驗證的 SAML 2.0
- 用於佈建的 SCIM

實作這些標準通訊協定的任何身分提供者 (IdP) 預期會與 IAM Identity Center 成功互通，但有下列特殊考量：

- SAML
 - IAM Identity Center 需要電子郵件地址的 SAML nameID 格式（即 `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`）。
 - 宣告中 nameID 欄位的值必須是 RFC 2822 (<https://tools.ietf.org/html/rfc2822>) addr-spec 合規（“name@domain.com”）字串 (<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 entityId、X509 憑證和 SingleSignOnService，做為登入 URL 的一部分。
 - 不支援加密金鑰。
 - IAM Identity Center 不支援簽署傳送至外部 IdPs SAML 身分驗證請求。
 - 如果您打算將 IAM Identity Center 複寫到其他區域，IdP 必須支援多個聲明消費者服務 (ACS) URLs，並充分利用多區域 IAM Identity Center 的優勢。如需詳細資訊，請參閱[跨多個 使用 IAM Identity Center AWS 區域](#)。使用單一 ACS URL 可能會影響其他區域中的使用者體驗。您的主要區域會繼續正常運作。如需使用單一 ACS URL 在其他區域中使用者體驗的詳細資訊，請參閱 [the section called “使用沒有多個 ACS URLs AWS 受管應用程式”](#)和 [the section called “AWS 帳戶 在沒有多個 ACS URLs存取彈性”](#)。
- SCIM
 - IAM Identity Center SCIM 實作是以 SCIM RFCs7642 (<https://tools.ietf.org/html/rfc7642>)、7643 (<https://tools.ietf.org/html/rfc7643>) 和 7644 (<https://tools.ietf.org/html/rfc7644>) 為基礎，以及 FastFed Basic SCIM Profile 1.0 (https://openid.net/specs/fastfed-scim-1_0-02.html#rfc.section.4) 的 2020 年 3 月草案中概述的互通性要求。IAM Identity Center SCIM 實作開發人員指南的[支援 API 操作](#)一節說明這些文件與 IAM Identity Center 中目前實作之間的差異。

不支援不符合上述標準和考量事項的 IdPs。如需有關其產品是否符合這些標準和考量事項的問題或釐清，請聯絡您的 IdP。

如果您在將 IdP 連線至 IAM Identity Center 時遇到任何問題，建議您檢查：

- AWS CloudTrail 透過篩選事件名稱 ExternalIdPDirectoryLogin 的日誌
- IdP 特定的日誌和/或偵錯日誌
- [對 IAM Identity Center 問題進行故障診斷](#)

Note

有些 IdPs，例如中的 IdP [IAM Identity Center 身分來源教學課程](#)，以專為 IAM Identity Center 建置的「應用程式」或「連接器」形式，為 IAM Identity Center 提供簡化的組態體驗。如果您的 IdP 提供此選項，我們建議您使用它，請小心選擇專為 IAM Identity Center 建置的項目。其他稱為「AWS」、「AWS 聯合」或類似一般「AWS」名稱的項目可能會使用其他聯合方法和/或端點，並且可能無法如預期與 IAM Identity Center 搭配使用。

SCIM 設定檔和 SAML 2.0 實作

SCIM 和 SAML 都是設定 IAM Identity Center 的重要考量事項。

SAML 2.0 實作

IAM Identity Center 支援 [SAML \(安全性聲明標記語言\)](#) 2.0 的聯合身分。這可讓 IAM Identity Center 從外部身分提供者 (IdPs) 驗證身分。SAML 2.0 是一項開放標準，用於安全地交換 SAML 聲明。SAML 2.0 會在 SAML 授權單位 (稱為身分提供者或 IdP) 與 SAML 消費者 (稱為服務提供者或 SP) 之間傳遞使用者的相關資訊。IAM Identity Center 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提供者憑證來存取 AWS 帳戶 和設定應用程式。

IAM Identity Center 會將 SAML IdP 功能新增至您的 IAM Identity Center 存放區 AWS Managed Microsoft AD 或外部身分提供者。然後，使用者可以單一登入支援 SAML 的服務，包括 AWS 管理主控台 和第三方應用程式 Concur，例如 Microsoft 365、和 Salesforce。

不過，SAML 通訊協定不提供查詢 IdP 以了解使用者和群組的方式。因此，您必須將使用者和群組佈建到 IAM Identity Center，讓 IAM Identity Center 知道這些使用者和群組。

SCIM 設定檔

IAM Identity Center 支援跨網域身分管理 (SCIM) 2.0 版標準。SCIM 讓您的 IAM Identity Center 身分與 IdP 中的身分保持同步。這包括在您的 IdP 與 IAM Identity Center 之間佈建、更新和取消佈建使用者。

如需如何實作 SCIM 的詳細資訊，請參閱 [使用 SCIM 從外部身分提供者佈建使用者和群組](#)。如需 IAM Identity Center SCIM 實作的其他詳細資訊，請參閱 [IAM Identity Center SCIM 實作開發人員指南](#)。

主題

- [使用 SCIM 從外部身分提供者佈建使用者和群組](#)
- [輪換 SAML 2.0 憑證](#)

使用 SCIM 從外部身分提供者佈建使用者和群組

IAM Identity Center 支援使用跨網域身分管理 (SCIM) 2.0 版通訊協定，將身分提供者 (IdP) 的使用者和群組資訊自動佈建（同步）至 IAM Identity Center。當您設定 SCIM 同步時，您可以建立身分提供者 (IdP) 使用者屬性與 IAM Identity Center 中具名屬性的映射。這會導致 IAM Identity Center 和 IdP 之間的預期屬性相符。您可以使用 IAM Identity Center 的 SCIM 端點和您在 IAM Identity Center 中建立的承載字符，在 IdP 中設定此連線。

主題

- [使用自動佈建的考量事項](#)
- [如何監控存取權杖過期](#)
- [產生存取權杖](#)
- [啟用自動佈建](#)
- [刪除存取權杖](#)
- [停用自動佈建](#)
- [輪換存取字符](#)
- [稽核和協調自動佈建的資源](#)
- [手動佈建](#)

使用自動佈建的考量事項

開始部署 SCIM 之前，建議您先檢閱下列有關其如何與 IAM Identity Center 搭配使用的重要考量。如需其他佈建考量，請參閱 [IAM Identity Center 身分來源教學課程](#) 適用於 IdP 的。

- 如果您要佈建主要電子郵件地址，則每個使用者的此屬性值必須是唯一的。在某些 IdPs 中，主要電子郵件地址可能不是真正的電子郵件地址。例如，它可能是僅看起來像電子郵件的通用主體名稱 (UPN)。這些 IdPs 可能有次要或「其他」電子郵件地址，其中包含使用者的真實電子郵件地址。您必須在 IdP 中設定 SCIM，將非空的唯一電子郵件地址對應至 IAM Identity Center 主要電子郵件地址屬性。而且，您必須將使用者非空的唯一登入識別符映射至 IAM Identity Center 使用者名稱屬性。檢查您的 IdP 是否有單一值同時是登入識別符和使用者的電子郵件名稱。如果是這樣，您可以將該 IdP 欄位映射到 IAM Identity Center 主要電子郵件和 IAM Identity Center 使用者名稱。
- 若要讓 SCIM 同步運作，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。如果使用者遺失任何這些值，將不會佈建該使用者。
- 如果您需要使用第三方應用程式，您必須先將傳出 SAML 主體屬性映射至使用者名稱屬性。如果第三方應用程式需要可路由的電子郵件地址，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提供者控制。只有在您的身分提供者將變更傳送至 IAM Identity Center 之後，您的身分提供者的使用者和群組變更才會反映在 IAM Identity Center 中。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，不會使用 SCIM 佈建多值屬性（例如指定使用者的多個電子郵件或電話號碼）。嘗試將多值屬性與 SCIM 同步至 IAM Identity Center 將會失敗。為了避免失敗，請確保每個屬性只傳遞一個值。如果您有具有多值屬性的使用者，請在 IdP 移除或修改 SCIM 中重複的屬性映射，以連線至 IAM Identity Center。
- 確認 IdP 的 externalId SCIM 映射對應至使用者唯一、永遠存在且最不可能變更的值。例如，您的 IdP 可能會提供保證 objectId 或其他識別符，不受名稱和電子郵件等使用者屬性的變更影響。如果是這樣，您可以將該值映射到 SCIM externalId 欄位。如果您需要變更使用者的名稱或電子郵件，這可確保您的使用者不會遺失 AWS 權利、指派或許可。
- 尚未指派給應用程式或 AWS 帳戶 無法佈建至 IAM Identity Center 的使用者。若要同步使用者和群組，請確定他們已指派給應用程式或其他代表 IdP 與 IAM Identity Center 連線的設定。
- 使用者取消佈建行為由身分提供者管理，並可能因其實作而有所不同。如需取消佈建使用者的詳細資訊，請洽詢您的身分提供者。
- 使用 IdP 的 SCIM 設定自動佈建之後，您無法再在 IAM Identity Center 主控台中新增或編輯使用者。如果您需要新增或修改使用者，您必須從外部 IdP 或身分來源執行此操作。

如需 IAM Identity Center SCIM 實作的詳細資訊，請參閱 [IAM Identity Center SCIM 實作開發人員指南](#)。

如何監控存取權杖過期

SCIM 存取字符的產生有效期為一年。當您的 SCIM 存取權杖設定為在 90 天內過期時，會在 IAM Identity Center 主控台和儀表板中 AWS 傳送提醒 AWS Health，以協助您輪換權杖。透過在過期之前輪換 SCIM 存取權杖，您可以持續保護使用者和群組資訊的自動佈建。如果 SCIM 存取權杖過期，使用者和群組資訊從您的身分提供者同步到 IAM Identity Center 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，並影響對您服務的存取。

Identity Center 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的或過期的存取權杖為止。AWS Health 儀表板事件每週續約 90 到 60 天、每週兩次從 60 到 30 天、每週三次從 30 到 15 天，以及每天 15 天，直到 SCIM 存取字符過期為止。

產生存取權杖

使用下列程序在 IAM Identity Center 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[啟用自動佈建](#)。

產生新的存取權杖

1. 在 [IAM Identity Center 主控台](#) 中，選擇左側導覽窗格中的設定。
2. 在設定頁面上，選擇身分來源索引標籤，然後選擇動作 > 管理佈建。
3. 在自動佈建頁面的存取字符下，選擇產生字符。
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地方。
5. 選擇關閉。

啟用自動佈建

使用下列程序，使用 SCIM 通訊協定，將使用者和群組從 IdP 自動佈建至 IAM Identity Center。

Note

在開始此程序之前，建議您先檢閱適用於 IdP 的佈建考量。如需詳細資訊，請參閱 IdP [IAM Identity Center 身分來源教學課程](#) 的。

在 IAM Identity Center 中啟用自動佈建

1. 完成先決條件後，請開啟 [IAM Identity Center 主控台](#)。
2. 在左側導覽窗格中選擇設定。
3. 在設定頁面上，找到自動佈建資訊方塊，然後選擇啟用。這會立即在 IAM Identity Center 中啟用自動佈建，並顯示必要的 SCIM 端點和存取字符資訊。
4. 在傳入自動佈建對話方塊中，複製 SCIM 端點和存取字符。稍後在 IdP 中設定佈建時，您需要將這些項目貼入。
 - a. SCIM 端點 - 例如，`https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-4444-55555555/scim/v2`
 - b. 存取字符 - 選擇顯示字符以複製值。

Warning

這是您唯一可以取得 SCIM 端點和存取權杖的時間。在繼續之前，請務必複製這些值。您將在本教學稍後輸入這些值，以設定 IdP 中的自動佈建。

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，請參閱 IdP [IAM Identity Center 身分來源教學課程](#)的。

刪除存取權杖

使用下列程序刪除 IAM Identity Center 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 Identity Center 主控台](#) 中，選擇左側導覽窗格中的設定。
2. 在設定頁面上，選擇身分來源索引標籤，然後選擇動作 > 管理佈建。
3. 在自動佈建頁面的存取字符下，選取您要刪除的存取字符，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。

停用自動佈建

使用下列程序在 IAM Identity Center 主控台中停用自動佈建。

⚠ Important

您必須先刪除存取權杖，才能開始此程序。如需詳細資訊，請參閱[刪除存取權杖](#)。

在 IAM Identity Center 主控台中停用自動佈建

1. 在 [IAM Identity Center 主控台](#) 中，選擇左側導覽窗格中的設定。
2. 在設定頁面上，選擇身分來源索引標籤，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。

輪換存取字符

IAM Identity Center 目錄一次最多支援兩個存取字符。若要在任何輪換之前產生額外的存取權杖，請刪除任何過期或未使用的存取權杖。

如果您的 SCIM 存取權杖即將過期，您可以使用下列程序在 IAM Identity Center 主控台中輪換現有的存取權杖。

輪換存取字符

1. 在 [IAM Identity Center 主控台](#) 中，選擇左側導覽窗格中的設定。
2. 在設定頁面上，選擇身分來源索引標籤，然後選擇動作 > 管理佈建。
3. 在自動佈建頁面的存取字符下，記下您要輪換的字符的字符 ID。
4. 請依照 中的步驟[產生存取權杖](#)建立新的權杖。如果您已建立最大數量的 SCIM 存取權杖，您必須先刪除其中一個現有的權杖。
5. 前往您的身分提供者的網站，設定新的存取字符以進行 SCIM 佈建，然後使用新的 SCIM 存取字符測試與 IAM Identity Center 的連線。確認佈建使用新的字符成功運作後，請繼續此程序的下一個步驟。
6. 請依照 中的步驟[刪除存取權杖](#)，刪除您先前記下的舊存取字符。您也可以使用字符的建立日期作為要移除字符的提示。

稽核和協調自動佈建的資源

SCIM 可讓您自動將使用者、群組和群組成員資格從身分來源佈建至 IAM Identity Center。本指南可協助您驗證和協調這些資源，以維持準確的同步。

為什麼要稽核您的資源？

定期稽核有助於確保您的存取控制保持準確，且您的身分提供者 (IdP) 與 IAM Identity Center 保持適當同步。這對安全合規和存取管理尤其重要。

您可以稽核的資源：

- 使用者
- Groups (群組)
- 群組成員資格

您可以使用 AWS Identity Store [APIs](#) 或 [CLI 命令](#) 來執行稽核和調校。下列範例使用 AWS CLI 命令。如需 API 替代方案，請參閱 Identity Store API 參考中的 [對應操作](#)。

如何稽核資源

以下是如何使用 AWS CLI 命令稽核這些資源的範例。

開始前，請確保您具備以下條件：

- IAM Identity Center 的管理員存取權。
- AWS CLI 已安裝並設定。如需詳細資訊，請參閱 [AWS 命令列界面使用者指南](#)。
- Identity Store 命令所需的 IAM 許可。

步驟 1：列出目前的資源

您可以使用 檢視目前的 資源 AWS CLI。

Note

使用 時 AWS CLI，除非您指定 `--no-paginate`，否則系統會自動處理分頁。如果您直接呼叫 API（例如，使用 SDK 或自訂指令碼），請在回應 `NextToken` 中處理。這可確保您擷取跨多個頁面的所有結果。

Example適用於 使用者

```
aws identitystore list-users \  
  --region REGION \  
  --output text
```

```
--identity-store-id IDENTITY_STORE_ID
```

Example適用於 群組的

```
aws identitystore list-groups \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Example群組成員資格

```
aws identitystore list-group-memberships \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID
```

步驟 2：與您的身分來源比較

將列出的資源與您的身分來源進行比較，以識別任何差異，例如：

- IAM Identity Center 中應佈建的遺失資源。
- 應從 IAM Identity Center 移除的額外資源。

Example適用於 使用者

```
# Create missing users  
aws identitystore create-user \  
  --identity-store-id IDENTITY_STORE_ID \  
  --user-name USERNAME \  
  --display-name DISPLAY_NAME \  
  --name GivenName=FIRST_NAME,FamilyName=LAST_NAME \  
  --emails Value=EMAIL,Primary=true  
  
# Delete extra users  
aws identitystore delete-user \  
  --identity-store-id IDENTITY_STORE_ID \  
  --user-id USER_ID
```

Example適用於 群組的

```
# Create missing groups
```

```
aws identitystore create-group \  
  --identity-store-id IDENTITY_STORE_ID \  
  [group attributes]  
  
# Delete extra groups  
aws identitystore delete-group \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID
```

Example 群組成員資格

```
# Add missing members  
aws identitystore create-group-membership \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID \  
  --member-id '{"UserId": "USER_ID"}'  
  
# Remove extra members  
aws identitystore delete-group-membership \  
  --identity-store-id IDENTITY_STORE_ID \  
  --membership-id MEMBERSHIP_ID
```

考量事項

- 命令受限於[服務配額和 API 限流](#)。
- 當您在對帳期間發現許多差異時，請對 AWS Identity Store 進行小型、漸進的變更。這可協助您避免影響多個使用者的錯誤。
- SCIM 同步可以覆寫您的手動變更。檢查您的 IdP 設定以了解此行為。

手動佈建

有些 IdPs 沒有跨網域身分管理 (SCIM) 支援系統，或具有不相容的 SCIM 實作。在這些情況下，您可以透過 IAM Identity Center 主控台手動佈建使用者。當您將使用者新增至 IAM Identity Center 時，請確定您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的名稱。如需詳細資訊，請參閱[使用者名稱和電子郵件地址唯一性](#)。

您還必須在 IAM Identity Center 中手動管理所有群組。若要這樣做，您可以使用 IAM Identity Center 主控台建立群組並新增群組。這些群組不需要符合 IdP 中存在的內容。如需詳細資訊，請參閱[Groups \(群組\)](#)。

輪換 SAML 2.0 憑證

IAM Identity Center 使用憑證來設定 IAM Identity Center 與您的外部身分提供者 (IdP) 之間的 SAML 信任關係。在 IAM Identity Center 中新增外部 IdP 時，您還必須從外部 IdP 取得至少一個公有 SAML 2.0 X.509 憑證。該憑證通常在信任建立期間的 IdP SAML 中繼資料交換期間自動安裝。

身為 IAM Identity Center 管理員，您偶爾需要用較新的 IdP 憑證取代較舊的 IdP 憑證。例如，當憑證上的過期日期接近時，您可能需要取代 IdP 憑證。使用較新的憑證取代較舊憑證的程序稱為憑證輪換。

主題

- [輪換 SAML 2.0 憑證](#)
- [憑證過期狀態指示燈](#)

輪換 SAML 2.0 憑證

您可能需要定期匯入憑證，才能輪換身分提供者發行的無效或過期憑證。這有助於防止身分驗證中斷或停機。所有匯入的憑證都會自動啟用。只有在確保憑證不再與相關聯的身分提供者搭配使用之後，才應該刪除憑證。

您也應該考慮某些 IdPs 可能不支援多個憑證。在這種情況下，使用這些 IdPs 輪換憑證的行為可能意味著使用者暫時的服務中斷。成功重新建立與該 IdP 的信任時，會還原服務。如果可能，請在尖峰時段仔細規劃此操作。

Note

作為安全最佳實務，在現有 SAML 憑證發生任何入侵或處理不當的跡象時，您應該立即移除並輪換憑證。

輪換 IAM Identity Center 憑證是一個包含下列項目的多步驟程序：

- 從 IdP 取得新憑證
- 將新憑證匯入 IAM Identity Center
- 在 IdP 中啟用新憑證
- 刪除較舊的憑證

使用下列所有程序來完成憑證輪換程序，同時避免任何身分驗證停機時間。

步驟 1：從 IdP 取得新憑證

前往 IdP 網站並下載其 SAML 2.0 憑證。請確定已下載 PEM 編碼格式的憑證檔案。大多數提供者允許您在 IdP 中建立多個 SAML 2.0 憑證。這些項目可能會標示為已停用或非作用中。

步驟 2：將新憑證匯入 IAM Identity Center

使用下列程序，使用 IAM Identity Center 主控台匯入新憑證。

1. 在 [IAM Identity Center 主控台](#) 中，選擇設定。
2. 在設定頁面上，選擇身分來源索引標籤，然後選擇動作 > 管理身分驗證。
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，導覽至您的憑證檔案並加以選取，然後選擇匯入憑證。

此時，IAM Identity Center 會信任從您匯入的兩個憑證簽署的所有傳入 SAML 訊息。

步驟 3：在 IdP 中啟用新憑證

返回 IdP 網站，並將您先前建立的新憑證標記為主要憑證或作用中憑證。此時，IdP 簽署的所有 SAML 訊息都應使用新的憑證。

步驟 4：刪除舊憑證

使用下列程序來完成 IdP 的憑證輪換程序。至少必須列出一個有效的憑證，而且無法移除。

Note

刪除之前，請確定您的身分提供者不再使用此憑證簽署 SAML 回應。

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，輸入 **DELETE** 進行確認，然後選擇刪除。
3. 返回 IdP 的網站並執行必要的步驟，以移除較舊的非作用中憑證。

憑證過期狀態指示燈

管理 SAML 2.0 憑證頁面會在清單中每個憑證旁的過期資料欄中顯示彩色狀態指示燈圖示。以下說明 IAM Identity Center 用來判斷每個憑證顯示哪個圖示的條件。

- 紅色 – 表示憑證已過期。
- 黃色 – 表示憑證會在 90 天內過期。
- 綠色 – 表示憑證有效，且至少再維持有效 90 天。

檢查憑證的目前狀態

1. 在 [IAM Identity Center 主控台](#) 中，選擇設定。
2. 在設定頁面上，選擇身分來源索引標籤，然後選擇動作 > 管理身分驗證。
3. 在管理 SAML 2.0 身分驗證頁面的管理 SAML 2.0 憑證下，檢閱清單中憑證的狀態，如 過期資料欄所示。

Microsoft AD 目錄

透過 AWS IAM Identity Center，您可以使用 來連接 Active Directory (AD) 中的自我管理目錄或 中的目錄 AWS Managed Microsoft AD AWS Directory Service。此 Microsoft AD 目錄定義了管理員在使用 IAM Identity Center 主控台指派單一登入存取時可從中提取的身分集區。將公司目錄連線至 IAM Identity Center 之後，您就可以授予 AD 使用者或群組對應用程式或兩者 AWS 帳戶的存取權。

AWS Directory Service 可協助您設定和執行 中託管的獨立 AWS Managed Microsoft AD 目錄 AWS 雲端。您也可以使用 Directory Service 將 AWS 資源與現有的自我管理 AD 連線。若要設定 AWS Directory Service 以使用自我管理 AD，您必須先設定信任關係，將身分驗證延伸至雲端。

IAM Identity Center 使用 提供的連線 Directory Service，對來源 AD 執行個體執行傳遞身分驗證。當您使用 AWS Managed Microsoft AD 做為身分來源時，IAM Identity Center 可以與透過 AD 信任連線之任何網域 AWS Managed Microsoft AD 的使用者搭配使用。如果您想要在四個或多個網域中尋找使用者，使用者在執行登入 IAM Identity Center 時必須使用 DOMAIN\user 語法作為使用者名稱。

備註

- 作為先決條件步驟，請確定 AWS Managed Microsoft AD 中的 AD Connector 或目錄 Directory Service 位於您的 AWS Organizations 管理帳戶中。
- IAM Identity Center 不支援以 SAMBA 4 為基礎的 Simple AD 做為連線目錄。
- IAM Identity Center 無法同步外部安全委託人 (FSPs)。如果 中的 AWS Managed Microsoft AD 群組包含來自信任網域的成員做為 FSPs，這些成員將不會同步。

如需使用 Active Directory 做為 IAM Identity Center 身分來源的程序示範，請參閱下列YouTube影片：

[使用 Active Directory 做為 AWS IAM Identity Center | Amazon Web Services 的身分來源](#)

使用 Active Directory 的考量事項

如果您想要使用 Active Directory 做為身分來源，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，則必須在設定 AWS Managed Microsoft AD 目錄 AWS 區域 的相同 中啟用 IAM Identity Center。IAM Identity Center 會將指派資料存放在與 目錄相同的區域中。若要管理 IAM Identity Center，您可能需要切換到已設定 IAM Identity Center 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 管理帳戶中的 Active Directory：

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 AWS Managed Microsoft AD 一次只能連接一個 AD Connector 目錄或 中的一個目錄。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 中的目錄 AWS Managed Microsoft AD 連接至 IAM Identity Center](#)
- [將 Active Directory 中的自我管理目錄連接到 IAM Identity Center](#)
- 使用位於委派管理員帳戶中的 Active Directory：

如果您計劃啟用 IAM Identity Center 委派管理員，並使用 Active Directory 做為 IAM Identity Center 身分來源，您可以使用位於委派管理員帳戶中的 AWS 目錄中設定的現有 AD Connector 或 AWS Managed Microsoft AD 目錄。

如果您決定將 IAM Identity Center 身分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，則目錄必須位於（由擁有）IAM Identity Center 委派管理員成員帳戶中，如果存在的話，則必須位於管理帳戶中。

連接 Active Directory 並指定使用者

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至 IAM Identity Center。

您可以使用 IAM Identity Center 連接 Active Directory 中的 目錄 AWS Managed Microsoft AD 或自我管理目錄。

 Note

IAM Identity Center 不支援以 SAMBA4-based Simple AD 做為身分來源。

AWS Managed Microsoft AD

1. 檢閱 中的指引[Microsoft AD 目錄](#)。
2. 請遵循 [將 中的目錄 AWS Managed Microsoft AD 連接至 IAM Identity Center](#) 中的步驟。
3. 設定 Active Directory 以同步您要將管理許可授予 IAM Identity Center 的使用者。如需詳細資訊，請參閱[將管理使用者同步至 IAM Identity Center](#)。

Active Directory 中的自我管理目錄

1. 檢閱 中的指引[Microsoft AD 目錄](#)。
2. 請遵循 [將 Active Directory 中的自我管理目錄連接到 IAM Identity Center](#) 中的步驟。
3. 設定 Active Directory 以同步您要將管理許可授予 IAM Identity Center 的使用者。如需詳細資訊，請參閱[將管理使用者同步至 IAM Identity Center](#)。

外部 IdP

1. 檢閱 中的指引[外部身分提供者](#)。
2. 請遵循 [如何連線至外部身分提供者](#) 中的步驟。
3. 設定 IdP 將使用者佈建至 IAM Identity Center。

 Note

在設定從 IdP 到 IAM Identity Center 的所有人力資源身分的自動群組型佈建之前，建議您將要授予管理許可的單一使用者同步到 IAM Identity Center。

將管理使用者同步至 IAM Identity Center

將 Active Directory 連線至 IAM Identity Center 之後，您可以指定要授予管理許可的使用者，然後將該使用者從目錄同步到 IAM Identity Center。

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，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，然後選擇新增。
6. 在新增的使用者和群組下，執行下列動作：
 - a. 確認已指定您要授予管理許可的使用者。
 - 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清單中的使用者中。
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出現在清單中。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。您將建立管理許可集，並將使用者指派給該許可集，藉此設定此帳戶的管理存取權。如需詳細資訊，請參閱[建立許可集](#)。

使用者來自 Active Directory 時的佈建

IAM Identity Center 使用 提供的連線 Directory Service，將 Active Directory 中來源目錄的使用者、群組和成員資格資訊同步到 IAM Identity Center 身分存放區。不會將密碼資訊同步至 IAM Identity Center，因為使用者身分驗證會直接從 Active Directory 中的來源目錄進行。應用程式會使用此身分資料來促進應用程式內查詢、授權和協同合作案例，而不會將 LDAP 活動傳遞回 Active Directory 中的來源目錄。

如需佈建的詳細資訊，請參閱 [使用者和群組佈建](#)。

主題

- [將 中的目錄 AWS Managed Microsoft AD 連接至 IAM Identity Center](#)
- [將 Active Directory 中的自我管理目錄連接到 IAM Identity Center](#)
- [IAM Identity Center 與外部身分提供者目錄之間的屬性映射](#)
- [IAM Identity Center 可設定的 AD 同步](#)

將 中的目錄 AWS Managed Microsoft AD 連接至 IAM Identity Center

使用下列程序，將 管理 AWS Managed Microsoft AD 的 目錄連線至 AWS Directory Service IAM Identity Center。

AWS Managed Microsoft AD 連線至 IAM Identity Center

1. 開啟 [IAM Identity Center 主控台](#)。

Note

請確定 IAM Identity Center 主控台正在使用目錄 AWS Managed Microsoft AD 所在的其中一個區域，然後再移至下一個步驟。

2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，然後選擇動作 > 變更身分來源。
4. 在選擇身分來源下，選取 Active Directory，然後選擇下一步。
5. 在連線作用中目錄下，AWS Managed Microsoft AD 從清單中選擇 中的目錄，然後選擇下一步。
6. 在確認變更下，檢閱資訊和就緒類型 ACCEPT，然後選擇變更身分來源。

Important

若要將 Active Directory 中的使用者指定為 IAM Identity Center 中的管理使用者，您必須先將要將管理許可從 Active Directory 授予的使用者同步至 IAM Identity Center。若要啟用，請依照「[將管理使用者同步至 IAM Identity Center](#)」中的步驟進行。

將 Active Directory 中的自我管理目錄連接到 IAM Identity Center

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 AWS 帳戶 和 應用程式的單一登入 AWS 存取權。若要為這些使用者設定單一登入存取，您可以執行下列其中一項操作：

- 建立雙向信任關係 – 在 AD 中於 AWS Managed Microsoft AD 和自我管理目錄之間建立雙向信任關係時，AD 中自我管理目錄中的使用者可以使用其公司登入資料登入各種 AWS 服務和業務應用程式。單向信任不適用於 IAM Identity Center。

AWS IAM Identity Center 需要雙向信任，使其具有從您的網域讀取使用者和群組資訊的許可，以同步使用者和群組中繼資料。IAM Identity Center 會在指派許可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合作，例如當您與其他使用者或群組共用儀表板時。從 Directory Service for Microsoft Active Directory 到您網域的信任允許 IAM Identity Center 信任您的網域進行身分驗證。相反方向的信任會授予讀取使用者和群組中繼資料的 AWS 許可。

如需設定雙向信任的詳細資訊，請參閱《AWS Directory Service 管理指南》中的[何時建立信任關係](#)。

Note

為了使用 AWS 應用程式，例如 IAM Identity Center 從信任的網域讀取 Directory Service 目錄使用者，Directory Service 帳戶需要信任使用者的 userAccountControl 屬性許可。如果沒有此屬性的讀取許可，AWS 應用程式就無法判斷帳戶是啟用或停用。

建立信任時，預設會提供此屬性的讀取存取權。如果您拒絕存取此屬性（不建議），您會讓 Identity Center 之類的應用程式無法讀取信任的使用者。解決方案是特別允許在 AWS 預留 OU（字首為 AWS_）下 AWS 讀取服務帳戶上的 userAccountControl 屬性。

- 建立 AD Connector – AD Connector 是一種目錄閘道，可將目錄請求重新導向至自我管理 AD，而不會快取雲端中的任何資訊。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的[連線至目錄](#)。以下是使用 AD Connector 時的考量事項：
 - 如果您要將 IAM Identity Center 連線至 AD Connector 目錄，任何未來的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 存取入口網站重設密碼。
 - 如果您使用 AD Connector 將 Active Directory Domain Service 連線至 IAM Identity Center，IAM Identity Center 只能存取 AD Connector 連接的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，請將 Directory Service 用於 Microsoft Active Directory。

Note

IAM Identity Center 不適用於SAMBA4-based Simple AD 目錄。

IAM Identity Center 與外部身分提供者目錄之間的屬性映射

屬性映射用於映射 IAM Identity Center 中存在的屬性類型，在您的外部身分來源中具有類似的屬性，例如 Google Workspace、Microsoft Active Directory (AD) 和 Okta。IAM Identity Center 會從您的身分來源擷取使用者屬性，並將其映射至 IAM Identity Center 使用者屬性。

如果您的 IAM Identity Center 已同步使用外部身分提供者 (IdP) Okta，例如 Google Workspace、或 Ping 做為身分來源，您將需要在 IdP 中映射屬性。

IAM Identity Center 會在其組態頁面上的屬性映射索引標籤下為您預先填入一組屬性。IAM Identity Center 使用這些使用者屬性來填入傳送至應用程式的 SAML 聲明（做為 SAML 屬性）。這些使用者屬性會接著從您的身分來源擷取。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。如需詳細資訊，請參閱[將應用程式中的屬性映射至 IAM Identity Center 屬性](#)。

如果您使用 Active Directory 做為身分來源，IAM Identity Center 也會在 Active Directory 組態頁面的屬性映射區段下為您管理一組屬性。如需詳細資訊，請參閱[在 IAM Identity Center 和 Microsoft AD 目錄之間映射使用者屬性](#)。

支援的外部身分提供者屬性

下表列出支援的所有外部身分提供者 (IdP) 屬性，並可映射至您可以在 IAM Identity Center [存取控制的屬性](#)中設定時使用的屬性。使用 SAML 聲明時，您可以使用 IdP 支援的任何屬性。

IdP 中支援的屬性

```
${path:userName}
```

```
${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}
```

IdP 中支援的屬性

`${path:userType}``${path:title}``${path:locale}``${path:timezone}``${path:enterprise.employeeNumber}``${path:enterprise.costCenter}``${path:enterprise.organization}``${path:enterprise.division}``${path:enterprise.department}``${path:enterprise.manager.value}`

IAM Identity Center 與 之間的預設映射 Microsoft AD

下表列出 IAM Identity Center 中使用者屬性與Microsoft AD目錄中使用者屬性的預設映射。IAM Identity Center 僅支援 IAM Identity Center 中使用者屬性欄中的屬性清單。

IAM Identity Center 中的使用者屬性	映射至 Active Directory 中的此屬性
displayname	<code>\${displayname}</code>
emails[?primary].value *	<code>\${mail}</code>
externalid	<code>\${objectguid}</code>
name.givenname	<code>\${givenname}</code>
name.familyname	<code>\${sn}</code>
name.middlename	<code>\${initials}</code>

IAM Identity Center 中的使用者屬性	映射至 Active Directory 中的此屬性
sid	<code>\${objectsid}</code>
username	<code>\${userprincipalname}</code>

* IAM Identity Center 中的電子郵件屬性在目錄中必須是唯一的。

IAM Identity Center 中的群組屬性	映射至 Active Directory 中的此屬性
externalid	<code>\${objectguid}</code>
description	<code>\${description}</code>
displayname	<code>\${samaccountname}@{associateddomain}</code>

考量事項

- 啟用可設定的 AD 同步時，如果您在 IAM Identity Center 中沒有任何使用者和群組的指派，則會使用先前資料表中的預設映射。如需如何自訂這些映射的資訊，請參閱 [為您的同步設定屬性映射](#)。
- 某些 IAM Identity Center 屬性無法修改，因為它們是不可變的，預設會映射到特定的 Microsoft AD 目錄屬性。

例如，「username」是 IAM Identity Center 中的必要屬性。如果您將 "username" 對應至具有空值的 AD 目錄屬性，IAM Identity Center 會將該 windowsUpn 值視為 "username" 的預設值。如果您想要從目前的映射中變更 "username" 的屬性映射，請確認對 "username" 具有相依性的 IAM Identity Center 流程將繼續如預期運作，然後再進行變更。

IAM Identity Center 支援的 Microsoft AD 屬性

下表列出支援且可映射至 IAM Identity Center 中使用者屬性的所有 Microsoft AD 目錄屬性。

Microsoft AD 目錄中受支援的屬性
<code>\${samaccountname}</code>

Microsoft AD 目錄中受支援的屬性

`${description}`

`${objectguid}`

`${objectsid}`

`${givenname}`

`${sn}`

`${initials}`

`${mail}`

`${userprincipalname}`

`${displayname}`

`${distinguishedname}`

`${proxyaddresses[?type == "SMTP"].value}`

`${proxyaddresses[?type == "smtp"].value}`

`${useraccountcontrol}`

`${associateddomain}`

考量事項

- 您可以指定支援的Microsoft AD目錄屬性的任意組合，以映射到 IAM Identity Center 中的單一可變屬性。

支援的 IAM Identity Center 屬性 Microsoft AD

下表列出支援且可映射至Microsoft AD目錄中使用使用者屬性的所有 IAM Identity Center 屬性。設定應用程式屬性映射後，您可以使用這些相同的 IAM Identity Center 屬性來映射至該應用程式使用的實際屬性。

IAM Identity Center for Active Directory 中支援的屬性

`${user:AD_GUID}`

`${user:AD_SID}`

`${user:email}`

`${user:familyName}`

`${user:givenName}`

`${user:middleName}`

`${user:name}`

`${user:preferredUsername}`

`${user:subject}`

在 IAM Identity Center 和 Microsoft AD 目錄之間映射使用者屬性

您可以使用下列程序來指定 IAM Identity Center 中的使用者屬性應如何對應至 Microsoft AD 目錄中的對應屬性。

將 IAM Identity Center 中的屬性映射至目錄中的屬性

1. 開啟 [IAM Identity Center 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. 在存取控制的管理屬性頁面上，尋找您要映射的 IAM Identity Center 屬性，然後在文字方塊中輸入值。例如，您可能想要將 IAM Identity Center 使用者屬性映射 **email** 至 Microsoft AD 目錄屬性 **`${mail}`**。
5. 選擇儲存變更。

IAM Identity Center 可設定的 AD 同步

IAM Identity Center 可設定的 Active Directory (AD) 同步可讓您在 Microsoft Active Directory 中明確設定會自動同步至 IAM Identity Center 的身分，並控制同步程序。

- 使用此同步方法，您可以執行下列動作：
 - 透過明確定義 Microsoft Active Directory 中自動同步至 IAM Identity Center 的使用者和群組來控制資料邊界。您可以隨時[新增使用者和群組](#)，或[移除使用者和群組](#)以變更同步的範圍。
 - 指派同步使用者和群組對應用程式的單一登入[存取 AWS 帳戶](#)或[存取](#)。應用程式可以是 AWS 受管應用程式或客戶受管應用程式。
 - 視需要[暫停並繼續同步，以控制同步](#)程序。這可協助您調節生產系統的負載。

先決條件和考量事項

在使用可設定的 AD 同步之前，請注意下列先決條件和考量事項：

- 在 Active Directory 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，然後將新使用者和群組的存取權指派給 AWS 帳戶 AWS 受管應用程式或客戶受管應用程式，然後同步到 IAM Identity Center。

- 可設定的 AD 同步 – IAM Identity Center 不會直接搜尋您的網域控制器中的使用者和群組。反之，您必須先指定要同步的使用者和群組清單。您可以採用下列其中一種方式來設定此清單，也稱為同步範圍，取決於您是否擁有已同步至 IAM Identity Center 的使用者和群組，或是您第一次使用可設定的 AD 同步來同步的新使用者和群組。
 - 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，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。若要指派新的使用者或群組，您必須將他們特別新增至同步範圍。如需詳細資訊，請參閱[將使用者和群組新增至您的同步範圍](#)。
 - 新使用者和群組：如果您想要將新使用者和群組的存取權指派給 AWS 帳戶 應用程式，您必須先在可設定的 AD 同步中指定要新增至同步範圍的使用者和群組，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您的同步範圍](#)。

- 在 Active Directory 中對巢狀群組進行指派

屬於其他群組成員的群組稱為巢狀群組（或子群組）。

- 可設定的 AD 同步 – 使用可設定的 AD 同步對 Active Directory 中包含巢狀群組的群組進行指派，可能會增加有權存取 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，群組 B 的成員也會繼承此存取權。

- 更新自動化工作流程

如果您有使用 IAM Identity Center 身分存放區 API 動作和 IAM Identity Center 指派 API 動作的自動化工作流程，將新使用者和群組的存取權指派給帳戶和應用程式，並將它們同步到 IAM Identity Center，則必須在 2022 年 4 月 15 日之前調整這些工作流程，以便它們以可設定的 AD 同步如預期般運作。可設定的 AD 同步會變更使用者和群組指派和佈建的順序，以及執行查詢的方式。

- 可設定的 AD 同步 – 佈建會先發生，而且不會自動執行。相反地，您必須先將使用者和群組新增至同步範圍，以明確地將其新增至身分存放區。如需自動化可設定 AD 同步之同步組態的建議步驟相關資訊，請參閱 [自動化可設定 AD 同步的同步組態](#)。

主題

- [可設定的 AD 同步如何運作](#)
- [為您的同步設定屬性映射](#)
- [第一次 Active Directory 到 IAM Identity Center 同步設定](#)
- [將使用者和群組新增至您的同步範圍](#)
- [從您的同步範圍移除使用者和群組](#)
- [暫停並繼續同步](#)
- [自動化可設定 AD 同步的同步組態](#)

可設定的 AD 同步如何運作

IAM Identity Center 使用以下程序重新整理身分存放區中的 AD 型身分資料。若要進一步了解先決條件，請參閱 [先決條件和考量事項](#)。

建立

將 Active Directory 中的自我管理目錄或 AWS Managed Microsoft AD 管理的目錄連接到 IAM Identity Center Directory Service 之後，您可以明確設定要同步到 IAM Identity Center 身分存放區的 Active Directory 使用者和群組。您選擇的身分將每三小時同步到 IAM Identity Center 身分存放區。根據您的目錄大小，同步程序可能需要更長的時間。

屬於其他群組（稱為巢狀群組或子群組）的群組也會寫入身分存放區。

您只能在新使用者或群組同步到 IAM Identity Center 身分存放區之後，將存取權指派給新使用者或群組。

更新

IAM Identity Center 身分存放區中的身分資料會定期從 Active Directory 中的來源目錄中讀取資料，以保持最新狀態。根據預設，IAM Identity Center 會在同步週期中每小時從您的 Active Directory 同步資料。根據 Active Directory 的大小，資料可能需要 30 分鐘到 2 小時才能同步到 IAM Identity Center。

在同步範圍內的使用者和群組物件及其成員資格會在 IAM Identity Center 中建立或更新，以對應至 Active Directory 中來源目錄中的對應物件。對於使用者屬性，IAM Identity Center 主控台的存取控制屬性區段中列出的屬性子集只會在 IAM Identity Center 中更新。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 Identity Center 中。

您也可以更新同步到 IAM Identity Center 身分存放區中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。您新增的任何身分都會在下一次排定的同步時同步。您從子集移除的身分將停止在 IAM Identity Center 身分存放區中更新。任何未同步超過 28 天的使用者都會在 IAM Identity Center 身分存放區中停用。在下一個同步週期中，IAM Identity Center 身分存放區中會自動停用對應的使用者物件，除非它們仍屬於同步範圍的其他群組。

刪除

從 Active Directory 的來源目錄中刪除對應的使用者或群組物件時，會從 IAM Identity Center 身分存放區刪除使用者和群組。或者，您可以使用 IAM Identity Center 主控台，從 IAM Identity Center 身分存放區明確刪除使用者物件。如果您使用 IAM Identity Center 主控台，您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 Identity Center。

您也可以隨時暫停和重新啟動同步。如果您暫停同步超過 28 天，則會停用所有使用者。

為您的同步設定屬性映射

如需可用屬性的詳細資訊，請參閱 [IAM Identity Center 與外部身分提供者目錄之間的屬性映射](#)。

在 IAM Identity Center 中設定屬性映射至您的目錄

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，選擇動作，然後選擇管理同步。
4. 在管理同步下，選擇檢視屬性映射。
5. 在 Active Directory 使用者屬性下，設定 IAM Identity Center 身分存放區屬性和 Active Directory 使用者屬性。例如，您可能想要將 IAM Identity Center 身分存放區屬性映射 email 至 Active Directory 使用者目錄屬性 `${objectguid}`。

Note

在群組屬性下，無法變更 IAM Identity Center 身分存放區屬性和 Active Directory 群組屬性。

6. 選擇儲存變更。這會讓您返回管理同步頁面。

第一次 Active Directory 到 IAM Identity Center 同步設定

如果您是第一次將使用者和群組從 Active Directory 同步到 IAM Identity Center，請遵循下列步驟。或者，您可以遵循中所述的步驟[變更您的身分來源](#)，將身分來源從 IAM Identity Center 變更為 Active Directory。

引導式設定

1. 開啟 [IAM Identity Center 主控台](#)。

Note

在移至下一個步驟之前，請確定 IAM Identity Center 主控台使用 AWS 區域 AWS Managed Microsoft AD 目錄所在的其中一個。

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：設定屬性映射中，檢閱預設使用者和群組屬性映射。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。接著，選擇群組索引標籤。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。如果您想要稍後將使用者和群組新增至同步範圍，請不要進行任何變更，然後選擇下一步。
6. 在步驟 3：檢閱並儲存組態中，確認步驟 1：屬性映射中的屬性映射，以及步驟 2：同步範圍中的使用者和群組。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您的同步範圍

Note

將群組新增至同步範圍時，請直接從信任的內部部署網域同步群組，而不是從 AWS Managed Microsoft AD 網域中的群組同步群組。直接從信任網域同步的群組包含 IAM Identity Center 可以成功存取和同步的實際使用者物件。

請依照下列步驟，將 Active Directory 使用者和群組新增至 IAM Identity Center。

新增使用者

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，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，然後選擇新增。
6. 在新增的使用者和群組下，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。如果您指定的使用者未顯示在清單中，請選擇重新整理圖示以更新使用者清單。

新增群組

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，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，然後選擇新增。
6. 在新增的使用者和群組下，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)。如果您指定的群組未顯示在清單中，請選擇重新整理圖示以更新群組清單。

從您的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所發生情況的詳細資訊，請參閱 [可設定的 AD 同步如何運作](#)。

移除使用者

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，選擇動作，然後選擇管理同步。
4. 選擇使用者索引標籤。
5. 在同步範圍內的使用者下，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的核取方塊。
6. 選擇移除。

移除群組

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，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未來的同步週期，並防止您在 Active Directory 中對使用者和群組所做的任何變更反映在 IAM Identity Center 中。在您繼續同步後，同步週期會從下一次排定的同步中取得這些變更。

暫停同步

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，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。

恢復同步

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，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不是繼續同步，則從 Active Directory 到 IAM Identity Center 的同步已恢復。

自動化可設定 AD 同步的同步組態

為了確保自動化工作流程可如預期使用可設定的 AD 同步，建議您執行下列步驟來自動化同步組態。

若要自動化可設定 AD 同步的同步組態

1. 在 Active Directory 中，建立父同步群組，以包含您要同步至 IAM Identity Center 的所有使用者和群組。例如，您可以命名群組 IAMIdentityCenterAllUsersAndGroups。
2. 在 IAM Identity Center 中，將父同步群組新增至可設定的同步清單。IAM Identity Center 將同步父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，從父同步群組新增或移除使用者和群組。

在 Identity Center 目錄中管理使用者

IAM Identity Center 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 Identity Center 存放區中的使用者和群組，AWS 支援 [Identity Center Actions](#) 中列出的 API 操作。

使用者位於 IAM Identity Center 時的佈建

當您直接在 IAM Identity Center 中建立使用者和群組時，會自動佈建。這些身分可立即用於進行指派和供應應用程式使用。如需詳細資訊，請參閱[使用者和群組佈建](#)。

變更您的身分來源

如果您想要在 中管理使用者 AWS Managed Microsoft AD，您可以隨時停止使用 Identity Center 目錄，並使用 將 IAM Identity Center 連接到 Microsoft AD 中的目錄 Directory Service。如需詳細資訊，請參閱 的考量事項[在 IAM Identity Center 目錄和 Active Directory 之間變更](#)。

如果您偏好管理外部身分提供者 (IdP) 中的使用者，您可以將 IAM Identity Center 連線至 IdP，並啟用自動佈建。如需詳細資訊，請參閱 的考量事項[從 IAM Identity Center 變更為外部 IdP](#)。

主題

- [將使用者新增至 Identity Center 目錄](#)
- [將群組新增至 Identity Center 目錄](#)
- [將使用者新增至群組](#)
- [在 IAM Identity Center 中刪除群組](#)
- [在 IAM Identity Center 中刪除使用者](#)
- [從群組中移除使用者](#)
- [編輯 Identity Center 目錄使用者屬性](#)

將使用者新增至 Identity Center 目錄

您在 Identity Center 目錄中建立的使用者和群組只能在 IAM Identity Center 中使用。使用下列程序將使用者新增至 Identity Center 目錄。或者，您可以呼叫 AWS API 操作[CreateUser](#)來新增使用者。

Console

若要新增使用者

1. 開啟 [IAM Identity Center 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 – 登入 AWS 存取入口網站時需要此使用者名稱，之後無法變更。長度必須介於 1 與 100 個字元之間。
- b. 密碼 – 您可以使用密碼設定指示（這是預設選項）傳送電子郵件，或產生一次性密碼。如果您正在建立管理使用者，並選擇傳送電子郵件，請確定您指定您可以存取的電子郵件地址。
 - i. 使用密碼設定指示傳送電子郵件給此使用者 – 此選項會自動將來自 Amazon Web Services 的電子郵件傳送給使用者，主旨行邀請加入 AWS IAM Identity Center。電子郵件會代表您的公司邀請使用者存取 IAM Identity Center AWS 存取入口網站，並註冊密碼。電子郵件邀請將在七天後過期。如果發生這種情況，您可以選擇重設密碼，然後選擇傳送電子郵件給使用者，其中包含重設密碼的說明。在使用者接受邀請之前，您會看到傳送電子郵件驗證連結，這是用來驗證其電子郵件地址。不過，此步驟是選用的，會在使用者接受邀請並註冊密碼後消失。

 Note

在某些區域中，IAM Identity Center 會從另一個使用 Amazon Simple Email Service 傳送電子郵件給使用者 AWS 區域。如需電子郵件傳送方式的相關資訊，請參閱 [使用 Amazon SES 的跨區域電子郵件](#)。

IAM Identity Center 服務傳送的所有電子郵件都將來自地址 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，而不會將其視為垃圾郵件或垃圾郵件處理。

- ii. 產生您可以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。使用者將需要驗證其電子郵件地址。您可以選擇傳送電子郵件驗證連結來啟動程序。電子郵件驗證連結將在七天後過期。如果發生這種情況，您可以選擇重設密碼來重新傳送電子郵件驗證連結，然後選擇產生一次性密碼並與使用者共用密碼。
- c. 電子郵件地址 – 電子郵件地址必須是唯一的。
- d. 確認電子郵件地址
- e. 名字 – 您必須在這裡輸入名稱，自動佈建才能運作。如需詳細資訊，請參閱 [使用 SCIM 從外部身分提供者佈建使用者和群組](#)。
- f. 姓氏 – 您必須在這裡輸入名稱，自動佈建才能運作。
- g. 顯示名稱

Note

(選用) 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，以協助為使用者提供特定商業應用程式的單一登入存取權。

4. 選擇下一步。
5. 如果適用，請選取您要新增使用者的一或多個群組，然後選擇下一步。
6. 檢閱您在步驟 1：指定使用者詳細資訊和步驟 2：將使用者新增至群組中指定的資訊 - 選用。選擇依任一步驟編輯，以進行任何變更。確認兩個步驟都指定正確的資訊後，請選擇新增使用者。

AWS CLI

若要新增使用者

下列 `create-user` 命令會在 Identity Center 目錄中建立新的使用者。

```
aws identitystore create-user \  
  --identity-store-id d-1234567890 \  
  --user-name johndoe \  
  --name "GivenName=John,FamilyName=Doe" \  
  --display-name "John Doe" \  
  --emails "Type=work,Value=johndoe@example.com"
```

輸出：

```
{  
  "UserId": "1234567890-abcdef",  
  "IdentityStoreId": "d-1234567890"  
}
```

Note

當您使用 CLI `create-user` 命令或 [CreateUser](#) API 操作建立使用者時，使用者沒有密碼。您可以更新 IAM Identity Center 中的設定，在使用者第一次嘗試登入後傳送驗證電子郵件給這些使用者，讓他們可以設定密碼。如果您未啟用此設定，則必須產生一次性密碼。

並與使用者共用。如需詳細資訊，請參閱[透過電子郵件將一次性密碼傳送給使用 API 或 CLI 建立的使用者](#)。

將群組新增至 Identity Center 目錄

使用下列程序將群組新增至 Identity Center 目錄。或者，您可以呼叫 AWS API 操作[CreateGroup](#)來新增群組。

Console

新增群組

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Groups (群組)。
3. 選擇建立群組。
4. 輸入群組名稱和描述 - 選用。描述應提供有關已指派給或將指派給群組之許可的詳細資訊。在新增使用者至群組 - 選用下，尋找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. 選擇建立群組。

AWS CLI

新增群組

下列create-group命令會在 Identity Center 目錄中建立新的群組。

```
aws identitystore create-group \  
  --identity-store-id d-1234567890 \  
  --display-name "Developers" \  
  --description "Group that contains all developers"
```

輸出：

```
{  
  "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",  
  "IdentityStoreId": "d-1234567890"  
}
```

將此群組新增至 Identity Center 目錄後，您可以將單一登入存取權指派給群組。如需詳細資訊，請參閱[將使用者或群組存取權指派給 AWS 帳戶](#)。

將使用者新增至群組

使用下列程序，將使用者新增為您先前在 Identity Center 目錄中建立之群組的成員。或者，您可以呼叫 AWS API 操作[CreateGroupMembership](#)，將使用者新增為群組的成員。

Console

新增使用者做為群組的成員

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Groups (群組)。
3. 選擇您要更新的群組名稱。
4. 在群組詳細資訊頁面的此群組中的使用者下，選擇新增使用者至群組。
5. 在新增使用者至群組頁面的其他使用者下，找到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)。

AWS CLI

新增使用者做為群組的成員

下列create-group-membership命令會將使用者新增至 Identity Center 目錄中的群組。

```
aws identitystore create-group-membership \
  --identity-store-id d-1234567890 \
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
  --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

輸出：

```
{
  "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
  "IdentityStoreId": "d-1234567890"
}
```

在 IAM Identity Center 中刪除群組

當您刪除 IAM Identity Center 目錄中的群組時，它會移除此群組成員之所有使用者的 AWS 帳戶 和 應用程式存取權。刪除群組之後，就無法復原。使用下列程序刪除 Identity Center 目錄中的群組。

Important

本頁面上的指示適用於 [AWS IAM Identity Center](#)。它們不適用於 [AWS Identity and Access Management \(IAM\)](#)。IAM Identity Center 使用者、群組和使用憑證與 IAM 使用者、群組和 IAM 使用者憑證不同。如果您要尋找在 IAM 中刪除群組的指示，請參閱 [《使用者指南》中的刪除 IAM 使用者群組](#)。AWS Identity and Access Management

Console

刪除群組

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Groups (群組)。
3. 有兩種方法可以刪除群組：
 - 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. 您可能需要確認刪除群組的意圖。
 - 如果您一次刪除多個群組，**Delete**請在刪除群組對話方塊中輸入 來確認您的意圖。
 - 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，以確認您的意圖。
5. 選擇 Delete group (刪除群組)。如果您選取多個群組進行刪除，請選擇刪除 # 群組。

AWS CLI

刪除群組

下列delete-group命令會從 Identity Center 目錄中刪除指定的群組。

```
aws identitystore delete-group \
```

```
--identity-store-id d-1234567890 \  
--group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

在 IAM Identity Center 中刪除使用者

當您刪除 IAM Identity Center 目錄中的使用者時，它會移除其對 AWS 帳戶 和 應用程式的存取權。刪除使用者後，您無法復原此動作。使用下列程序刪除 Identity Center 目錄中的使用者。

Note

當您在 IAM Identity Center 中停用使用者存取或刪除使用者時，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[了解 IAM Identity Center 中的身分驗證工作階段](#)。

Important

本頁面上的指示適用於 [AWS IAM Identity Center](#)。它們不適用於 [AWS Identity and Access Management \(IAM\)](#)。IAM Identity Center 使用者、群組和使用者憑證與 IAM 使用者、群組和 IAM 使用者憑證不同。如果您要尋找在 IAM 中刪除使用者的指示，請參閱《[使用者指南](#)》中的[刪除 IAM 使用者](#)。AWS Identity and Access Management

Console

若要刪除使用者

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Users (使用者)。
3. 有兩種方式可以刪除使用者：
 - 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。
 - 選擇您要刪除的使用者名稱。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，**Delete**請在刪除使用者對話方塊中輸入 來確認您的意圖。
5. 選擇刪除使用者。如果您選取多個使用者進行刪除，請選擇刪除 # 個使用者。

AWS CLI

若要刪除使用者

下列delete-user命令會從 Identity Center 目錄中刪除使用者。

```
aws identitystore delete-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

從群組中移除使用者

使用下列程序從群組中移除成員。或者，您可以呼叫 AWS API 操作[DeleteGroupMembership](#)，從群組中移除使用者。

Console

從群組移除使用者

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Groups (群組)。
3. 選擇您要更新的群組。
4. 在群組詳細資訊頁面的此群組中的使用者下，選擇要移除的使用者。
5. 選擇從群組中移除使用者。
6. 在移除使用者對話方塊中，選擇從群組中移除使用者，以確認您想要移除使用者對指派給群組的帳戶和應用程式的存取權。

AWS CLI

從群組移除使用者

下列delete-group-membership命令會從群組中移除成員資格。

```
aws identitystore delete-group-membership  
  --identity-store-id d-1234567890 \  
  --membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```


編輯 Identity Center 目錄使用者屬性

使用下列程序來編輯 Identity Center 目錄中使用者的屬性。或者，您可以呼叫 AWS API 操作 [UpdateUser](#) 來更新使用者屬性。

Console

在 IAM Identity Center 中編輯使用者屬性

1. 開啟 [IAM Identity Center 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訊旁，選擇編輯。
5. 在編輯設定檔詳細資訊頁面上，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 Immutable ID，以協助將 IAM Identity Center 中的使用者身分映射到使用者需要使用的特定商業應用程式。

Note

電子郵件地址屬性是可編輯的欄位，您提供的值必須是唯一的。

AWS CLI

在 IAM Identity Center 中編輯使用者屬性

下列 update-user 命令會更新使用者的暱稱。

```
aws identitystore update-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
  --operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

設定人力資源存取 AWS 資源

設定您的人力資源使用者如何透過 IAM Identity Center 驗證和存取 AWS 資源。本節涵蓋下列管理人力資源使用者存取您 AWS 環境的元件：

- 身分驗證工作階段 – 了解 IAM Identity Center 如何管理不同類型的使用者工作階段，從互動式入口網站工作階段到背景應用程式工作階段，以及它們如何彼此互動。
- 使用者存取管理 – 設定工作階段持續時間、停用使用者帳戶，以及實作整個組織的存取區塊，以維護安全性和合規性。
- 密碼管理 – 對於在 Identity Center 目錄中建立的使用者，請設定密碼需求、處理使用者登入資料設定，以及管理使用者的密碼重設。
- 多重要素驗證 – 對於在 Identity Center 目錄中建立的使用者，請使用驗證器應用程式、安全金鑰或內建驗證器來增強 MFA 的安全性，以保護使用者登入。

主題

- [了解 IAM Identity Center 中的身分驗證工作階段](#)
- [在 IAM Identity Center 中設定工作階段持續時間](#)
- [在 IAM Identity Center 中停用使用者對 AWS 帳戶和應用程式的存取](#)
- [使用服務控制政策拒絕使用者存取](#)
- [管理 Identity Center 目錄中使用者的存取權](#)

了解 IAM Identity Center 中的身分驗證工作階段

當使用者登入[AWS 存取入口網站](#)時，IAM Identity Center 會建立代表使用者已驗證身分的身分驗證工作階段。

通過身分驗證後，使用者可以存取管理員授予他們使用許可的所有已指派 AWS 帳戶、[AWS 受管應用程式](#)和[客戶受管應用程式](#)，而無需額外的登入。

身分驗證工作階段的類型

使用者互動式工作階段

使用者登入 AWS 存取入口網站後，IAM Identity Center 會建立使用者互動式工作階段。此工作階段代表使用者在 IAM Identity Center 中的已驗證狀態，並做為建立其他工作階段類型的基礎。使用者互動式工作階段可持續 IAM Identity Center 中設定的持續時間，最長可達 90 天。

使用者互動式工作階段是主要身分驗證機制。它們會在使用者登出或管理員結束其工作階段時結束。這些工作階段的持續時間應根據組織的安全需求仔細設定。

如需設定使用者互動式工作階段持續時間的資訊，請參閱 [the section called “設定工作階段持續時間”](#)。

應用程式工作階段

應用程式工作階段是 IAM Identity Center 透過單一登入建立的使用者與 AWS 受管應用程式（例如 Kiro 或 Amazon Quick）之間的驗證連線。

根據預設，應用程式工作階段有一小時的生命週期，但只要基礎使用者互動式工作階段仍然有效，系統就會自動重新整理這些工作階段。此重新整理機制可為使用者提供無縫體驗，同時維護安全控制。當使用者互動式工作階段結束時，無論是透過使用者登出或管理員動作，應用程式工作階段都會在下一次重新整理嘗試時結束，通常在 30 分鐘內結束。

使用者背景工作階段

使用者背景工作階段是延長持續時間工作階段，專為需要執执行程序數小時或數天而不會中斷的應用程式而設計。目前，此工作階段類型主要適用於 [Amazon SageMaker Studio](#)，其中資料科學家可能會執行需要數小時才能完成的機器學習訓練任務。

如需設定使用者背景工作階段持續時間的資訊，請參閱[使用者背景工作階段](#)。

Kiro 工作階段

您可以擴展 Kiro 工作階段，以允許開發人員在 IDEs 中使用 Kiro 來維持身分驗證長達 90 天。當您處理程式碼時，此功能可減少登入中斷。

這些工作階段獨立於其他工作階段類型，不會影響使用者互動式工作階段或其他 AWS 受管應用程式。視您啟用 IAM Identity Center 的時間而定，此功能預設可能會啟用。

如需設定擴充 Kiro 工作階段的詳細資訊，請參閱 [???](#)。

IAM Identity Center 建立的 IAM 角色工作階段

當使用者存取 AWS 管理主控台 或 時，IAM Identity Center 會建立不同類型的工作階段 AWS CLI。在這些情況下，IAM Identity Center 會使用登入工作階段，透過擔任使用者許可集中指定的 IAM 角色來取得 IAM 工作階段。

Important

與應用程式工作階段不同，IAM 角色工作階段會在建立後獨立運作。無論原始登入工作階段的狀態為何，它們會保留在許可集中設定的持續時間，最長可達 12 小時。此行為可確保長時間執行的 CLI 操作或主控台工作階段不會意外結束。

IAM Identity Center 中最終使用者工作階段的方法

使用者啟動

當使用者登出 AWS 存取入口網站時，登入工作階段會結束，讓使用者無法存取任何新資源。

不過，現有的應用程式工作階段不會立即結束。相反地，當他們嘗試下一次重新整理並發現登入工作階段不再有效時，他們會在大約 30 分鐘內結束。現有的 IAM 角色工作階段會繼續，直到根據許可集組態過期為止，最長可能在 12 小時後。

管理員啟動

組織中具有 IAM Identity Center 管理許可的任何人，通常是 IT 管理員或安全團隊，都可以[結束使用者](#)的工作階段。此動作的運作方式與使用者自行登出的方式相同，可讓管理員在需要時要求使用者再次登入。當安全政策變更或偵測到可疑活動時，此功能很有用。

當 IAM Identity Center 管理員[刪除使用者](#)或[停用使用者的存取權](#)時，使用者將失去 AWS 存取入口網站的存取權，且無法重新登入以啟動新的應用程式或 IAM 角色工作階段。使用者將在 30 分鐘內失去對現有應用程式工作階段的存取權。任何現有的 IAM 角色工作階段都會根據 IAM Identity Center 許可集中設定的工作階段持續時間繼續。工作階段持續時間上限為 12 小時。

當您結束工作階段時，使用者存取會發生什麼情況

此參考提供 IAM Identity Center 工作階段在採取管理動作時如何運作的詳細資訊。本節中的表格顯示使用者管理動作的持續時間和效果，以及存取 AWS 入口網站、應用程式和 AWS 帳戶 工作階段的許可變更。

使用者管理

此表格摘要說明使用者管理變更如何影響對 AWS 資源、應用程式工作階段和 AWS 帳戶工作階段的存取。

Action	使用者失去 IAM Identity Center 存取權	使用者無法建立新的應用程式工作階段	使用者無法存取現有的應用程式工作階段	使用者失去對現有 AWS 帳戶工作階段的存取權
使用者存取已停用	立即生效	立即生效	30 分鐘內	12 小時內。持續時間取決於為許可集設定的 IAM 角色工作階段到期持續時間。
使用者已刪除	立即生效	立即生效	30 分鐘內	12 小時內。持續時間取決於為許可集設定的 IAM 角色工作階段到期持續時間。
使用者工作階段已撤銷	使用者必須再次登入才能重新取得存取權	立即生效	30 分鐘內	12 小時內。持續時間取決於為許可集設定的 IAM 角色工作階段到期持續時間。
使用者登出	使用者必須再次登入才能重新取得存取權	立即生效	30 分鐘內	12 小時內。持續時間取決於為許可集設定的 IAM 角色工作階段到期持續時間。

群組成員資格

此資料表摘要說明使用者許可和群組成員資格的變更如何影響對 AWS 資源、應用程式工作階段和 AWS 帳戶工作階段的存取。

Action	使用者失去 IAM Identity Center 存取權	使用者無法建立新的應用程式工作階段	使用者無法存取現有的應用程式工作階段	使用者失去對現有 AWS 帳戶工作階段的存取權
從使用者移除的應用程式或 AWS 帳戶 存取權	否 - 使用者可以繼續存取 IAM Identity Center	立即生效	1 小時內	12 小時內。持續時間取決於為許可集設定的 IAM 角色工作階段到期持續時間。
從已指派應用程式或的群組中移除使用者 AWS 帳戶	否 - 使用者可以繼續存取 IAM Identity Center	1 小時內	2 小時內	12 小時內。持續時間取決於為許可集設定的 IAM 角色工作階段到期持續時間。
從群組移除的應用程式或 AWS 帳戶 存取權	否 - 使用者可以繼續存取 IAM Identity Center	立即生效	1 小時內	12 小時內。持續時間取決於為許可集設定的 IAM 角色工作階段到期持續時間。

Note

AWS 存取入口網站 和 AWS CLI 會在您從該群組新增或移除使用者後 1 小時內反映更新的使用者許可。

了解計時差異

- 立即生效 – 需要立即重新驗證的動作。
- 在 30 分鐘到 2 小時內 – 應用程式工作階段需要時間與 IAM Identity Center 檢查並探索任何變更。
- 在 12 小時內 – IAM 角色工作階段會獨立運作，且只會在其設定的持續時間過期時結束。

單一登出

IAM Identity Center 不支援由做為[您的身分來源](#)的身分提供者啟動的 SAML 單一登出（當使用者登出時自動登出所有連線應用程式的通訊協定）。此外，它不會將 SAML 單一登出傳送至使用 IAM Identity Center 做為身分提供者的 [SAML 2.0 應用程式](#)。

工作階段管理的最佳實務

有效的工作階段管理需要深思熟慮的組態和監控。組織應設定適合其安全需求的工作階段持續時間，通常針對敏感應用程式和環境使用較短的持續時間。

當使用者變更角色或離開組織時，實作程序以結束工作階段對於維護安全界限至關重要。應將作用中工作階段的定期審查納入安全監控實務中，以偵測可能表示安全問題的異常行為，例如異常存取模式、非預期的登入時間或位置，或存取正常工作職能以外的資源。

在 IAM Identity Center 中設定工作階段持續時間

您可以在員工使用者使用與 IAM Identity Center 搭配使用的 AWS 存取入口網站 和 應用程式時，為他們設定工作階段持續時間，包括 Kiro。IAM Identity Center 提供下列工作階段類型：使用者互動式工作階段、使用者背景工作階段，以及 Kiro 的延伸工作階段。

主題

- [使用者互動式工作階段](#)
- [使用者背景工作階段](#)
- [Kiro 的延伸工作階段](#)
- [檢視和結束人力使用者的作用中工作階段](#)
- [使用身分來源、CLI 和 SDK AWS 的工作階段持續時間考量 AWS SDKs](#)

使用者互動式工作階段

使用者互動式工作階段是與使用者登入 AWS 存取入口網站或受[AWS 管應用程式](#)的存取相關聯的工作階段。和 AWS 存取入口網站 應用程式的工作階段身分驗證持續時間是使用者無需重新身分驗證即可登入的時間上限。如果您結束作用中的 AWS 存取入口網站工作階段，這也會結束這些受管應用程式的任何工作階段。

使用者互動式工作階段的預設工作階段持續時間為 8 小時。您可以指定不同的持續時間，從最短 15 分鐘到最長 90 天。自訂持續時間值必須以分鐘為單位輸入，且介於 15 分鐘到 129,600 分鐘 (90 天) 之間。如需詳細資訊，請參閱[了解 IAM Identity Center 中的身分驗證工作階段](#)。

如需 IAM Identity Center 身分來源如何影響使用者互動式工作階段持續時間等考量事項，請參閱 [the section called “身分來源、CLI AWS 和 AWS SDKs 考量事項”](#)。

設定使用者互動式工作階段的持續時間

1. 開啟 IAM Identity Center 主控台。
2. 選擇設定。
3. 在設定頁面上，選擇身分驗證索引標籤。
4. 在身分驗證下，工作階段持續時間旁，選擇設定。隨即出現設定工作階段持續時間對話方塊。
5. 在設定工作階段持續時間對話方塊中，在使用者互動式工作階段下，選取下拉式箭頭，為您的使用者選擇工作階段持續時間上限。選擇工作階段的長度，然後選擇儲存。

 Note

工作階段持續時間的變更僅適用於新的工作階段。目前的工作階段會保留其原始持續時間。

6. 您會返回身分驗證索引標籤。標籤上方出現綠色通知訊息，表示工作階段設定已成功更新。

使用者背景工作階段

使用者背景工作階段允許使用者在 [Amazon SageMaker Studio](#) 等 AWS 受管應用程式上啟動長時間執行的任務，而不需要該使用者在任務執行期間保持登入狀態。任務會立即執行，並使用 IAM Identity Center [的信任身分傳播](#) 功能，以確保在背景執行任務時維持使用者的許可。即使使用者關閉電腦、IAM Identity Center 登入工作階段過期，或使用者登出 AWS 存取入口網站，任務仍可繼續執行。此功能可讓資料科學家、機器學習工程師和其他人員開始在背景執行的分析和機器學習工作流程，而無需主動的使用者參與。

預設會針對支援的 AWS 受管應用程式啟用使用者背景工作階段，例如 Amazon SageMaker Studio。不過，若要使用此功能，您必須在建立或更新網域時，在 Amazon SageMaker Studio 中啟用信任的身分傳播。如需詳細資訊，請參閱[在您的 Amazon SageMaker AI 網域中啟用信任的身分傳播](#)。

使用者背景工作階段的預設工作階段持續時間為 7 天。您可以指定不同的持續時間，從最短 15 分鐘到最長 90 天。自訂持續時間值必須以分鐘為單位輸入，且介於 15 分鐘到 129,600 分鐘 (90 天) 之間。

請記住下列使用者背景工作階段的考量事項：

- 只有當使用者在 Amazon SageMaker Studio 中手動啟動任務時，才能建立使用者背景工作階段。自動化的排程工作流程不支援此功能。
- 如需支援使用者背景工作階段 AWS 的區域清單，請參閱[支援 AWS 的區域](#)。
- 您可以在 CloudTrail 中檢視使用者背景工作階段。如需詳細資訊，請參閱[識別使用者背景工作階段詳細資訊](#)。
- 您也可以結束組織中使用者的作用中工作階段。如需詳細資訊，請參閱[結束人力使用者的作用中工作階段](#)。

設定使用者背景工作階段的持續時間

1. 開啟 IAM Identity Center 主控台。
2. 選擇設定。
3. 在設定頁面上，選擇身分驗證索引標籤。
4. 在身分驗證下，工作階段持續時間旁，選擇設定。設定工作階段持續時間對話方塊隨即出現。
5. 在設定工作階段持續時間對話方塊中，如果尚未選取啟用使用者背景工作階段核取方塊，請選取它。清除核取方塊以停用使用者背景工作階段。

 Note

如果您停用使用者背景工作階段，目前工作階段不會受到影響。

6. 在使用者背景工作階段下，選取下拉式箭頭，以選擇工作階段持續時間上限。選擇工作階段的長度，然後選擇儲存。

 Note

工作階段持續時間的變更僅適用於新的工作階段。目前的工作階段會保留其原始持續時間。

7. 您會返回身分驗證索引標籤。標籤上方出現綠色通知訊息，表示工作階段設定已成功更新。

Note

客戶受管應用程式無法建立使用者背景工作階段。

Kiro 的延伸工作階段

如果您的開發人員使用 Kiro 做為整合開發環境 (IDE) 的一部分，您可以將 Kiro 的工作階段持續時間設定為 90 天。視您啟用 IAM Identity Center 的時間而定，預設可能會啟用 Kiro 的延長工作階段持續時間。此延伸工作階段不會影響 AWS 存取入口網站或其他 AWS 受管應用程式的工作階段持續時間。

如需 IAM Identity Center 身分來源如何影響延長工作階段持續時間等考量，請參閱 [the section called “身分來源、CLI AWS 和 AWS SDKs 考量事項”](#)。

Note

Kiro 可從設定為商業 AWS 區域且預設為啟用的主控台存取。如果您的 IAM Identity Center 執行個體位於目前無法存取 Kiro 的區域，則啟用 90 天的延長工作階段持續時間不會覆寫預設設定。這表示無論您是否啟用 90 天的延長工作階段持續時間，工作階段持續時間都不會改變。如需詳細資訊，請參閱 [Kiro 支援的 AWS 區域](#)。

擴展 Kiro 的工作階段

1. 開啟 IAM Identity Center 主控台。
2. 選擇設定。
3. 在設定頁面上，選擇身分驗證索引標籤。
4. 在身分驗證下，工作階段持續時間旁，選擇設定。隨即出現設定工作階段持續時間對話方塊。
5. 在設定工作階段持續時間對話方塊中，選取啟用 Kiro 的延伸工作階段核取方塊。清除核取方塊以停用 Kiro 的延伸工作階段工作階段。
6. 選擇儲存以返回設定頁面。

檢視和結束人力使用者的作用中工作階段

身為 IAM Identity Center 管理員，您可以檢視人力使用者作用中工作階段的清單，並視需要結束使用者的一或多個工作階段。例如，您可能需要在以下情況下結束使用者的工作階段：

- 使用者不再需要工作階段。
- 使用者不應維持其目前的身分驗證狀態。當他們離開公司或其許可變更時，可能會發生這種情況。

您可以使用 IAM Identity Center 主控台來檢視和結束這些工作階段。您的使用者也可以使用 AWS 存取入口網站檢視和結束自己的工作階段。如需有關您的人力資源使用者如何在無需管理員協助的情況下檢視和結束其工作階段的資訊，請參閱 [檢視和結束作用中工作階段](#)。

 Note

結束 IAM Identity Center 使用者的作用中工作階段不會結束 AWS 管理主控台 或 中的任何作用中 IAM 角色工作階段 AWS CLI。如需詳細資訊，請參閱 [了解 IAM Identity Center 中的身分驗證工作階段](#)。

結束人力使用者的作用中工作階段 (IAM Identity Center 主控台)

1. 開啟 IAM Identity Center 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的使用者名稱。這會帶您前往包含使用者資訊的頁面。
4. 在使用者頁面上，選擇作用中工作階段索引標籤。作用中工作階段旁的括號中的數字表示此使用者的作用中工作階段數量。
5. 搜尋使用者背景工作階段 (選用)

若要依使用工作階段之任務的 Amazon Resource Name (ARN) 搜尋工作階段，請在工作階段類型清單中，選擇使用者背景工作階段，然後在搜尋方塊中輸入任務 ARN。

 Note

您只能結束載入的作用中工作階段。如果使用者有許多工作階段，請選擇載入更多作用中工作階段以顯示其他工作階段。

6. 選取您要結束的每個工作階段旁的核取方塊，然後選擇結束工作階段。
7. 隨即出現對話方塊，確認您要結束此使用者的作用中工作階段。檢閱資訊，如果您想要繼續，請輸入 confirm，然後選擇結束工作階段。
8. 您會回到使用者的頁面。會出現綠色通知訊息，指出選取的工作階段已成功結束。

使用身分來源、CLI 和 SDK AWS 的工作階段持續時間考量 AWS SDKs

如果您使用 Microsoft Active Directory (AD) 或外部身分提供者 (IdP) 做為身分來源，或 AWS 軟體開發套件 (SDKs) 或其他 AWS 開發工具以程式設計方式存取 AWS 服務 AWS Command Line Interface，則設定工作階段持續時間的考量如下。

Kiro 的 Microsoft Active Directory、使用者互動式工作階段和延伸工作階段

如果您使用 Microsoft Active Directory (AD) 做為身分來源，並為 Kiro 的使用者互動式工作階段或延伸工作階段設定工作階段持續時間，請謹記下列考量。

Note

這些考量不適用於使用者背景工作階段。

無論您是在 中 使用 AWS Managed Microsoft AD 或 AD Connector AWS Directory Service，在 Microsoft AD 中定義的使用者 Kerberos 票證最長生命週期可能會影響 Kiro 的使用者互動式工作階段和延伸工作階段的有效時間。如需此設定的詳細資訊，請參閱 Microsoft 網站上的[使用者票證生命週期上限](#)。

- **AWS Managed Microsoft AD**：如果您在 中 使用 AWS Managed Microsoft AD 設定 AWS Directory Service，使用者 Kerberos 票證的生命週期上限固定為 10 小時。因此，使用者互動式工作階段持續時間設定為較短的 IAM Identity Center 設定和 10 小時。例如，如果您將使用者互動式工作階段持續時間設定為 12 小時，您的使用者必須在 10 小時後在 AWS 存取入口網站中重新驗證身分。相同的 10 小時限制適用於 Kiro 的延伸工作階段。
- **AD Connector**：如果您使用在 中 設定的 AD Connector AWS Directory Service，使用者 Kerberos 票證的最長生命週期會在 AD Connector 後方的 Microsoft AD 中定義。預設值為 10 小時，且對使用者互動式工作階段和延伸工作階段的影響與 相同 AWS Managed Microsoft AD。雖然此限制可能可在 Microsoft AD 中設定，但我們建議您與 IT 管理員合作考慮風險，尤其是因為此設定可能會影響其他 Microsoft AD 用戶端應用程式的工作階段持續時間。

Kiro 的外部身分提供者、使用者互動式工作階段和延伸工作階段

如果您使用外部身分提供者 (IdP)，並為 Kiro 的使用者互動式工作階段或延伸工作階段設定工作階段持續時間，請謹記下列考量。

Note

這些考量不適用於使用者背景工作階段。

IAM Identity Center 使用來自 SAML 聲明的 `SessionNotOnOrAfter` 屬性，以協助判斷工作階段的有效時間長度。

- 如果 `SessionNotOnOrAfter` 未在 SAML 聲明中傳遞，則 AWS 存取入口網站（使用者互動式）工作階段的持續時間和延伸工作階段不受外部 IdP 工作階段的持續時間影響。例如，如果您的 IdP 工作階段持續時間為 24 小時，而且您在 IAM Identity Center 中設定了 18 小時的工作階段持續時間，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。同樣地，如果您為 Kiro 設定 90 天的延長工作階段，您的 Kiro 使用者需要在 90 天後重新驗證。
- 如果 `SessionNotOnOrAfter` 傳入 SAML 聲明，工作階段持續時間值會設定為較短的 AWS 存取入口網站（使用者互動式）工作階段或延長工作階段持續時間和您的 SAML IdP 工作階段持續時間。如果您在 IAM Identity Center 中設定 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，您的使用者將有權存取 IdP 中定義的 18 小時 AWS 的資源。同樣地，如果您為 Kiro 設定 90 天的延長工作階段，您的 Kiro 使用者需要在 18 小時後在 Kiro 中重新驗證身分。
- 如果 IdP 的工作階段持續時間超過 IAM Identity Center 中設定的工作階段持續時間，您的使用者可以啟動新的 IAM Identity Center 工作階段，而無需根據其使用 IdP 的仍然有效登入工作階段重新輸入其憑證。

AWS CLI 和 SDK 工作階段

如果您使用 AWS CLI、AWS SDKs 或其他 AWS 開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 AWS 受管應用程式的工作階段持續時間。

- 您必須在 IAM Identity Center 主控台中[設定 AWS 存取入口網站工作階段持續時間](#)。
- 您必須為共用 AWS 組態檔案中的單一登入設定定義設定檔。此設定檔用於連線至 AWS 存取入口網站。我們建議您使用 SSO 權杖提供者組態。使用此組態，您的 AWS SDK 或工具可以自動擷取重新整理的身分驗證字符。如需詳細資訊，請參閱 AWS SDK 和工具參考指南中的[SSO 權杖提供者組態](#)。
- 使用者必須執行支援工作階段管理的 AWS CLI 或 SDK 版本。

AWS CLI 支援工作階段管理的 最低版本

以下是 AWS CLI 支援工作階段管理的 最低版本。

- AWS CLI V2 2.9 或更新版本
- AWS CLI V1 1.27.10 或更新版本

Note

對於帳戶存取使用案例，如果您的使用者正在執行 AWS CLI，如果您在 IAM Identity Center 工作階段設定為過期之前重新整理許可集，且工作階段持續時間設定為 20 小時，而許可集持續時間設定為 12 小時，則 AWS CLI 工作階段的執行時間最長為 20 小時，加上 12 小時，總計為 32 小時。如需 IAM Identity Center CLI 的詳細資訊，請參閱 [AWS CLI 命令參考](#)。

支援 IAM Identity Center 工作階段管理的 SDKs 最低版本

以下是支援 IAM Identity Center 工作階段管理的 SDKs 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 的 SDK v2 (2.18.13)
Go V2	整個 SDK：Release-2022-11-11 和特定 Go 模組：credentials/v1.13.0、config/v1.18.0
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

在 IAM Identity Center 中停用使用者對 AWS 帳戶 和應用程式的存取

當您在 IAM Identity Center 目錄中停用使用者存取權時，您無法編輯其使用者詳細資訊、重設密碼、將使用者新增至群組，或檢視其群組成員資格。停用使用者存取可防止他們登入 AWS 存取入口網站，而且他們將無法再存取其指派 AWS 帳戶 的應用程式。當您稍後可能需要還原存取權時，請使用停用使用者存取權來移除臨時存取權。

使用下列程序，使用 IAM Identity Center 主控台停用 Identity Center 目錄中的使用者存取。

Note

當您在 IAM Identity Center 中停用使用者存取或刪除使用者時，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[了解 IAM Identity Center 中的身分驗證工作階段](#)。

在 IAM Identity Center 中停用使用者存取

1. 開啟 [IAM Identity Center 主控台](#)。

Important

本頁面上的指示適用於 [AWS IAM Identity Center](#)。它們不適用於 [AWS Identity and Access Management](#)(IAM)。IAM Identity Center 使用者、群組和使用者憑證與 IAM 使用者、群組和 IAM 使用者憑證不同。如果您要尋找在 IAM 中停用使用者的指示，請參閱 [《使用者指南》中的管理 IAM 使用者](#)。AWS Identity and Access Management

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使用者名稱下方，在一般資訊區段中，選擇停用使用者存取權。
5. 在停用使用者存取對話方塊中，選擇停用使用者存取。

使用服務控制政策拒絕使用者存取

若要在停用 IAM Identity Center 使用者的存取權或刪除使用者時，立即拒絕存取以進行授權的 API 呼叫，您可以：

1. [新增或更新](#)指派給使用者的許可集的[內嵌政策](#)（透過在所有資源上新增所有動作的明確Deny效果）。
2. 指定 `aws:userid`或 `identitystore:userid`條件索引鍵。

或者，您可以使用[服務控制政策](#)來拒絕使用者在您組織中所有成員帳戶的存取權。

Example拒絕存取的 SCP 範例

此拒絕政策會封鎖特定使用者的所有 AWS 動作，無論他們可能在別處獲得其他許可。此政策會覆寫任何Allow政策。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:UserId": "*:deleteduser@domain.com"
        }
      }
    }
  ]
}
```

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
```

```
    "StringEquals": {  
        "identitystore:UserId": "DELETEDUSER_ID"  
    }  
  }  
}
```

管理 Identity Center 目錄中使用者的存取權

了解如何在 IAM Identity Center 目錄中管理使用者的密碼和多重驗證 (MFA)。這些安全功能有助於保護使用者帳戶。

Note

這些功能不適用於 Active Directory 使用者或外部身分提供者使用者。

管理員可以透過 IAM Identity Center 主控台管理密碼和 MFA。這些安全功能僅適用於內建的 Identity Center 目錄。

密碼管理

密碼管理包含下列功能：

- 使用電子郵件指示重設密碼
- 產生一次性密碼
- 為 API 建立的使用者設定自動電子郵件驗證

AWS 強制執行固定的安全要求，包括複雜性規則和密碼重複使用限制。

MFA

MFA 預設為啟用，並支援每個使用者最多八個裝置。

支援的裝置類型包括：

- 驗證器應用程式

- 安全金鑰
- 內建生物識別驗證器

管理員可以為使用者註冊和管理 MFA 裝置。

主題

- [設定使用者密碼](#)
- [MFA for Identity Center 目錄使用者](#)

設定使用者密碼

對於在 Identity Center 目錄中建立的使用者，管理員可以管理密碼政策、在沒有初始密碼的情況下處理使用者，以及在需要時重設密碼。這些密碼管理功能僅適用於內建 Identity Center 目錄中的使用者。如果您使用的是 Active Directory 或外部身分提供者，則必須在這些系統中管理密碼。

密碼管理選項

- 密碼要求 – 使用者在設定或變更密碼時必須符合的安全要求。這包括複雜性規則和重複使用限制。
- 一次性密碼設定 – 為沒有初始密碼的 API 或 CLI 建立的使用者設定電子郵件驗證。您也可以產生臨時密碼以供立即存取。
- 密碼重設 – 為遭鎖定或需要新登入資料的使用者重設密碼。您可以使用電子郵件傳送重設指示或產生一次性密碼。

主題

- [在 IAM Identity Center 中管理身分時的密碼需求](#)
- [透過電子郵件將一次性密碼傳送給使用 API 或 CLI 建立的使用者](#)
- [重設最終使用者的 IAM Identity Center 使用者密碼](#)

在 IAM Identity Center 中管理身分時的密碼需求

Note

這些要求僅適用於在 Identity Center 目錄中建立的使用者。如果您已設定 IAM Identity Center 以外的身分來源進行身分驗證，例如 [Active Directory](#) 或 [外部身分提供者](#)，則會在這些系統中定義和強制執行使用者的密碼政策，而不是在 IAM Identity Center 中。如果您的身分來源是

AWS Managed Microsoft AD，請參閱[管理的密碼政策 AWS Managed Microsoft AD](#)以取得更多資訊。

當您使用 IAM Identity Center 做為身分來源時，使用者必須遵循下列密碼要求來設定或變更其密碼：

- 密碼區分大小寫。
- 密碼長度必須介於 8 到 64 個字元之間。
- 密碼必須至少包含下列四個類別中的一個字元：
 - 小寫字母 (a-z)
 - 大寫字母 (A-Z)
 - 數字 (0-9)
 - 非英數字元 (~!@#\$%^&* _+=`|()\{}[]:;'"<>.,?/)
- 最後三個密碼無法重複使用。
- 無法使用透過從第三方洩露的資料集公開知道的密碼。

透過電子郵件將一次性密碼傳送給使用 API 或 CLI 建立的使用者

當您使用 API [CreateUser](#) 操作或 CLI `create-user` 命令建立使用者時，使用者沒有密碼。如果您在建立使用者時已為使用者指定電子郵件，則可以更新 IAM Identity Center 中的設定，在使用者第一次嘗試登入後傳送驗證電子郵件給這些使用者。收到驗證電子郵件後，使用者必須設定密碼以登入。

如果您未啟用此設定，則必須[產生一次性密碼](#)，並與使用 CreateUser API 或 CLI `create-user` 命令建立的使用者共用。

將電子郵件地址驗證電子郵件傳送給使用 CreateUser API 或 CLI **create-user** 命令建立的使用者

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分驗證索引標籤。
4. 在標準身分驗證區段中，選擇設定。
5. 在設定標準身分驗證對話方塊中，選取傳送電子郵件 OTP 核取方塊。然後選擇 Save (儲存)。狀態會從已停用更新為已啟用。

重設最終使用者的 IAM Identity Center 使用者密碼

此程序適用於需要重設 IAM Identity Center 目錄中使用者密碼的管理員。您將使用 IAM Identity Center 主控台來重設密碼。

身分提供者和使用者類型的考量事項

- Microsoft Active Directory 或外部提供者 – 如果您要將 IAM Identity Center 連線至 Microsoft Active Directory 或外部提供者，則必須從 Active Directory 或外部提供者中重設使用者密碼。這表示無法從 IAM Identity Center 主控台重設這些使用者的密碼。
- IAM Identity Center 目錄中的使用者 – 如果您是 IAM Identity Center 使用者，您可以重設自己的 IAM Identity Center 密碼，請參閱 [重設您的 AWS 存取入口網站使用者密碼](#)。

重設 IAM Identity Center 最終使用者的密碼

Important

本頁面上的指示適用於 [AWS IAM Identity Center](#)。它們不適用於 [AWS Identity and Access Management](#)(IAM)。IAM Identity Center 使用者、群組和使用者憑證與 IAM 使用者、群組和 IAM 使用者憑證不同。如果您要尋找變更 IAM 使用者密碼的指示，請參閱 AWS Identity and Access Management 《使用者指南》中的 [管理 IAM 使用者的密碼](#)。

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Users (使用者)。
3. 選取您要重設其密碼的使用者名稱。
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. 向使用者傳送電子郵件，其中包含重設密碼的指示 – 此選項會自動向使用者傳送來自 Amazon Web Services 的電子郵件，引導他們如何重設密碼。

Warning

基於安全最佳實務，請先驗證此使用者的電子郵件地址是否正確，再選取此選項。如果此密碼重設電子郵件傳送到不正確或設定錯誤的電子郵件地址，惡意收件人可能會使用它來未經授權存取您的 AWS 環境。

- b. 產生一次性密碼並與使用者共用密碼 – 此選項為您提供密碼詳細資訊，您可以從您的電子郵件地址手動傳送給使用者。

MFA for Identity Center 目錄使用者

Important

IAM Identity Center 中的 MFA 目前不支援[外部身分提供者](#)。

IAM Identity Center 預設會預先設定多重要素驗證 (MFA)，因此所有使用者除了使用者名稱和密碼之外，還必須使用 MFA 登入。這可確保使用者必須使用下列兩個因素登入 AWS 存取入口網站：

- 他們的使用者名稱和密碼。這是使用者知道的第一個因素。
- 程式碼、安全金鑰或生物識別。這是第二個因素，是使用者擁有（擁有）或（生物指標）的項目。第二個因素可能是從其行動裝置產生的身分驗證代碼、連接到其電腦的安全金鑰，或使用者的生物識別掃描。

除非已成功完成有效的 MFA 挑戰，否則這些因素可共同防止未經授權存取您的 AWS 資源，從而提高安全性。

每個使用者最多可以註冊兩個虛擬驗證器應用程式，這是安裝在行動裝置或平板電腦上的一次性密碼驗證器應用程式，以及六個 FIDO 驗證器，其中包含內建驗證器和安全金鑰，總共八個 MFA 裝置。進一步了解 [IAM Identity Center 可用的 MFA 類型](#)。

主題

- [IAM Identity Center 可用的 MFA 類型](#)
- [在 IAM Identity Center 中設定 MFA](#)
- [為使用者註冊 MFA 裝置](#)
- [在 IAM Identity Center 中重新命名和刪除 MFA 裝置](#)

IAM Identity Center 可用的 MFA 類型

多重要素驗證 (MFA) 是一種簡單且有效的機制，可增強使用者的安全性。使用者的第一個因素 — 其密碼 — 是他們記住的秘密，也稱為知識因素。其他因素可以是擁有因素 (您擁有的事物，例如安全金鑰)

或繼承因素 (您自身的事物，例如生物特徵掃描)。我們強烈建議您設定 MFA 為您的帳戶新增額外的安全層。

IAM Identity Center MFA 支援下列裝置類型。所有 MFA 類型都支援瀏覽器型主控台存取，以及搭配 IAM Identity Center 使用 AWS CLI v2。

- [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](#)
- 您自己的[RADIUS MFA](#)實作透過 連線 AWS Managed Microsoft AD

使用者最多可以有八個 MFA 裝置，其中包含最多兩個虛擬驗證器應用程式和六個 FIDO 驗證器，註冊到一個 AWS 帳戶。您也可以將 MFA 設定設定為當 MFA 嘗試從新裝置或瀏覽器登入，或從未知 IP 地址登入時需要 MFA。如需如何為使用者設定 MFA 設定的詳細資訊，請參閱 [選擇 MFA 類型進行使用者身分驗證](#)和 [設定 MFA 裝置強制執行](#)。

FIDO2 驗證器

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

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

主題

- [內建驗證器](#)
- [安全金鑰](#)
- [密碼管理員、通行金鑰提供者和其他 FIDO 驗證器](#)

內建驗證器

許多現代電腦和行動電話都有內建的身分驗證器，例如 Macbook 上的 TouchID 或 Windows Hello 相容相機。如果您的裝置具有與 FIDO 相容的內建驗證器，您可以使用指紋、臉部或裝置接腳做為第二個因素。

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 購買並連線至您的裝置。系統提示您輸入 MFA 時，您只需使用金鑰的感應器完成手勢即可。安全金鑰的一些範例包括

YubiKeys 和 Feitian 金鑰，而最常見的安全金鑰會建立裝置繫結 FIDO 憑證。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、通行金鑰提供者和其他 FIDO 驗證器

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

Note

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

虛擬驗證器應用程式

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

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

已測試的驗證器應用程式

任何符合 TOTP 的應用程式都可以使用 IAM Identity Center MFA。下表列出知名的第三方驗證器應用程式供您選擇。

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

RADIUS MFA

[遠端身分驗證撥入使用者服務 \(RADIUS\)](#) 是一種業界標準的用戶端伺服器通訊協定，可提供身分驗證、授權和會計管理，讓使用者可以連線至網路服務。Directory Service 包含 RADIUS 用戶端，可連線至您已實作 MFA 解決方案的 RADIUS 伺服器。如需詳細資訊，請參閱[啟用的多重要素驗證 AWS Managed Microsoft AD](#)。

您可以在 IAM Identity Center 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。IAM Identity Center 中的 MFA 是 RADIUS MFA 的替代方案，如果您需要 AWS 原生雙重驗證來存取入口網站。

當您在 IAM Identity Center 中啟用 MFA 時，您的使用者需要 MFA 裝置才能登入 AWS 存取入口網站。如果您先前已使用 RADIUS MFA，在 IAM Identity Center 中啟用 MFA 會有效地覆寫登入 AWS 存取入口網站的使用者的 RADIUS MFA。不過，RADIUS MFA 會在使用者登入使用的所有其他應用程式時繼續挑戰使用者 Directory Service，例如 Amazon RDS for SQL Server。

如果您的 MFA 在 IAM Identity Center 主控台上已停用，且您已使用設定 RADIUS MFA Directory Service，則 RADIUS MFA 會管理 AWS 存取入口網站登入。這表示如果停用 MFA，IAM Identity Center 會回到 RADIUS MFA 組態。

在 IAM Identity Center 中設定 MFA

使用 IAM Identity Center 的身分存放區或 AD Connector 設定身分來源時 AWS Managed Microsoft AD，您可以在 IAM Identity Center 中設定多重要素驗證 (MFA) 功能。IAM Identity Center 中的 MFA 目前不支援[外部身分提供者](#)。

以下是一般 MFA 建議，取決於您的 IAM Identity Center 設定和組織偏好設定。

- 建議使用者為所有啟用的 MFA 類型註冊多個備份驗證器。如果 MFA 裝置損壞或放置錯誤，此做法可以防止存取遺失。
- 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，請勿選擇需要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 中使用來讀取其電子郵件。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 裝置強制執行](#)。
- 如果您已使用您設定的 RADIUS MFA Directory Service，則不需要在 IAM Identity Center 中啟用 MFA。IAM Identity Center 中的 MFA 是 IAM Identity Center Microsoft Active Directory 使用者的 RADIUS MFA 替代方案。如需詳細資訊，請參閱[RADIUS MFA](#)。
- 下列 YouTube 影片提供 MFA 和 IAM Identity Center 的概觀：

IAM Identity Center：新執行個體的多重要素驗證預設值

主題

- [MFA 提示使用者](#)
- [選擇 MFA 類型進行使用者身分驗證](#)
- [設定 MFA 裝置強制執行](#)
- [允許使用者註冊自己的 MFA 裝置](#)

MFA 提示使用者

您可以使用下列步驟，判斷當員工使用者嘗試登入 AWS 存取入口網站時，提示他們進行多重要素驗證 (MFA) 的頻率。開始之前，建議您先了解 [IAM Identity Center 可用的 MFA 類型](#)。

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 Identity Center 使用者、群組和使用者憑證與 IAM 使用者、群組和 IAM 使用者憑證不同。如果您要尋找停用 IAM 使用者 MFA 的指示，請參閱 AWS Identity and Access Management 《使用者指南》中的 [停用 MFA 裝置](#)。

Note

如果您使用的是外部 IdP，則多重要素驗證區段將無法使用。您的外部 IdP 會管理 MFA 設定，而不是管理它們的 IAM Identity Center。

設定 MFA

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在左側的導覽窗格中，選擇設定。
3. 在設定頁面上，選擇身分驗證索引標籤。
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 MFA 使用者下，根據您的業務需求，選擇下列其中一種身分驗證模式：

- 每次他們登入時（一律開啟）

在此模式中（預設設定），IAM Identity Center 會要求具有已註冊 MFA 裝置的使用者在每次登入時收到提示。這是最安全的設定，並要求每次登入 AWS 存取入口網站時都使用 MFA，以確保強制執行您的組織或合規政策。例如，PCI DSS 強烈建議在每次登入期間使用 MFA，以存取支援高風險付款交易的應用程式。

- 只有當其登入內容變更時 (context-aware)

在此模式中，IAM Identity Center 提供使用者在登入期間信任其裝置的選項。在使用者指出他們想要信任裝置之後，IAM Identity Center 會提示使用者 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 Identity Center 會判斷使用者是否使用先前信任的內容登入。如果使用者的登入內容變更，除了其電子郵件地址和密碼登入資料之外，IAM Identity Center 還會提示使用者輸入 MFA。

此模式為經常從其工作場所登入，但相較於永遠開啟選項較不安全的使用者提供易於使用的功能。只有在使用者的登入內容變更時，才會提示使用者輸入 MFA。

- 從不（已停用）

在此模式中，所有使用者只會使用其標準使用者名稱和密碼登入。選擇此選項會停用 IAM Identity Center MFA，不建議這麼做。

為使用者停用 Identity Center 目錄的 MFA 時，您無法在其使用者詳細資訊中管理 MFA 裝置，而 Identity Center 目錄使用者無法從 AWS 存取入口網站管理 MFA 裝置。

Note

如果您已經搭配使用 RADIUS MFA Directory Service，並想要繼續使用它做為預設 MFA 類型，則可以將身分驗證模式保持停用狀態，以略過 IAM Identity Center 中的 MFA 功能。從停用模式變更為上下文感知或永遠開啟模式會覆寫現有的 RADIUS MFA 設定。如需詳細資訊，請參閱[RADIUS MFA](#)。

6. 選擇 Save changes (儲存變更)。

相關主題

- [選擇 MFA 類型進行使用者身分驗證](#)
- [設定 MFA 裝置強制執行](#)
- [允許使用者註冊自己的 MFA 裝置](#)

選擇 MFA 類型進行使用者身分驗證

使用下列程序，選擇使用者在 AWS 存取入口網站中提示進行多重要素驗證 (MFA) 時，可以驗證的裝置類型。

為您的使用者設定 MFA 類型

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在左側的導覽窗格中，選擇設定。
3. 在設定頁面上，選擇身分驗證索引標籤。
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上，使用者可以使用這些 MFA 類型進行身分驗證，根據您的業務需求選擇下列其中一個 MFA 類型。如需詳細資訊，請參閱[IAM Identity Center 可用的 MFA 類型](#)。
 - 安全金鑰和內建驗證器
 - 驗證器應用程式
6. 選擇儲存變更。

設定 MFA 裝置強制執行

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。

如需 IAM 中 MFA 的詳細資訊，請參閱 [AWS IAM 中的多重要素驗證](#)。

為您的使用者設定 MFA 裝置強制執行

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在左側的導覽窗格中，選擇設定。
3. 在設定頁面上，選擇身分驗證索引標籤。
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上，如果使用者還沒有已註冊的 MFA 裝置，請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 Identity Center 設定 MFA 時的預設設定。當您想要要求尚未註冊 MFA 裝置的使用者在成功密碼身分驗證後，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 AWS 的環境，而不必個別註冊身分驗證裝置並將其分發給使用者。在自我註冊

期間，您的使用者可以從[IAM Identity Center 可用的 MFA 類型](#)先前啟用的可用註冊任何裝置。完成註冊後，使用者可以選擇為其新註冊的 MFA 裝置提供易記名稱，之後 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，您可以從其帳戶移除該裝置，IAM Identity Center 會要求他們在下次登入時自行註冊新裝置。

- 要求他們提供透過電子郵件傳送的一次性密碼來登入

如果您想要透過電子郵件將驗證碼傳送給使用者，請使用此選項。由於電子郵件未繫結至特定裝置，此選項不符合業界標準多重要素驗證的標準。但它確實比單獨使用密碼來提高安全性。只有在使用者尚未註冊 MFA 裝置時，才會請求電子郵件驗證。如果已啟用內容感知身分驗證方法，使用者將有機會將收到電子郵件的裝置標記為信任。之後，他們不需要在未來從該裝置、瀏覽器 and IP 地址組合登入時驗證電子郵件代碼。

Note

如果您使用 Active Directory 做為已啟用 IAM Identity Center 的身分來源，則電子郵件地址一律會以 Active Directory email 屬性為基礎。自訂 Active Directory 屬性映射不會覆寫此行為。

- 封鎖他們的登入

當您想要強制每個使用者使用 MFA 時，請在他們可以登入之前，使用封鎖他們的登入選項 AWS。

Important

如果您的身分驗證方法設定為了解內容，使用者可以在登入頁面上選取這是信任的裝置核取方塊。在這種情況下，即使您已啟用封鎖其登入設定，也不會提示該使用者輸入 MFA。如果您希望系統提示這些使用者，請將您的身分驗證方法變更為 Always On。

- 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 提示。

6. 選擇儲存變更。

允許使用者註冊自己的 MFA 裝置

IAM Identity Center 管理員可以允許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 Identity Center 主控台](#)。
2. 在左側的導覽窗格中，選擇設定。
3. 在設定頁面上，選擇身分驗證索引標籤。
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後，建議您將程序的連結傳送給他們 [為您的裝置註冊 MFA](#)。本主題說明如何設定自己的 MFA 裝置。

為使用者註冊 MFA 裝置

IAM Identity Center 管理員可以在 IAM Identity Center 主控台中設定新 MFA 裝置以供特定使用者存取。管理員必須擁有使用者 MFA 裝置的實體存取權，才能註冊它。例如，如果您為將在智慧型手機上執行的 MFA 裝置的使用者設定 MFA，您將需要智慧型手機的實體存取權才能完成註冊程序。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](#)。

註冊 MFA 裝置

1. 開啟 [IAM Identity Center 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。請勿選取此步驟的使用者旁的核取方塊。
3. 在使用者詳細資訊頁面上，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，選取下列其中一個 MFA 裝置類型，然後遵循指示：
 - 驗證器應用程式
 1. 在設定驗證器應用程式頁面上，IAM Identity Center 會顯示新 MFA 裝置的組態資訊，包括 QR 碼圖形。圖形是秘密金鑰的表示，可在不支援 QR 代碼的裝置上手動輸入。
 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. 判斷 MFA 應用程式是否支援 QR 代碼，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，您可以選擇攝影機圖示或選擇類似於掃描碼的選項。然後使用裝置的攝影機掃描程式碼。
 - ii. 選擇顯示私密金鑰，然後在 MFA 應用程式中輸入該私密金鑰。

 Important

當您為 IAM Identity Center 設定 MFA 裝置時，建議您將 QR 碼或私密金鑰的副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，這會很有幫助。如果發生上述任一情況，您可以快速重新設定應用程式以使用相同的 MFA 組態。這可避免需要在 IAM Identity Center 中為使用者建立新的 MFA 裝置。

3. 在設定驗證器應用程式頁面的驗證器程式碼下，輸入目前出現在實體 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，然後等待太久才提交請求，MFA 裝置就會成功與使用者建立關聯。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。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 搭配使用 AWS。

- 安全金鑰

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

這裡的體驗會根據不同的作業系統和瀏覽器而有所不同，因此請遵循瀏覽器或平台顯示的指示。成功註冊使用者的裝置後，您可以選擇將易記顯示名稱與使用者新註冊的裝置建立關聯。如果您想要變更此項目，請選擇重新命名、輸入新名稱，然後選擇儲存。如果您已啟用選項以允許使用者管理自己的裝置，使用者將在 AWS 存取入口網站中看到此易記名稱。

在 IAM Identity Center 中重新命名和刪除 MFA 裝置

IAM Identity Center 管理員可以使用下列程序來重新命名或刪除使用者的 MFA 裝置。

重新命名 MFA 裝置

1. 開啟 [IAM Identity Center 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。請勿選取此步驟的使用者旁的核取方塊。
3. 在使用者詳細資訊頁面上，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。

刪除 MFA 裝置

1. 開啟 [IAM Identity Center 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. 在使用者詳細資訊頁面上，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。

設定對應用程式的存取

透過 AWS IAM Identity Center，您可以控制誰可以對應用程式進行單一登入存取。使用者使用其目錄登入資料登入後，即可無縫存取這些應用程式。

IAM Identity Center 透過 IAM Identity Center 與應用程式服務提供者之間的信任關係，安全地與這些應用程式通訊。此信任可以透過不同方式建立，具體取決於應用程式類型。

IAM Identity Center 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](#)。受 AWS 管應用程式是直接從相關應用程式主控台或透過應用程式 APIs 設定。客戶受管應用程式必須新增至 IAM Identity Center 主控台，並使用 IAM Identity Center 和服務提供者的適當中繼資料進行設定。

設定應用程式以使用 IAM Identity Center 後，您可以管理哪些使用者或群組存取應用程式。根據預設，不會將使用者指派給應用程式。

您也可以授予員工對 AWS 帳戶 組織中特定 AWS 管理主控台 的存取權。如需詳細資訊，請參閱[設定的存取權 AWS 帳戶](#)。

主題

- [AWS 受管應用程式](#)
- [客戶受管應用程式](#)
- [信任的身分傳播概觀](#)
- [設定您自己的 OAuth 2.0 應用程式](#)
- [輪換 IAM Identity Center 憑證](#)
- [了解 IAM Identity Center 主控台內的應用程式屬性](#)
- [在 IAM Identity Center 主控台中指派使用者對應用程式的存取權](#)
- [移除使用者對 SAML 2.0 應用程式的存取權](#)
- [將應用程式中的屬性映射至 IAM Identity Center 屬性](#)

AWS 受管應用程式

AWS IAM Identity Center 可簡化將人力資源使用者連線至 Kiro 和 Amazon Quick 等 AWS 受管應用程式的任務。透過 IAM Identity Center，您可以連接現有的身分提供者一次，並從目錄同步使用者和群組，或直接在 IAM Identity Center 中建立和管理使用者。透過提供一個聯合點，IAM Identity Center 無需為每個應用程式設定聯合或使用者和群組同步，並減少您的管理工作。您也可以取得[使用者和群組指派的通用檢視](#)。

如需使用 IAM Identity Center AWS 的應用程式資料表，請參閱 [AWS 可與 IAM Identity Center 搭配使用的 受管應用程式](#)。

控制 AWS 受管應用程式的存取

AWS 受管應用程式的存取有兩種控制方式：

- 應用程式初始項目

IAM Identity Center 會透過指派給應用程式來管理此項目。根據預設，AWS 受管應用程式需要指派。如果您是應用程式管理員，您可以選擇是否需要指派給應用程式。

如果需要指派，當使用者登入時 AWS 存取入口網站，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圖磚。

如果不需要指派，您可以允許所有 IAM Identity Center 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，而造訪的所有使用者都可看見應用程式圖磚 AWS 存取入口網站。

Important

如果您是 IAM Identity Center 管理員，您可以使用 IAM Identity Center 主控台來移除 AWS 受管應用程式的指派。移除指派之前，建議您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或自動化應用程式指派的設定，您也應該與應用程式管理員協調。

- 存取應用程式資源

應用程式會透過其控制的獨立資源指派來管理此項目。

AWS 受管應用程式提供管理使用者介面，您可以用來管理對應用程式資源的存取。例如，快速管理員可以指派使用者根據其群組成員資格來存取儀表板。大多數 AWS 受管應用程式也提供可讓您將使用者指派給應用程式 AWS 管理主控台的體驗。這些應用程式的主控台體驗可能會整合這兩個函數，以結合使用者指派功能與管理應用程式資源存取的能力。

共用身分資訊

在 中共用身分資訊的考量事項 AWS 帳戶

IAM Identity Center 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、地址和偏好的語言。仔細考慮哪些應用程式和哪些帳戶可以使用此個人身分識別資訊。

您可以透過下列其中一種方式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 AWS Organizations。
- 或者，您可以使用服務控制政策 (SCPs) 來控制哪些應用程式可以存取 中帳戶的資訊 AWS Organizations。

例如，如果您只啟用 AWS Organizations 管理帳戶中的存取，則成員帳戶中的應用程式無法存取資訊。不過，如果您在所有帳戶中啟用存取，您可以使用 SCPs 來禁止所有應用程式存取，但您想要允許的應用程式除外。

服務控制政策是 的一項功能 AWS Organizations。如需連接 SCP 的說明，請參閱《使用者指南》中的[連接和分離服務控制政策](#)。AWS Organizations

設定 IAM Identity Center 以共用身分資訊

IAM Identity Center 提供身分存放區，其中包含使用者和群組屬性，但不包括登入憑證。您可以使用下列其中一種方法來讓 IAM Identity Center 身分存放區中的使用者和群組保持最新狀態：

- 使用 IAM Identity Center 身分存放區做為主要身分來源。如果您選擇此方法，您可以從 IAM Identity Center 主控台或 AWS Command Line Interface () 中管理您的使用者、其登入憑證和群組AWS CLI。如需詳細資訊，請參閱[在 Identity Center 目錄中管理使用者](#)。
- 設定從下列任一身分來源到 IAM Identity Center 身分存放區的使用者和群組佈建（同步）：
 - Active Directory – 如需詳細資訊，請參閱 [Microsoft AD 目錄](#)。
 - 外部身分提供者 – 如需詳細資訊，請參閱 [外部身分提供者](#)。

如果您選擇此佈建方法，您可以繼續從身分來源管理使用者和群組，並將這些變更同步至 IAM Identity Center 身分存放區。

無論您選擇哪個身分來源，IAM Identity Center 都可以與 AWS 受管應用程式共用使用者和群組資訊。如此一來，您可以將身分來源連線至 IAM Identity Center 一次，然後與 中的多個應用程式共用身分資訊 AWS 雲端。這樣就不需要為每個應用程式獨立設定聯合和身分佈建。此共用功能也可讓您的使用者輕鬆存取不同 中的許多應用程式 AWS 帳戶。

限制使用 AWS 受管應用程式

當您第一次啟用 IAM Identity Center 時，它會成為 中所有帳戶受管 AWS 應用程式的身分來源 AWS Organizations。若要限制應用程式，您必須實作服務控制政策 SCPs)。SCPs是 的一項功能 AWS

Organizations，可用來集中控制組織中身分（使用者和角色）可以擁有的最大許可。您可以使用 SCPs 來封鎖對 IAM Identity Center 使用者和群組資訊的存取，並防止應用程式啟動，但在指定的帳戶中除外。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[服務控制政策 \(SCP\)](#)。

下列 SCP 範例會封鎖對 IAM Identity Center 使用者和群組資訊的存取，並防止應用程式啟動，但指定帳戶 (111111111111 和 222222222222 除外)：

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

AWS 可與 IAM Identity Center 搭配使用的 受管應用程式

IAM Identity Center 可讓您連接現有的身分來源或建立使用者一次。這可讓應用程式管理員管理對下列 AWS 受管應用程式的存取，而無需個別聯合或使用者和群組同步。

下表中的所有 AWS 受管應用程式都會與 [IAM Identity Center 的組織執行個體](#) 整合。資料表也提供受支援 AWS 受管應用程式下列項目的相關資訊：

- 應用程式是否也與 IAM Identity Center 的帳戶執行個體整合
- 應用程式是否可以透過 IAM Identity Center 啟用受信任身分傳播
- 應用程式是否支援使用客戶受管 KMS 金鑰設定的 IAM Identity Center
- 應用程式是否支援在 IAM Identity Center 的其他區域中部署

Note

支援在其他 IAM Identity Center 區域中部署的應用程式也支援使用客戶受管 KMS 金鑰設定的 IAM Identity Center。此處列出的每個 AWS 受管應用程式都支援在主要區域中部署。如需詳細資訊，請參閱[the section called “在多個 之間部署和管理 AWS 受管應用程式 AWS 區域”](#)。

AWS 與 IAM Identity Center 整合的受管應用程式

AWS 受管應用程式	與 IAM Identity Center 的帳戶執行個體整合	透過 IAM Identity Center 啟用受信任的身分傳播	支援使用客戶受管 KMS 金鑰設定的 IAM Identity Center	支援在 IAM Identity Center 的其他區域中部署
Amazon Athena SQL	是	是	是	是
Amazon CodeCatalyst	是	否	是	否
Amazon DataZone	是	是	是	否
Amazon EKS 功能	是	是	是	否
EC2 上的 Amazon EMR	是	是	是	否
Amazon EMR on EKS	是	是	是	否
Amazon EMR Serverless	是	是	是	否
Amazon EMR Studio	是	是	是	否
Amazon Kendra	否	否	是	否
Amazon Managed Grafana	否	否	是	否
Amazon Monitron	否	否	否	否
Amazon OpenSearch Service	是	是	是	否
Amazon OpenSearch Service Serverless Service	是	是	是	否

AWS 受管應用程式	與 IAM Identity Center 的帳戶執行個體整合	透過 IAM Identity Center 啟用受信任的身分傳播	支援使用客戶受管 KMS 金鑰設定的 IAM Identity Center	支援在 IAM Identity Center 的其他區域中部署
Amazon Q Business	是	是	是	否
Amazon Quick	是	是	是	否
Amazon Redshift	是 ²	是	是	是
Amazon S3 Access Grants	是	是	是	是
Amazon SageMaker Studio	否	是	是	否
Amazon SageMaker Unified Studio	是	是	是	是
Amazon WorkMail	是	是	是	否
Amazon WorkSpaces	是	否	是	否
Amazon WorkSpaces Secure Browser	否	否	是	否
AWS App Studio	是	否	否	否
AWS Deadline Cloud	是	否	是	是
AWS Glue	是	是	是	否
AWS IoT Events	否	否	否	否
AWS IoT SiteWise	否	否	否	否
AWS Lake Formation	是	是	是	是
AWS re:Post Private	是	否	是	否
AWS Supply Chain	是	否	是	否

AWS 受管應用程式	與 IAM Identity Center 的帳戶執行個體整合	透過 IAM Identity Center 啟用受信任的身分傳播	支援使用客戶受管 KMS 金鑰設定的 IAM Identity Center	支援在 IAM Identity Center 的其他區域中部署
AWS Systems Manager	否	否	是	是 - Fleet Manager 遠端桌面
AWS Transfer Family Web 應用程式	是	是	是	是
AWS 轉換	是	否	是	否
AWS Verified Access	否	否	是	否
開羅	是 ¹	是	是	否
多方核准	否	是	是	否
OpenSearch user interface (Dashboards)	是	是	是	否

¹ 對於 Kiro，支援 IAM Identity Center 的帳戶執行個體，除非您的使用者需要存取 AWS 網站上完整的 Kiro 功能集。如需詳細資訊，請參閱《[Kiro 使用者指南](#)》中的設定 Kiro。

² 對於 Amazon Redshift，IAM Identity Center 的帳戶執行個體受支援，但如查詢編輯器 v2 等需要許可集的應用程式除外，這些應用程式不受帳戶執行個體支援。

Note

雖然您可以搭配 IAM Identity Center 使用某些 AWS 服務，例如 Amazon Connect 和 AWS Client VPN 不會列在此資料表中。這是因為它們只使用 SAML 與 IAM Identity Center 整合，因此歸類為[客戶受管應用程式](#)。

快速入門：設定 IAM Identity Center 以測試 AWS 受管應用程式

如果您的管理員尚未提供 IAM Identity Center 的存取權，您可以使用本主題中的步驟來設定 IAM Identity Center 來測試 AWS 受管應用程式。您將了解如何啟用 IAM Identity Center、直接在 IAM Identity Center 中建立使用者，並將該使用者指派給 AWS 受管應用程式。

本主題提供如何以下列其中一種方式啟用 IAM Identity Center 的快速入門步驟：

- 使用 AWS Organizations – 如果您選擇此選項，則會建立 IAM Identity Center 的組織執行個體。
- 僅在您的特定 AWS 帳戶- 如果您選擇此選項，則會建立 IAM Identity Center 的帳戶執行個體。

如需這些執行個體類型的詳細資訊，請參閱 [IAM Identity Center 的組織和帳戶執行個體](#)。

先決條件

啟用 IAM Identity Center 之前，請確認下列事項：

- 您有 AWS 帳戶- 如果您沒有 AWS 帳戶，請參閱《帳戶管理參考指南》中的 [入門 AWS 帳戶](#)。AWS
- AWS 受管應用程式可與 IAM Identity Center 搭配使用 – 檢閱的清單，[AWS 可與 IAM Identity Center 搭配使用的受管應用程式](#)以確認您要測試的 AWS 受管應用程式可與 IAM Identity Center 搭配使用。
- 您已檢閱區域考量 – 請確定您要測試的 AWS 受管應用程式在您啟用 IAM Identity Center AWS 區域的中受到支援。如需詳細資訊，請參閱受管 AWS 應用程式的文件。

Note

您必須在計劃啟用 IAM Identity Center 的相同區域中部署 AWS 受管應用程式。

設定 IAM Identity Center 的組織執行個體以測試 AWS 受管應用程式

Note

本主題說明如何使用 啟用 IAM Identity Center AWS Organizations，這是啟用 IAM Identity Center 的建議方法。

確認您的許可

若要使用 啟用 IAM Identity Center AWS Organizations，您必須以下列其中一種方式登入 AWS 管理主控台：

- 在將啟用 IAM Identity Center 的 AWS 帳戶 中具有管理許可的使用者 AWS Organizations。
- 根使用者（除非不存在其他管理使用者，否則不建議使用）。

Important

根使用者可存取帳戶中的所有 AWS 服務和資源。作為安全最佳實務，除非您沒有其他登入資料，否則請勿使用您帳戶的根登入資料來存取 AWS 資源。這些登入資料可讓未管制的帳戶存取和很難撤銷這些帳戶。

步驟 1. 使用 啟用 IAM Identity Center AWS Organizations

1. 執行下列其中一項操作來登入 AWS 管理主控台。
 - 新使用者 AWS（根使用者）– 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者的身分登入。在下一頁中，輸入您的密碼。
 - 已使用 AWS 搭配獨立 AWS 帳戶 (IAM 憑證) – 使用您的 IAM 憑證搭配管理許可來登入。
2. 在 AWS 管理主控台首頁上，選取 IAM Identity Center 服務或導覽至 [IAM Identity Center 主控台](#)。
3. 選擇啟用，並使用 啟用 IAM Identity Center AWS Organizations。執行此操作時，您要建立 IAM Identity Center [的組織執行個體](#)。

步驟 2. 在 IAM Identity Center 中建立管理使用者

此程序說明如何直接在內建 Identity Center 目錄中建立使用者。此目錄不會連接到管理員可能用來管理人力資源使用者的任何其他目錄。在 IAM Identity Center 中建立使用者後，您將為此使用者指定新的登入資料。當您以此使用者身分登入以測試受 AWS 管應用程式時，您將使用新的登入資料登入，而不是您用來存取公司資源的任何現有登入資料。

Note

我們建議您使用此方法來建立使用者，僅用於測試目的。

1. 在 IAM Identity Center 主控台的導覽窗格中，選擇使用者，然後選擇新增使用者。

2. 遵循 主控台 中的指引來新增使用者。保留選取密碼設定指示來傳送電子郵件給此使用者，並確認指定您有權存取的電子郵件地址。
3. 在導覽窗格中，選擇 AWS 帳戶，選取您帳戶旁的核取方塊，然後選擇指派使用者或群組。
4. 選擇使用者索引標籤，選取您剛新增的使用者旁的核取方塊，然後選擇下一步。
5. 選擇建立許可集，然後遵循主控台 中的指引來建立 AdministratorAccess 預先定義的許可集。
6. 完成後，新的許可集會出現在清單中。關閉瀏覽器視窗中的許可集索引標籤，返回指派使用者和群組索引標籤，然後選擇建立許可集旁的重新整理圖示。
7. 在指派使用者和群組瀏覽器索引標籤上，新的許可集會出現在清單中。選取許可集名稱旁的核取方塊，選擇下一步，然後選擇提交。
8. 登出 主控台。

步驟 3. 以管理使用者身分登入 AWS 存取入口網站

AWS 存取入口網站是一種 Web 入口網站，可讓您建立可存取 AWS 管理主控台的使用者。您必須先接受加入 IAM Identity Center 的邀請並啟用您的使用者登入資料，才能登入 AWS 存取入口網站。

1. 檢查您的電子郵件是否有主旨行邀請加入 AWS IAM Identity Center。
2. 選擇接受邀請，並遵循註冊頁面上的指引，為您的使用者設定新密碼、登入和註冊 MFA 裝置。
3. 註冊 MFA 裝置後，AWS 存取入口網站會開啟。
4. 在 AWS 存取入口網站中，選取您的 AWS 帳戶，然後選擇 AdministratorAccess。系統會將您重新導向至 AWS 管理主控台。

步驟 4. 設定 AWS 受管應用程式以使用 IAM Identity Center

1. 當您登入 AWS 管理主控台時，請為您計劃使用的 AWS 受管應用程式開啟主控台。
2. 遵循 主控台 中的指引，將 AWS 受管應用程式設定為使用 IAM Identity Center。在此過程中，您可以將您建立的使用者指派給應用程式。

設定 IAM Identity Center 的帳戶執行個體以測試 AWS 受管應用程式

Note

IAM Identity Center 的帳戶執行個體會將您的部署限制為單一 AWS 帳戶。您必須在與要測試 AWS 的應用程式相同的 AWS 區域 中啟用此執行個體。

確認您的應用程式

使用 IAM Identity Center 的所有 AWS 受管應用程式都可以與 IAM Identity Center 的組織執行個體搭配使用。不過，只有其中一些應用程式可以與 IAM Identity Center 的帳戶執行個體搭配使用。檢閱的清單 [AWS 可與 IAM Identity Center 搭配使用的 受管應用程式](#)。

Step1：啟用 IAM Identity Center 的帳戶執行個體。

1. 執行下列其中一項操作來登入 AWS 管理主控台。
 - 新使用者 AWS（根使用者）– 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者的身分登入。在下一頁中，輸入您的密碼。
 - 已使用 AWS 搭配獨立 AWS 帳戶 (IAM 憑證) – 使用您的 IAM 憑證搭配管理許可來登入。
2. 在 AWS 管理主控台首頁上，選取 IAM Identity Center 服務或導覽至 [IAM Identity Center 主控台](#)。
3. 選擇啟用。
4. 在使用 啟用 IAM Identity Center AWS Organizations 頁面上，選擇啟用 IAM Identity Center 的帳戶執行個體。
5. 在啟用 IAM Identity Center 帳戶執行個體頁面上，檢閱資訊並選擇性地新增要與此帳戶執行個體建立關聯的標籤。然後選擇啟用。

步驟 2. 在 IAM Identity Center 中建立使用者

此程序說明如何直接在內建 Identity Center 目錄中建立使用者。此目錄不會連接到管理員可能用來管理人力資源使用者的任何其他目錄。在 IAM Identity Center 中建立使用者後，您將為此使用者指定新的登入資料。當您以此使用者身分登入以測試受 AWS 管應用程式時，您將使用新的登入資料登入。新的登入資料將不允許您存取其他公司資源。

Note

我們建議您使用此方法來建立使用者，僅用於測試目的。

1. 在 IAM Identity Center 主控台的導覽窗格中，選擇使用者，然後選擇新增使用者。
2. 遵循 主控台 中的指引來新增使用者。保留選取密碼設定指示來傳送電子郵件給此使用者，並確認指定您有權存取的電子郵件地址。
3. 登出 主控台。

步驟 3. 以您的 IAM Identity Center 使用者身分登入 AWS 存取入口網站

AWS 存取入口網站是一種 Web 入口網站，可讓您建立可存取 AWS 管理主控台的使用者。您必須先接受加入 IAM Identity Center 的邀請並啟用您的使用者登入資料，才能登入 AWS 存取入口網站。

1. 檢查您的電子郵件是否有主旨行邀請加入 AWS IAM Identity Center。
2. 選擇接受邀請，並遵循註冊頁面上的指引，為您的使用者設定新密碼、登入和註冊 MFA 裝置。
3. 註冊 MFA 裝置後，AWS 存取入口網站會開啟。當應用程式可供您使用時，您可以在應用程式索引標籤下找到它們。

Note

AWS 支援帳戶執行個體的應用程式允許使用者登入應用程式，而不需要額外的許可。因此，帳戶索引標籤將保持空白。

步驟 4. 設定 AWS 受管應用程式以使用 IAM Identity Center

1. 當您登入 AWS 管理主控台時，請為您計劃使用的 AWS 受管應用程式開啟主控台。
2. 遵循 主控台 中的指引，將 AWS 受管應用程式設定為使用 IAM Identity Center。在此過程中，您可以將您建立的使用者指派給應用程式。

檢視和變更 AWS 受管應用程式的詳細資訊

使用 主控台 或 應用程式的 APIs 將 AWS 受管應用程式連線至 IAM Identity Center 後，應用程式會向 IAM Identity Center 註冊。向 IAM Identity Center 註冊應用程式後，您可以在 IAM Identity Center 主控台中檢視和變更應用程式的詳細資訊。

有關應用程式的資訊包括是否需要使用者和群組指派，以及如果適用，為身分傳播指派的使用者和群組和信任的應用程式。如需受信任身分傳播的資訊，請參閱 [信任的身分傳播概觀](#)。

在 IAM Identity Center 主控台中檢視和變更 AWS 受管應用程式的相關資訊

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Applications (應用程式)。
3. 選擇 AWS 受管索引標籤。
4. 選擇您要開啟和檢視之受管應用程式的連結。

5. 如果您想要變更 AWS 受管應用程式的相關資訊，請選擇動作，然後選擇編輯詳細資訊。
6. 您可以變更應用程式的顯示名稱、描述，以及使用者和群組指派方法。
 - a. 若要變更顯示名稱，請在顯示名稱欄位中輸入所需的名稱，然後選擇儲存變更。
 - b. 若要變更描述，請在描述欄位中輸入所需的描述，然後選擇儲存變更。
 - c. 若要變更使用者和群組指派方法，請進行所需的變更，然後選擇儲存變更。如需詳細資訊，請參閱[the section called “使用者、群組和佈建”](#)。

停用 AWS 受管應用程式

若要防止使用者驗證受 AWS 管應用程式，您可以在 IAM Identity Center 主控台中停用應用程式。

停用 AWS 受管應用程式

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Applications (應用程式)。
3. 在應用程式頁面的AWS 受管應用程式下，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. 在停用應用程式對話方塊中，選擇停用。
6. 在AWS 受管應用程式清單中，應用程式狀態會顯示為非作用中。

Note

如果停用 AWS 受管應用程式，您可以選擇動作，然後選擇啟用，以還原使用者對應用程式進行身分驗證的彈性。

啟用身分增強主控台工作階段

主控台的身分增強工作階段透過提供一些額外的使用者內容來個人化該使用者的使用體驗，來增強使用者的 AWS 主控台工作階段。[AWS 應用程式和網站上的 Kiro](#) Pro 使用者目前支援此功能。

您可以啟用身分增強主控台工作階段，而無需在 AWS 主控台中對現有的存取模式或聯合進行任何變更。如果您的使用者使用 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 的聯合身分存取），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 Identity Center 使用者憑證。

主題

- [先決條件和考量事項](#)
- [如何啟用identity-enhanced-console工作階段](#)
- [身分增強主控台工作階段的運作方式](#)

先決條件和考量事項

啟用身分增強主控台工作階段之前，請檢閱下列先決條件和考量事項：

- 如果您的使用者透過 Kiro Pro 訂閱在 AWS 應用程式和網站上存取 Kiro，您必須啟用身分增強主控台工作階段。

Note

Kiro 使用者可以在沒有身分增強工作階段的情況下存取 Kiro，但無法存取其 Kiro Pro 訂閱。

- 身分增強主控台工作階段需要 IAM Identity Center [的組織執行個體](#)。
- 如果您在選擇加入中啟用 IAM Identity Center，則不支援與 Kiro 整合 AWS 區域。
- 若要啟用身分增強主控台工作階段，您必須具有下列許可：
 - `sso:CreateApplication`
 - `sso:GetSharedSsoConfiguration`
 - `sso:ListApplications`
 - `sso:PutApplicationAssignmentConfiguration`
 - `sso:PutApplicationAuthenticationMethod`
 - `sso:PutApplicationGrant`
 - `sso:PutApplicationAccessScope`
 - `signin:CreateTrustedIdentityPropagationApplicationForConsole`
 - `signin:ListTrustedIdentityPropagationApplicationsForConsole`
- 若要讓使用者能夠使用身分增強主控台工作階段，您必須在以身分為基礎的政策中授予他們 `sts:setContext` 許可。如需詳細資訊，請參閱 [授予使用者使用身分增強主控台工作階段的許可](#)。

如何啟用identity-enhanced-console工作階段

您可以在 Kiro 主控台或 IAM Identity Center 主控台中啟用身分增強主控台工作階段。

在 Kiro 主控台中啟用身分增強主控台工作階段

啟用身分增強主控台工作階段之前，您必須擁有已連接身分來源的 IAM Identity Center 組織執行個體。如果您已設定 IAM Identity Center，請跳至步驟 3。

1. 開啟 IAM Identity Center 主控台。選擇啟用，然後建立 IAM Identity Center 的組織執行個體。如需相關資訊，請參閱[啟用 IAM Identity Center](#)。
2. 將您的身分來源連接至 IAM Identity Center，並將使用者佈建至 IAM Identity Center。如果您尚未使用其他身分來源，您可以將現有的身分來源連線至 IAM Identity Center，或使用 Identity Center 目錄。如需詳細資訊，請參閱[IAM Identity Center 身分來源教學課程](#)。
3. 完成設定 IAM Identity Center 後，請開啟 Kiro 主控台，並遵循 Kiro 使用者指南中的[訂閱](#)步驟。請務必啟用身分增強主控台工作階段。

Note

如果您沒有足夠的許可來啟用身分增強主控台工作階段，您可能需要要求 IAM Identity Center 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 Identity Center 主控台中啟用身分增強主控台工作階段

如果您是 IAM Identity Center 管理員，則其他管理員可能會要求您在 IAM Identity Center 主控台中啟用身分增強主控台工作階段。

1. 開啟 IAM Identity Center 主控台。
2. 在導覽窗格中，選擇設定。
3. 在啟用身分增強工作階段下，選擇啟用。
4. 在第二個訊息中，選擇啟用。
5. 完成啟用身分增強主控台工作階段後，確認訊息會出現在設定頁面頂端。
6. 在詳細資訊區段中，身分增強工作階段的狀態為已啟用。

身分增強主控台工作階段的運作方式

IAM Identity Center 會增強使用者目前的主控制台工作階段，以包含作用中 IAM Identity Center 使用者的 ID 和 IAM Identity Center 工作階段 ID。

身分增強主控台工作階段包含下列三個值：

- 身分存放區使用者 ID ([identitystore:UserId](#)) - 此值用於唯一識別連接到 IAM Identity Center 的身分來源中的使用者。
- 身分存放區目錄 ARN ([identitystore : IdentityStoreArn](#)) - 此值是連接到 IAM Identity Center 的身分存放區的 ARN，您可以在其中查詢的屬性 `identitystore:UserId`。
- IAM Identity Center 工作階段 ID - 此值指出使用者的 IAM Identity Center 工作階段是否仍然有效。

這些值相同，但以不同的方式取得，並在程序的不同點新增，取決於使用者登入的方式：

- IAM Identity Center (AWS 存取入口網站)：在此情況下，使用者的身分存放區使用者 ID 和 ARN 值已在作用中的 IAM Identity Center 工作階段中提供。IAM Identity Center 只會新增工作階段 ID，以增強目前的工作階段。
- 其他登入方法：如果使用者 AWS 以 IAM 使用者、IAM 角色或 IAM 聯合身分使用者身分登入，則不會提供任何這些值。IAM Identity Center 透過新增身分存放區使用者 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。

客戶受管應用程式

IAM Identity Center 可做為人力資源使用者和群組的中央身分服務。如果您已使用身分提供者 (IdP)，IAM Identity Center 可以與您的 IdP 整合，以便您可以將使用者和群組佈建至 IAM Identity Center，並使用 IdP 進行身分驗證。透過單一連線，IAM Identity Center 會在多個前面代表您的 IdP，AWS 服務並讓 OAuth 2.0 應用程式代表您的使用者請求存取這些服務中的資料。您也可以使用 IAM Identity Center 為您的使用者指派對 [SAML 2.0](#) 應用程式的存取權。這包括 Amazon Connect 和等 AWS 服務 AWS Client VPN，這些服務專門使用 SAML 與 IAM Identity Center 整合，因此歸類為客戶受管應用程式。

- 如果您的應用程式支援 JSON Web Token (JWTs)，您可以使用 IAM Identity Center 的信任身分傳播功能，讓您的應用程式 AWS 服務代表使用者請求存取中的資料。信任的身分傳播建立在 OAuth 2.0 授權架構上，並包含一個選項，讓應用程式交換來自外部 OAuth 2.0 授權伺服器的身分字符，用於 IAM Identity Center 發行並由識別的字符 AWS 服務。如需詳細資訊，請參閱[信任的身分傳播使用案例](#)。

- 如果您的應用程式支援 SAML 2.0，您可以將其連線到 [IAM Identity Center 的組織執行個體](#)。您可以使用 IAM Identity Center 將存取權指派給 SAML 2.0 應用程式。

 Note

將客戶受管應用程式與使用 [客戶受管 KMS 金鑰](#) 的 IAM Identity Center 執行個體整合時，請確認應用程式是否叫用 IAM Identity Center 服務 APIs。如果是這樣，請參閱必要許可的 [基準 KMS 金鑰政策](#)。

主題

- [單一登入存取 SAML 2.0 和 OAuth 2.0 應用程式](#)
- [設定客戶受管 SAML 2.0 應用程式](#)

單一登入存取 SAML 2.0 和 OAuth 2.0 應用程式

IAM Identity Center 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 是產業標準，用於在 SAML 授權單位（稱為身分提供者或 IdP）和 SAML 2.0 消費者（稱為服務提供者或 SP）之間安全地交換傳遞使用者相關資訊的 SAML 聲明。IAM Identity Center 會使用此資訊，為有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。

 Note

IAM Identity Center 不支援驗證來自 SAML 應用程式傳入 SAML 身分驗證請求的簽章。

OAuth 2.0

OAuth 2.0 是一種通訊協定，可讓應用程式安全地存取和共用使用者資料，而無需共用密碼。此功能為使用者提供安全且標準化的方式，以允許應用程式存取其資源。透過不同的 OAuth 2.0 授予流程來促進存取。

IAM Identity Center 可讓在公有用戶端上執行的應用程式擷取臨時憑證，以透過程式設計方式代表其使用者存取 AWS 帳戶 和服務。公有用戶端通常是用於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。在公有用戶端上執行的應用程式範例 AWS 包括 AWS Command Line Interface (AWS CLI) AWS 工具組、和 AWS 軟體開發套件 (SDKs)。為了讓這些應用程式能夠取得登入資料，IAM Identity Center 支援下列部分 OAuth 2.0 流程：

- 授權碼授予與程式碼交換的驗證金鑰 (PKCE) ([RFC 6749](#) 和 [RFC 7636](#))
- 裝置授權授予 ([RFC 8628](#))

Note

這些授予類型只能與支援此功能 AWS 服務 的 搭配使用。這些服務可能不會在所有 中支援此授予類型 AWS 區域。請參閱有關 AWS 服務 區域差異的文件。

OpenID Connect (OIDC) 是一種以 OAuth 2.0 架構為基礎的身分驗證通訊協定。OIDC 指定如何使用 OAuth 2.0 進行身分驗證。透過 [IAM Identity Center OIDC 服務 APIs](#)，應用程式會註冊 OAuth 2.0 用戶端，並使用其中一個流程來取得存取字符，以提供 IAM Identity Center 受保護 APIs 許可。應用程式會指定 [存取範圍](#) 來宣告其預期的 API 使用者。在身為 IAM Identity Center 管理員的您設定身分來源之後，如果應用程式最終使用者尚未完成登入程序。您的最終使用者接著必須提供其同意，以允許應用程式進行 API 呼叫。這些 API 呼叫會使用使用者的許可進行。IAM Identity Center 會傳回存取字符給應用程式，其中包含使用者同意的存取範圍。

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 受管應用程式使用。若要使用 OAuth 2.0 流程，您的 IAM Identity Center 執行個體和您使用的任何受支援 AWS 受管應用程式必須部署在單一 中 AWS 區域。請參閱每個 的文件 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 Identity Center 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與 IAM Identity Center 執行個體連線和註冊的 URL。視應用程式而定，身為管理員，您必須提供使用者 AWS 存取入口網站

URL 或 IAM Identity Center 執行個體的發行者 URL。您可以在 [IAM Identity Center 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最終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 [裝置授權授予](#)。

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. 如果使用者尚未驗證，瀏覽器會將他們重新導向以完成使用者身分驗證。
3. 身分驗證後，使用者會收到顯示下列資訊的同意畫面：
 - 應用程式的名稱
 - 應用程式請求同意使用的存取範圍
4. 使用者可以取消同意程序，也可以提供其同意，而應用程式會根據使用者的許可繼續存取。

裝置授權授予

此流程可供在含或不含瀏覽器的裝置上執行的應用程式使用。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驗證。使用者程式碼是必要的，因為啟動流程的應用程式可能在與使用者提供同意的裝置不同的裝置上執行。此程式碼可確保使用者同意他們在其他裝置上啟動的流程。

Note

如果您有用戶端使用 `device.sso.region.amazonaws.com`，您必須更新授權流程，以使用程式碼交換的驗證金鑰 (PKCE)。如需詳細資訊，請參閱 [《使用者指南》中的使用 設定 IAM Identity Center 身分驗證 AWS CLI](#)。AWS Command Line Interface

1. 當流程從具有瀏覽器的裝置啟動時，瀏覽器視窗會開啟。當流程從沒有瀏覽器的裝置啟動時，使用者必須在不同的裝置上開啟瀏覽器，並前往應用程式顯示的 URL。
2. 無論哪種情況，如果使用者尚未驗證，瀏覽器都會重新導向他們以完成使用者身分驗證。
3. 身分驗證後，使用者會收到顯示下列資訊的同意畫面：
 - 應用程式的名稱
 - 應用程式請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. 使用者可以取消同意程序，也可以提供其同意，而應用程式會根據使用者的許可繼續存取。

存取範圍

範圍定義可透過 OAuth 2.0 流程存取的服務存取。範圍是服務的一種方式，也稱為資源伺服器，用於將與動作和服務資源相關的許可分組，並指定 OAuth 2.0 用戶端可以請求的粗略精細操作。當 OAuth 2.0 用戶端向 [IAM Identity Center OIDC 服務](#) 註冊時，用戶端會指定宣告其預期動作的範圍，使用者必須提供同意。

OAuth 2.0 用戶端使用 [OAuth 2.0 \(RFC 6749\) 第 3.3 節](#) 中定義的 scope 值，來指定要為存取字符請求哪些許可。請求存取權杖時，用戶端最多可指定 25 個範圍。當使用者在授權碼授予與 PKCE 或裝置授權授予流程中提供同意時，IAM Identity Center 會將範圍編碼為傳回的存取權杖。

AWS 會將範圍新增至支援的 IAM Identity Center AWS 服務。下表列出 IAM Identity Center OIDC 服務在您註冊公有用戶端時支援的範圍。

註冊公有用戶端時，IAM Identity Center OIDC 服務支援的存取範圍

Scope (範圍)	Description	支援的服務
sso:account:access	存取 IAM Identity Center 受管帳戶和許可集。	IAM Identity Center
codewhisperer:analysis	啟用存取 Kiro 程式碼分析。	AWS 建構家 ID 和 IAM Identity Center
codewhisperer:completions	啟用存取 Kiro 內嵌程式碼建議。	AWS 建構家 ID 和 IAM Identity Center
codewhisperer:conversations	啟用存取 Kiro 聊天。	AWS 建構家 ID 和 IAM Identity Center
codewhisperer:taskassist	啟用存取 Kiro Agent 以進行軟體開發。	AWS 建構家 ID 和 IAM Identity Center

Scope (範圍)	Description	支援的服務
codewhisperer:transformations	啟用存取 Kiro Agent 以進程式碼轉換。	AWS 建構家 ID 和 IAM Identity Center
codecatalyst:read_write	讀取和寫入 Amazon CodeCatalyst 資源，允許存取所有現有的資源。	AWS 建構家 ID 和 IAM Identity Center
verified_access:application:connect	啟用 AWS Verified Access	AWS Verified Access
redshift:connect	連線至 Amazon Redshift	Amazon Redshift
datazone:domain:access	存取 DataZone 網域執行角色	Amazon DataZone
nosqlworkbench:datamodeladviser	建立和讀取資料模型	NoSQL Workbench
transform:read_write	啟用對 AWS Transform Agent 的存取權以進程式碼轉換	AWS 轉換

設定客戶受管 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 聯合到 IAM Identity Center，並使用 IAM Identity Center 管理使用者對這些應用程式的存取。您可以從 IAM Identity Center 主控台中常用應用程式的目錄中選取 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 的客戶受管應用程式，且您的使用者需要從這些應用程式存取 AWS 服務，則可以使用信任的身分傳播。透過受信任的身分傳播，使用者可以登入應用程式，且該應用程式可以在存取資料的請求中傳遞使用者的身分 AWS 服務。

主題

- [從 IAM Identity Center 應用程式目錄設定應用程式](#)
- [設定您自己的 SAML 2.0 應用程式](#)

從 IAM Identity Center 應用程式目錄設定應用程式

您可以使用 IAM Identity Center 主控台中的應用程式目錄，新增許多與 IAM Identity Center 搭配使用的常用 SAML 2.0 應用程式。範例包括 Salesforce、Box 和 Microsoft 365。

大多數應用程式提供有關如何設定 IAM Identity Center 與應用程式服務提供者之間信任的詳細資訊。在目錄中選取應用程式之後，此資訊可在應用程式的組態頁面中取得。設定應用程式後，您可以視需要將存取權指派給 IAM Identity Center 中的使用者或群組。

使用此程序來設定 IAM Identity Center 與您應用程式服務提供者之間的 SAML 2.0 信任關係。

在開始此程序之前，擁有服務供應商的中繼資料交換檔案會很有幫助，讓您可以更有效率地設定信任。如果您沒有此檔案，您仍然可以使用此程序來手動設定信任。

從應用程式目錄新增和設定應用程式

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Applications (應用程式)。
3. 選擇客戶管理索引標籤。
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，選擇我想要從目錄中選取應用程式。
6. 在應用程式目錄下，開始輸入您要在搜尋方塊中新增的應用程式名稱。
7. 當應用程式出現在搜尋結果中時，從清單中選擇應用程式的名稱，然後選擇下一步。
8. 在設定應用程式頁面上，顯示名稱和描述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 Identity Center 中繼資料下，執行下列動作：

- a. 在 IAM Identity Center SAML 中繼資料檔案下，選擇下載以下載身分提供者中繼資料。
- b. 在 IAM Identity Center 憑證下，選擇下載憑證以下載身分提供者憑證。

 Note

當您稍後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. (選用) 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[了解 IAM Identity Center 主控台中的應用程式屬性](#)。
11. 在應用程式中繼資料下，執行下列其中一項操作：
 - 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，選取選擇檔案以尋找並選取中繼資料檔案。
 - 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 Application ACS URL 和 Application SAML 對象值。
12. 選擇提交。系統會將您導向至您剛新增之應用程式的詳細資訊頁面。

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 的聯合身分，並將其新增至 IAM Identity Center。設定您自己的 SAML 2.0 應用程式的步驟大多與從 IAM Identity Center 主控台的應用程式目錄設定 SAML 2.0 應用程式相同。不過，您還必須為自己的 SAML 2.0 應用程式提供額外的 SAML 屬性映射。這些映射可讓 IAM Identity Center 為您的應用程式正確填入 SAML 2.0 聲明。您可以在第一次設定應用程式時提供此額外的 SAML 屬性映射。您也可以在此 IAM Identity Center 主控台的應用程式詳細資訊頁面上提供 SAML 2.0 屬性映射。

使用下列程序設定 IAM Identity Center 與 SAML 2.0 應用程式服務提供者之間的 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。

設定您自己的 SAML 2.0 應用程式

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Applications (應用程式)。
3. 選擇客戶管理索引標籤。
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下，選擇我有想要設定的應用程式。
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 Identity Center 中繼資料下，執行下列動作：
 - a. 在 IAM Identity Center SAML 中繼資料檔案下，選擇下載以下載身分提供者中繼資料。
 - b. 在 IAM Identity Center 憑證下，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. (選用) 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[了解 IAM Identity Center 主控台下的應用程式屬性](#)。
11. 在應用程式中繼資料下，選擇手動輸入中繼資料值。然後，提供 Application ACS URL 和 Application SAML 對象值。
12. 選擇提交。系統會將您導向至您剛新增之應用程式的詳細資訊頁面。

信任的身分傳播概觀

信任的身分傳播是 IAM Identity Center 的一項功能，可讓的管理員根據 群組關聯等使用者屬性 AWS 服務 授予許可。透過信任的身分傳播，身分內容會新增至 IAM 角色，以識別請求存取 AWS 資源的使用者。此內容會傳播到其他內容 AWS 服務。

身分內容包含的資訊，AWS 服務 用於在收到存取請求時做出授權決策。此資訊包含識別請求者的中繼資料（例如，IAM Identity Center 使用者）、請求存取的 AWS 服務（例如，Amazon Redshift），以及存取範圍（例如，唯讀存取）。接收 AWS 服務 使用此內容，以及指派給使用者的任何許可，來授權存取其資源。

受信任身分傳播的優點

信任的身分傳播可讓 管理員使用您人力的公司身分，將許可 AWS 服務 授予 資源，例如資料。此外，他們可以透過查看服務日誌或 來稽核誰存取了哪些資料 AWS CloudTrail。如果您是 IAM Identity Center 管理員，其他 AWS 服務 管理員可能會要求您啟用信任的身分傳播。

啟用信任的身分傳播

啟用受信任身分傳播的程序包含下列兩個步驟：

1. 啟用 IAM Identity Center 並將現有的身分來源連接到 IAM Identity Center - 您將繼續管理現有身分來源中的人力資源身分；將其連接到 IAM Identity Center 會建立對人力資源的參考，在您的 AWS 服務 使用案例中所有人都可以共用。它也可供資料擁有者在未來使用案例使用。
2. 將 的使用案例中 AWS 服務 的 連接到 IAM Identity Center - AWS 服務 信任的身分傳播使用案例中每個 的管理員遵循個別服務文件中的指引，將服務連接到 IAM Identity Center。

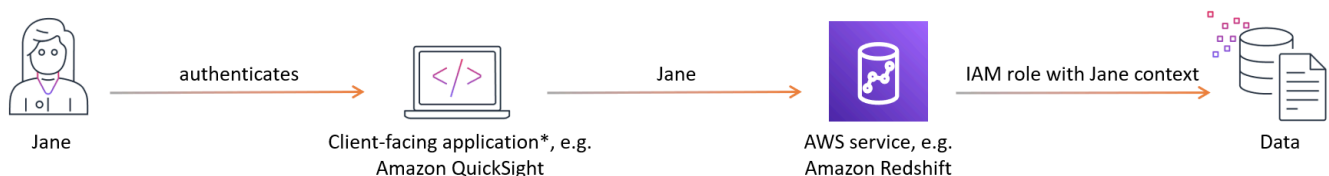
Note

如果您的使用案例涉及第三方或客戶開發的應用程式，您可以在驗證應用程式使用者和 IAM Identity Center 的身分提供者之間設定信任關係，以啟用信任的身分傳播。這可讓您的應用程式利用先前描述的信任身分傳播流程。

如需詳細資訊，請參閱[使用具有受信任權杖發行者的應用程式](#)。

受信任身分傳播的運作方式

下圖顯示受信任身分傳播的高階工作流程：



1. 使用者使用面向用戶端的應用程式進行身分驗證，例如 Quick。
2. 面向用戶端的應用程式會請求使用 AWS 服務 來查詢資料的存取權，並包含使用者的相關資訊。

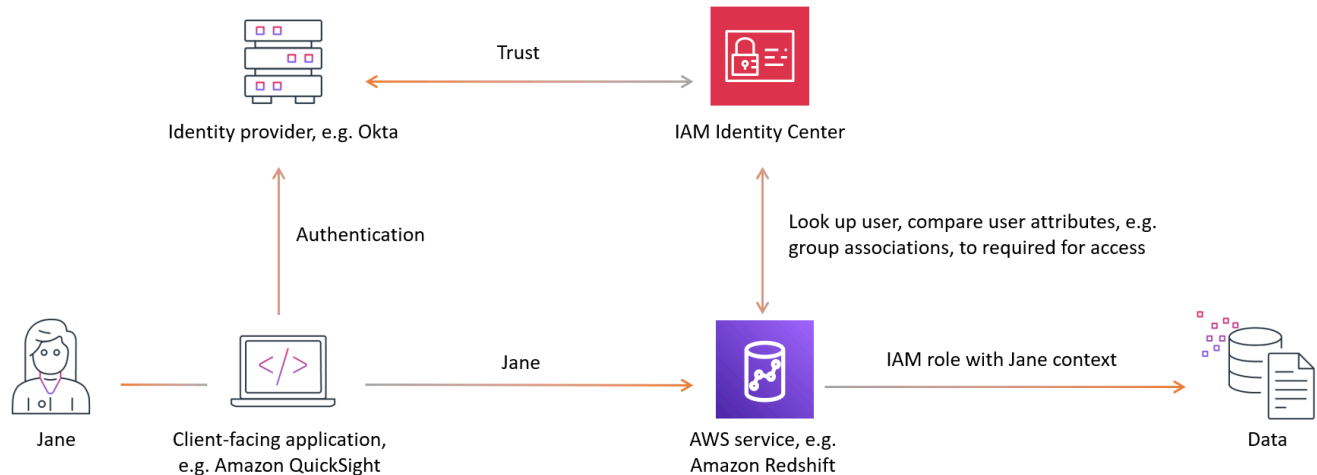
Note

有些信任的身分傳播使用案例涉及 AWS 服務 使用 服務驅動程式與 互動的工具。您可以在使用案例[指引中了解這是否適用於您的使用案例](#)。

3. 會向 AWS 服務 IAM Identity Center 驗證使用者身分，並比較使用者屬性，例如其群組關聯，以及存取所需的屬性。只要使用者或其群組具有必要的許可，就會 AWS 服務 授權存取權。

4. AWS 服務 可能會在 AWS CloudTrail 及其服務日誌中記錄使用者識別符。如需詳細資訊，請參閱服務文件。

下圖概述了信任的身分傳播工作流程中先前描述的步驟：



主題

- [先決條件和考量事項](#)
- [信任的身分傳播使用案例](#)
- [授權服務](#)

先決條件和考量事項

在您設定信任的身分傳播之前，請檢閱下列先決條件和考量事項。

主題

- [先決條件](#)
- [考量事項](#)
- [客戶受管應用程式的考量事項](#)

先決條件

若要使用信任的身分傳播，請確定您的環境符合下列先決條件：

- 啟用和佈建 IAM Identity Center

- 若要使用信任的身分傳播，您必須在使用者將存取 AWS 的應用程式和服務啟用 AWS 區域 的相同中啟用 IAM Identity Center。如需相關資訊，請參閱[啟用 IAM Identity Center](#)。
- 建議使用 IAM Identity Center Organization 執行個體 - 建議您使用在 管理帳戶中啟用的 IAM Identity Center [組織執行個體](#) AWS Organizations。您可以將 IAM Identity Center 組織執行個體的[管理委派](#)給成員帳戶。如果您選擇 IAM Identity Center [的帳戶執行個體](#)，您希望使用者透過信任 AWS 服務 的身分傳播存取的所有項目都必須位於啟用 IAM Identity Center AWS 帳戶 的相同位置。如需詳細資訊，請參閱[IAM Identity Center 的帳戶執行個體](#)。
- 將您現有的身分提供者連線至 IAM Identity Center，並將您的使用者和群組佈建至 IAM Identity Center。如需詳細資訊，請參閱[IAM Identity Center 身分來源教學課程](#)。
- 將受信任身分傳播使用案例中的 AWS 受管應用程式和服務連接到 IAM Identity Center。若要使用受信任的身分傳播，AWS 受管應用程式必須連線至 IAM Identity Center。

考量事項

設定和使用受信任身分傳播時，請注意下列考量：

- IAM Identity Center 的組織與帳戶執行個體
 - IAM Identity Center [的組織執行個體](#)將為您提供最大的控制和靈活性，將您的使用案例擴展到多個 AWS 帳戶、使用者和 AWS 服務。如果您無法使用組織執行個體，IAM Identity Center 的帳戶執行個體可能支援您的使用案例。若要進一步了解您的使用案例 AWS 服務 支援 IAM Identity Center 的帳戶執行個體，請參閱 [AWS 可與 IAM Identity Center 搭配使用的 受管應用程式](#)。
- 不需要多帳戶許可（許可集）
 - 信任的身分傳播不需要您設定[多帳戶許可](#)（許可集）。您可以啟用 IAM Identity Center，並僅用於受信任的身分傳播。

客戶受管應用程式的考量事項

即使您的使用者與非由 管理的用戶端應用程式互動 AWS，例如 Tableau或自訂開發的應用程式，您的人力資源也可以受益於受信任的身分傳播。這些應用程式的使用者可能無法在 IAM Identity Center 中佈建。為了讓使用者能夠順利辨識和授權存取 AWS 資源，IAM Identity Center 可讓您在身分提供者之間設定信任關係，以驗證使用者和 IAM Identity Center。如需詳細資訊，請參閱[使用具有受信任權杖發行者的應用程式](#)。

此外，為您的應用程式設定信任的身分傳播將需要：

- 您的應用程式必須使用 OAuth 2.0 架構進行身分驗證。信任的身分傳播不支援 SAML 2.0 整合。

- 您的應用程式必須由 IAM Identity Center 識別。遵循[使用案例](#)的特定指引。

信任的身分傳播使用案例

身為 IAM Identity Center 管理員，您可能需要協助設定使用者面向應用程式的受信任身分傳播 AWS 服務。若要支援此請求，您需要以下資訊：

- 您的使用者將與哪些面向用戶端的應用程式互動？
- 哪些 AWS 服務 用於查詢資料和授權存取資料？
- 何者 AWS 服務 授權存取資料？

在啟用不涉及第三方應用程式或自訂開發應用程式之受信任身分傳播使用案例時，您的角色是：

1. [啟用 IAM Identity Center](#)。
2. [將您現有的身分來源連接到 IAM Identity Center](#)。

這些使用案例的信任身分組態其餘步驟會在連線的 AWS 服務 和 應用程式中執行。連線 AWS 服務 或 應用程式的管理員應參閱各自的使用者指南，以取得完整的服務特定指引。

您在啟用涉及第三方應用程式或自訂開發應用程式之受信任身分傳播使用案例時所扮演的角色，包括身分來源[啟用 IAM Identity Center](#)的步驟和連線，以及：[IAM Identity Center 身分來源教學課程](#)

1. 設定您的身分提供者 (IdP) 與第三方或自訂開發應用程式的連線。
2. 讓 IAM Identity Center 識別第三方或自訂開發的應用程式。
3. 在 IAM Identity Center 中將您的 IdP 設定為信任的字符發行者。如需詳細資訊，請參閱[使用具有受信任權杖發行者的應用程式](#)。

已連線應用程式的管理員和 AWS 服務 應參閱各自的使用者指南，以取得完整的服務特定指引。

分析、資料湖和機器學習使用案例

您可以使用下列分析和機器學習服務來啟用受信任的傳播使用案例：

- Amazon Redshift - 如需指引，請參閱 [使用 Amazon Redshift 進行信任的身分傳播](#)。
- Amazon EMR - 如需指引，請參閱 [使用 Amazon EMR 進行信任的身分傳播](#)。
- Amazon Athena - 如需指引，請參閱 [使用 Amazon Athena 進行信任的身分傳播](#)。

- SageMaker Studio - 如需指引，請參閱 [使用 Amazon SageMaker Studio 進行信任的身分傳播](#)。

其他使用案例

您可以使用這些額外的 啟用 IAM Identity Center 和信任的身分傳播 AWS 服務：

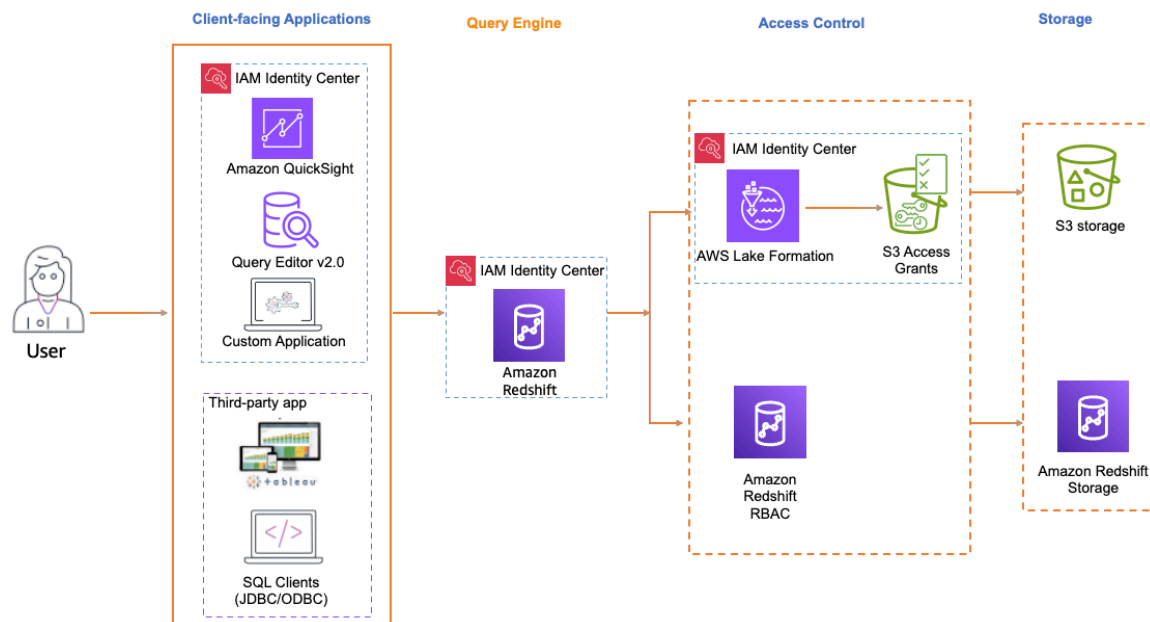
- Amazon Q Business - 如需指引，請參閱：
 - [使用 IAM Identity Center 的應用程式管理工作流程](#)。
 - [使用 IAM Identity Center 設定 Amazon Q Business 應用程式](#)。
 - [使用 IAM Identity Center 受信任身分傳播設定 Amazon Q Business](#)。
- Amazon OpenSearch Service - 如需指引，請參閱：
 - [Amazon OpenSearch Service 的 IAM Identity Center 受信任身分傳播支援](#)。
 - [使用 Amazon OpenSearch Service 的集中式 OpenSearch 使用者介面（儀表板）](#)。
- AWS Transfer Family - 如需指引，請參閱：
 - [Transfer Family Web 應用程式](#)。

主題

- [使用 Amazon Redshift 進行信任的身分傳播](#)
- [使用 Amazon EMR 進行信任的身分傳播](#)
- [使用 Amazon Athena 進行信任的身分傳播](#)
- [使用 Amazon SageMaker Studio 進行信任的身分傳播](#)

使用 Amazon Redshift 進行信任的身分傳播

啟用受信任身分傳播的步驟取決於您的使用者是否與 AWS 受管應用程式或客戶受管應用程式互動。下圖顯示用戶端應用程式 - AWS 受管或外部的受信任身分傳播組態 AWS，這些應用程式會使用 Amazon Redshift 或授權服務，例如 AWS Lake Formation 或 Amazon S3 提供的存取控制來查詢 Amazon Redshift 資料 Access Grants。



啟用可信任身分傳播至 Amazon Redshift 時，Redshift 管理員可以設定 Redshift 以 [自動建立](#) IAM Identity Center 的角色做為身分提供者、將 Redshift 角色映射至 IAM Identity Center 中的群組，並使用 [Redshift 角色型存取控制](#) 來授予存取權。

支援面向用戶端的應用程式

AWS 受管應用程式

下列 AWS 受管用戶端應用程式支援受信任的身分傳播至 Amazon Redshift：

- [Amazon Redshift Query Editor V2](#)
- [快速](#)

Note

如果您使用 Amazon Redshift Spectrum 存取 中的外部資料庫或資料表 AWS Glue Data Catalog，請考慮設定 [Lake Formation](#) 和 [Amazon S3 Access Grants](#) 以提供精細存取控制。

客戶受管應用程式

下列客戶受管應用程式支援 Amazon Redshift 的受信任身分傳播：

- Tableau 包括 Tableau Desktop、Tableau Server 和 Tableau Prep

- 若要為 的使用者啟用受信任身分傳播Tableau，請參閱 AWS 大數據部落格中的[使用 IAM Identity Center Okta與 Amazon Redshift 整合 Tableau 和](#)。
- SQL 用戶端 (DBeaver 和 DBVisualizer)
- 若要為 SQL 用戶端 (DBeaver 和) 的使用者啟用信任的身分傳播DBVisualizer，請參閱AWS 大數據部落格中的[使用 IAM Identity Center 整合身分提供者 \(IdP\) 與 Amazon Redshift 查詢編輯器 V2 和 SQL 用戶端，以實現無縫的單一登入。](#)

使用 Amazon Redshift 查詢編輯器 V2 設定受信任的身分傳播

下列程序會逐步解說如何實現從 Amazon Redshift 查詢編輯器 V2 到 Amazon Redshift 的受信任身分傳播。

先決條件

您必須先設定下列項目，才能開始使用本教學課程：

1. [啟用 IAM Identity Center](#)。建議使用[組織執行個體](#)。如需詳細資訊，請參閱[先決條件和考量事項](#)。
2. 將使用者和群組從您的身分來源佈建至 IAM Identity Center。

啟用受信任身分傳播包括 IAM Identity Center 主控台中 IAM Identity Center 管理員執行的任務，以及 Amazon Redshift 主控台中 Amazon Redshift 管理員執行的任務。

IAM Identity Center 管理員執行的任務

IAM Identity Center 管理員需要完成下列任務：

1. 在具有下列許可政策的 Amazon Redshift 叢集或無伺服器執行個體存在的帳戶中建立 [IAM 角色](#)。
如需詳細資訊，請參閱[建立 IAM 角色](#)。
 - 下列政策範例包含完成本教學課程所需的許可。若要使用此政策，請將範例政策中的 ##### 取代為您自己的資訊。如需其他指示，請參閱[建立政策](#)或[編輯政策](#)。

許可政策：

JSON

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

```

    {
      "Sid": "AllowRedshiftApplication",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowIDCPermissions",
      "Effect": "Allow",
      "Action": [
        "sso:DescribeApplication",
        "sso:DescribeInstance"
      ],
      "Resource": [
        "arn:aws:sso::instance/Your-IAM-Identity-Center-Instance
        ID",
        "arn:aws:sso::111122223333:application/Your-IAM-Identity-
Center-Instance-ID/*"
      ]
    }
  ]
}

```

信任政策：

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift-serverless.amazonaws.com",
          "redshift.amazonaws.com"
        ]
      }
    }
  ]
}

```



```

        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}

```

2. 在啟用 IAM Identity Center 的 AWS Organizations 管理帳戶中建立許可集。您將在下一個步驟中使用它，以允許聯合身分使用者存取 Redshift 查詢編輯器 V2。
 - a. 前往 IAM Identity Center 主控台，在多帳戶許可下，選擇許可集。
 - b. 選擇 Create permission set (建立許可集合)。
 - c. 選擇自訂許可集，然後選擇下一步。
 - d. 在AWS 受管政策下，選擇 **AmazonRedshiftQueryEditorV2ReadSharing**。
 - e. 在內嵌政策下，新增下列政策：

JSON

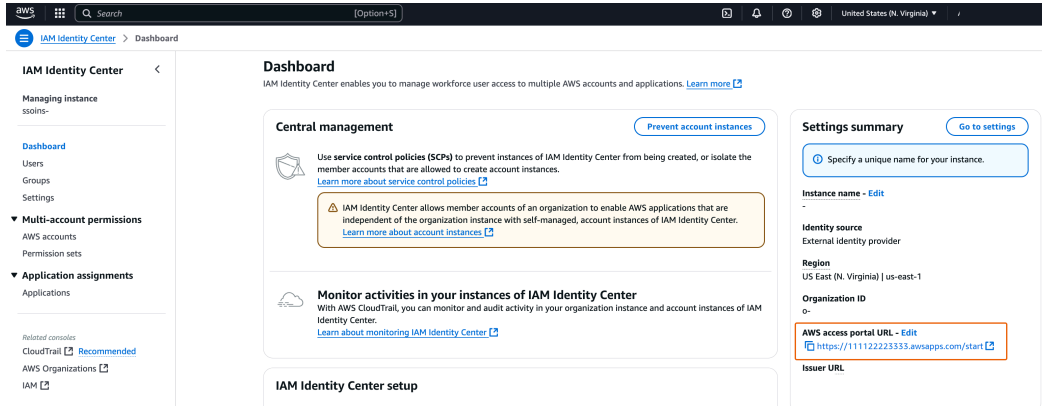
```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    }
  ]
}

```

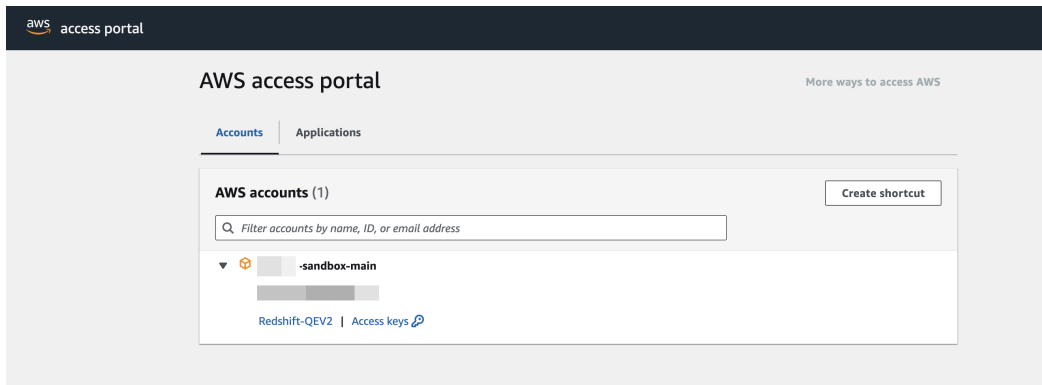
- f. 選取下一步，然後提供許可集名稱的名稱。例如 **Redshift-Query-Editor-V2**。

- g. 在轉送狀態 - 選用下，使用格式將預設轉送狀態設定為查詢編輯器 V2
URL : <https://your-region.console.aws.amazon.com/sqlworkbench/home>。
- h. 檢閱設定，然後選擇建立。
- i. 導覽至 IAM Identity Center Dashboard，然後從設定摘要區段複製 AWS 存取入口網站 URL。



- j. 開啟新的 Incognito 瀏覽器視窗並貼上 URL。

這將帶您前往 AWS 存取入口網站，確保您使用 IAM Identity Center 使用者登入。



如需許可集的詳細資訊，請參閱 [AWS 帳戶 使用許可集管理](#)。

3. 啟用聯合身分使用者存取 Redshift 查詢編輯器 V2。
 - a. 在 AWS Organizations 管理帳戶中，開啟 IAM Identity Center 主控台。
 - b. 在導覽窗格中的多帳戶許可下，選擇 AWS 帳戶。
 - c. 在 AWS 帳戶 頁面上，選取要為其指派存取權的 AWS 帳戶。
 - d. 選擇指派使用者或群組。
 - e. 在指派使用者和群組頁面上，選擇要為其建立許可集的使用者和/或群組。然後選擇下一步。
 - f. 在指派許可集頁面上，選擇您在上一個步驟中建立的許可集。然後選擇下一步。

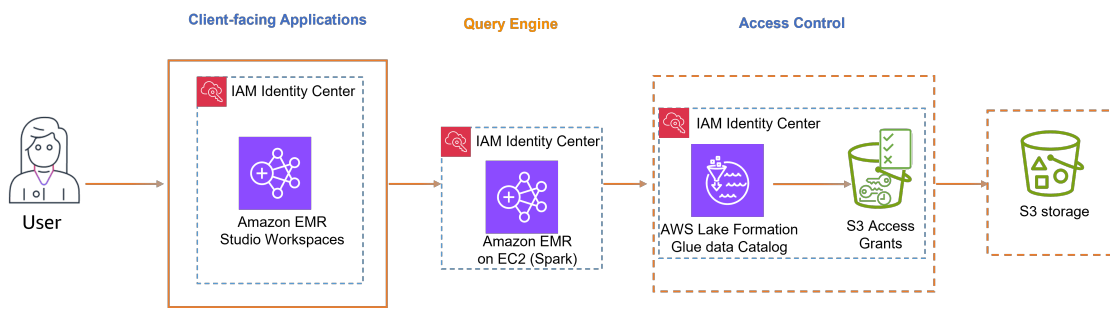
- g. 在檢閱和提交指派頁面上，檢閱您的選擇，然後選擇提交。

Amazon Redshift 管理員執行的任務

啟用 Amazon Redshift 的受信任身分傳播需要 Amazon Redshift 叢集管理員或 Amazon Redshift Serverless 管理員在 Amazon Redshift 主控台中執行許多任務。如需詳細資訊，請參閱AWS 大數據部落格中的[整合身分提供者 \(IdP\) 與使用 IAM Identity Center 的 Amazon Redshift 查詢編輯器 V2 和 SQL 用戶端，以實現無縫單一登入](#)。

使用 Amazon EMR 進行信任的身分傳播

下圖顯示使用 Amazon EMR on Amazon EC2 搭配 AWS Lake Formation 和 Amazon S3 提供之存取控制的 Amazon EMR Studio 的受信任身分傳播組態Access Grants。



支援面向用戶端的應用程式

- Amazon EMR Studio

若要啟用信任的身分傳播，請遵循下列步驟：

- 將 [Amazon EMR 設定為 Studio](#) Amazon EMR 叢集的面向用戶端應用程式。
- 使用 [在 Amazon EC2 上設定 Amazon EMR 叢集Apache Spark](#)。
- 建議：[AWS Lake Formation](#)和 [Amazon S3 Access Grants](#) 為 S3 中的 AWS Glue Data Catalog 和基礎資料位置提供精細的存取控制。

使用 Amazon EMR Studio 設定受信任的身分傳播

下列程序會逐步引導您在對執行的 Amazon Athena 工作群組或 Amazon EMR 叢集的查詢中，設定 Amazon EMR Studio以信任身分傳播Apache Spark。

先決條件

您必須先設定下列項目，才能開始使用本教學課程：

1. [啟用 IAM Identity Center](#)。建議使用[組織執行個體](#)。如需詳細資訊，請參閱[先決條件和考量事項](#)。
2. [將使用者和群組從您的身分來源佈建至 IAM Identity Center](#)。

若要從 Amazon EMR Studio 完成設定信任的身分傳播，EMR Studio 管理員必須執行下列步驟。

步驟 1. 建立 EMR Studio 所需的 IAM 角色

在此步驟中，Amazon EMR Studio 管理員會建立 IAM 服務角色，以及 EMR 的 IAM 使用者角色 Studio。

1. [建立 EMR Studio 服務角色](#) - EMR Studio 擔任此 IAM 角色，以安全地管理工作區和筆記本、連線至叢集，以及處理資料互動。
 - a. 導覽至 IAM 主控台 (<https://console.aws.amazon.com/iam/> : //) 並建立 IAM 角色。
 - b. 選取 AWS 服務做為信任的實體，然後選擇 Amazon EMR。連接下列政策以定義角色的許可和信任關係。

若要使用這些政策，請以您自己的資訊取代範例政策中的#####。如需其他指示，請參閱[建立政策](#)或[編輯政策](#)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectActions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
      ],
      "Condition": {
```

```

        "StringEquals": {
            "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
    },
    {
        "Sid": "BucketActions",
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket",
            "s3:GetEncryptionConfiguration"
        ],
        "Resource": [
            "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceAccount": "Your-AWS-Account-ID"
            }
        }
    }
]
}

```

如需所有服務角色許可的參考，請參閱 [EMR Studio 服務角色許可](#)。

2. [為 IAM Identity Center 身分驗證建立 EMR Studio 使用者角色](#) - 當使用者透過 IAM Identity Center 登入以管理工作區、EMR 叢集、任務、git 儲存庫時，EMR Studio 會擔任此角色。此角色用於啟動信任的身分傳播工作流程。

Note

EMR Studio 使用者角色不需要包含存取 AWS Glue Catalog. AWS Lake Formation permissions 中資料表 Amazon S3 位置的許可。註冊的湖位置將用於接收暫時許可。

下列範例政策可用於允許 EMR Studio 使用者使用 Athena 工作群組來執行查詢的角色。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-
policies": "true"
        }
      }
    },
    {
      "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*:*:security-group/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true",
          "ec2:CreateAction": "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid": "AllowSecretManagerListSecrets",
      "Action": [
        "secretsmanager:ListSecrets"
      ],
      "Resource": "*"
    }
  ]
}
```

```

        "Effect": "Allow"
    },
    {
        "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
        "Effect": "Allow",
        "Action": "secretsmanager:CreateSecret",
        "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true"
            }
        }
    },
    {
        "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
        "Effect": "Allow",
        "Action": "secretsmanager:TagResource",
        "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*"
    },
    {
        "Sid": "AllowPassingServiceRoleForWorkspaceCreation",
        "Action": "iam:PassRole",
        "Resource": [
            "arn:aws:iam::111122223333:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
        ],
        "Effect": "Allow"
    },
    {
        "Sid": "AllowS3ListAndLocationPermissions",
        "Action": [
            "s3:ListAllMyBuckets",
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws:s3:::*",
        "Effect": "Allow"
    },
    {
        "Sid": "AllowS3ReadOnlyAccessToLogs",
        "Action": [
            "s3:GetObject"
        ],

```



```

        "Resource": [
            "arn:aws:s3:::aws-logs-Your-AWS-Account-ID-Region/
elasticmapreduce/*"
        ],
        "Effect": "Allow"
    },
    {
        "Sid": "AllowAthenaQueryExecutions",
        "Effect": "Allow",
        "Action": [
            "athena:StartQueryExecution",
            "athena:GetQueryExecution",
            "athena:GetQueryResults",
            "athena:StopQueryExecution",
            "athena:ListQueryExecutions",
            "athena:GetQueryResultsStream",
            "athena:ListWorkGroups",
            "athena:GetWorkGroup",
            "athena:CreatePreparedStatement",
            "athena:GetPreparedStatement",
            "athena>DeletePreparedStatement"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowGlueSchemaManipulations",
        "Effect": "Allow",
        "Action": [
            "glue:GetDatabase",
            "glue:GetDatabases",
            "glue:GetTable",
            "glue:GetTables",
            "glue:GetPartition",
            "glue:GetPartitions"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowQueryEditorToAccessWorkGroup",
        "Effect": "Allow",
        "Action": "athena:GetWorkGroup",
        "Resource": "arn:aws:athena*:111122223333:workgroup*"
    },
    {

```

```

        "Sid": "AllowConfigurationForWorkspaceCollaboration",
        "Action": [
            "elasticmapreduce:UpdateEditor",
            "elasticmapreduce:PutWorkspaceAccess",
            "elasticmapreduce:DeleteWorkspaceAccess",
            "elasticmapreduce:ListWorkspaceAccessIdentities"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
            "StringEquals": {
                "elasticmapreduce:ResourceTag/creatorUserId":
"${aws:userId}"
            }
        },
    },
    {
        "Sid": "DescribeNetwork",
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups"
        ],
        "Resource": "*"
    },
    {
        "Sid": "ListIAMRoles",
        "Effect": "Allow",
        "Action": [
            "iam:ListRoles"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AssumeRole",
        "Effect": "Allow",
        "Action": [
            "sts:AssumeRole"
        ],
        "Resource": "*"
    }
]

```

}

下列信任政策允許 EMR Studio 擔任該角色：

Note

需要額外許可，才能利用 EMR Studio Workspaces 和 EMR Notebooks。如需詳細資訊，請參閱[建立 EMR Studio 使用者的許可政策](#)。

您可以透過以下連結找到更多資訊：

- [使用客戶管理政策定義自訂 IAM 許可](#)
- [EMR Studio 服務角色許可](#)

步驟 2. 建立和設定 EMR Studio

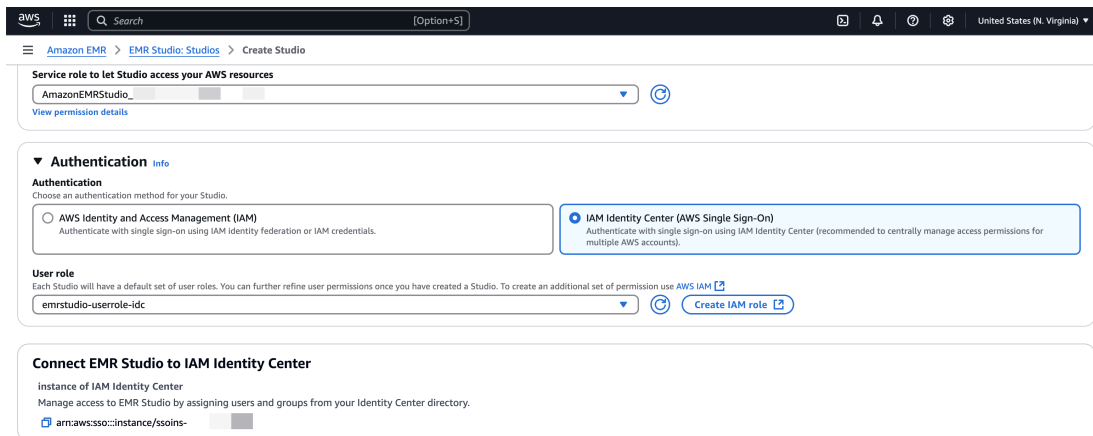
在此步驟中，您將在 EMR Studio 主控台中建立 Amazon EMR Studio，並使用您在 [步驟 1. 建立 EMR Studio 所需的 IAM 角色](#) 中建立的 IAM 角色。

1. 導覽至 EMR Studio 主控台，選取建立 Studio 和自訂設定選項。您可以建立新的 S3 儲存貯體或使用現有的儲存貯體。您可以勾選核取方塊，使用您自己的 KMS 金鑰加密工作區檔案。如需詳細資訊，請參閱[AWS Key Management Service](#)。

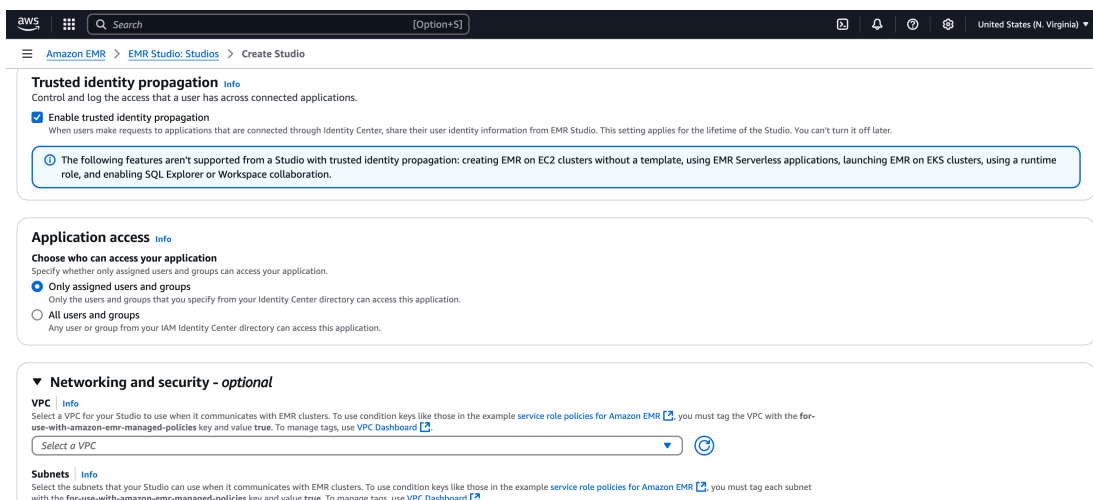
The screenshot shows the 'Create a Studio' page in the AWS EMR Studio console. The breadcrumb trail is 'Amazon EMR > EMR Studio: Studios > Create Studio'. The page is titled 'Create a Studio' with an 'Info' link. Under 'Setup options', there are three radio buttons: 'Interactive workloads', 'Batch jobs', and 'Custom' (which is selected). Below this is the 'Studio settings' section. It includes a 'Studio name' field with 'Studio_1' entered, a note 'Use up to 256 characters (alphanumeric, hyphens, or underscores).', an optional 'Description' field with the placeholder 'Describe the Studio', and a note '256 characters maximum'. The 'S3 location for Workspace storage' section has a note 'Specify an Amazon S3 location where Workspace work will be saved.' and two radio buttons: 'Create new bucket' (selected) and 'Select existing location'. Below this, it says 'We'll create a new bucket and use the location s3://aws-emr-studio-225989353012-us-east-1/1735848818523.' At the bottom, there is an unchecked checkbox for 'Encrypt Workspace files with your own AWS KMS key' and a note 'EMR Studio automatically uses the S3 location's encryption configuration. Choose this option if you want to override the S3 location's encryption configuration with your own AWS KMS key. This key information will not be editable past Studio creation.'

2. 在服務角色下，讓 Studio 存取您的資源，[步驟 1. 建立 EMR Studio 所需的 IAM 角色](#)從功能表中選取在 [步驟 1. 建立 EMR Studio 所需的 IAM 角色](#) 中建立的服務角色。

3. 在身分驗證下選擇 IAM Identity Center。選取在 中建立的使用者角色 [步驟 1. 建立 EMR Studio 所需的 IAM 角色](#)。



4. 勾選信任的身分傳播方塊。在應用程式存取區段下選擇僅指派的使用者和群組，這可讓您僅授予授權的使用者和群組存取此 Studio。
5. (選用) - 如果您搭配 EMR 叢集使用此 Studio，則可以設定 VPC 和子網路。



6. 檢閱所有詳細資訊，然後選取建立 Studio。
7. 設定 Athena WorkGroup 或 EMR 叢集之後，請登入 Studio 的 URL 以：
- 使用查詢編輯器執行 Athena 查詢。
 - 使用 Jupyter 筆記本在工作區中執行 Spark 任務。

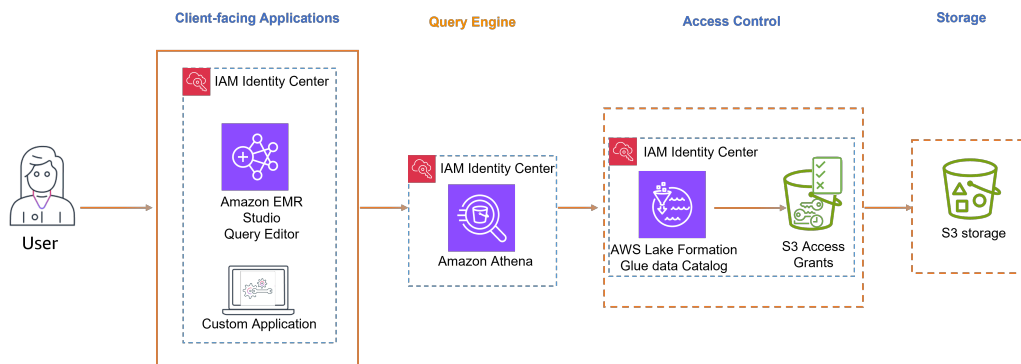
使用 Amazon Athena 進行信任的身分傳播

啟用受信任身分傳播的步驟取決於您的使用者是否與 AWS 受管應用程式或客戶受管應用程式互動。下圖顯示用戶端應用程式 - AWS 受管或外部的受信任身分傳播組態 AWS，這些應用程式使用 Amazon

Athena 透過 AWS Lake Formation 和 Amazon S3 提供的存取控制來查詢 Amazon S3 資料 Access Grants。

Note

- 使用 Amazon Athena 的信任身分傳播需要使用 Trino。
- 不支援透過 ODBC 和 JDBC 驅動程式連接到 Amazon Athena 的 Apache Spark 和 SQL 用戶端。



AWS 受管應用程式

下列 AWS 受管用戶端面向應用程式支援 Athena 的受信任身分傳播：

- Amazon EMR Studio

若要啟用信任的身分傳播，請遵循下列步驟：

- 將 [Amazon EMR 設定為 Studio](#) Athena 面向用戶端的應用程式。啟用受信任身分傳播時，需要 EMR Studio 中的查詢編輯器才能執行 Athena 查詢。
- [設定 Athena 工作群組](#)。
- [設定 AWS Lake Formation](#) 以根據 IAM Identity Center 中的使用者或群組啟用 AWS Glue 資料表的精細存取控制。
- [設定 Amazon S3 Access Grants](#) 以啟用對 S3 中基礎資料位置的暫時存取。

 Note

Lake Formation 和 Amazon S3 Access Grants 都需要對 Amazon S3 中的 Athena 查詢結果 AWS Glue Data Catalog 進行存取控制 Amazon S3。

客戶受管應用程式

若要為自訂開發應用程式的使用者啟用受信任身分傳播，請參閱 AWS 安全部落格中的 [使用受信任身分傳播以 AWS 服務 程式設計方式存取](#)。

使用 Amazon Athena 工作群組設定受信任的身分傳播

下列程序會逐步引導您設定 Amazon Athena 工作群組以進行信任的身分傳播。

先決條件

您必須先設定下列項目，才能開始使用本教學課程：

1. [啟用 IAM Identity Center](#)。建議使用[組織執行個體](#)。如需詳細資訊，請參閱[先決條件和考量事項](#)。
2. [將使用者和群組從您的身分來源佈建至 IAM Identity Center](#)。
3. 此組態需要 [Amazon EMR Studio](#)、[AWS Lake Formation](#) 和 [Amazon S3 Access Grants](#)。

使用 Athena 設定受信任的身分傳播

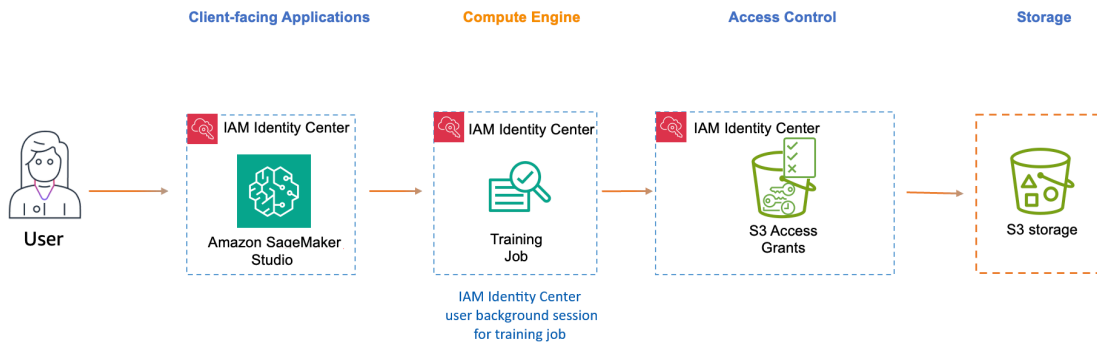
若要使用 Athena 設定信任的身分傳播，Athena 管理員必須：

1. 檢閱[使用啟用 IAM Identity Center 的 Athena 工作群組時的考量和限制](#)。
2. [建立已啟用 IAM Identity Center 的 Athena 工作群組](#)。

使用 Amazon SageMaker Studio 進行信任的身分傳播

[Amazon SageMaker Studio](#) 與 IAM Identity Center 整合，並支援[使用者背景工作階段](#)和信任的身分傳播。使用者背景工作階段允許使用者在 SageMaker Studio 上啟動長時間執行的任務，而不需要該使用者在任務執行時保持登入狀態。任務會立即在背景執行，並使用啟動任務之使用者的許可。即使使用者關閉電腦、IAM Identity Center 登入工作階段過期，或使用者登出 AWS 存取入口網站，任務仍可繼續執行。使用者背景工作階段的預設工作階段持續時間為 7 天，但您可以指定最長 90 天的持續時間。信任的身分傳播允許根據使用者的身分或群組成員資格，將精細存取提供給 AWS 資源，例如 Amazon S3 儲存貯體。

下圖顯示 SageMaker Studio 的受信任身分傳播組態，可存取存放在 Amazon S3 儲存貯體中的資料。IAM Identity Center 已啟用使用者背景工作階段，這可讓 SageMaker Studio 訓練任務在背景執行。訓練資料的存取控制由 Amazon S3 提供 Access Grants。



AWS 受管應用程式

下列 AWS 受管用戶端面向應用程式支援受信任的身分傳播：

- [Amazon SageMaker Studio](#)

若要啟用信任的身分傳播和使用者背景工作階段，請遵循下列步驟：

- [將 SageMaker Studio 設定為面向用戶端的應用程式。](#)
- [設定 Amazon S3 Access Grants](#) 以啟用暫時存取 Amazon S3 中的基礎資料位置。

使用 SageMaker Studio 設定受信任的身分傳播

下列程序會逐步引導您設定 SageMaker Studio 進行受信任身分傳播和使用者背景工作階段。

先決條件

您必須先完成下列任務，才能開始使用本教學課程：

1. [啟用 IAM Identity Center](#)。組織執行個體為必要項目。如需詳細資訊，請參閱[先決條件和考量事項](#)。
2. [將使用者和群組從您的身分來源佈建至 IAM Identity Center](#)。
3. [確認已在 IAM Identity Center 主控台中啟用使用者背景工作階段](#)。預設會啟用使用者背景工作階段，並將工作階段持續時間設定為 7 天。您可以變更此持續時間。

若要從 SageMaker Studio 設定信任的身分傳播，SageMaker Studio 管理員必須執行下列步驟。

步驟 1：在新的或現有的 SageMaker Studio 網域中啟用信任的身分傳播

SageMaker Studio 使用網域來組織使用者設定檔、應用程式及其相關資源。若要啟用受信任身分傳播，您必須建立 SageMaker Studio 網域或修改現有網域，如下列程序所述。

1. 開啟 SageMaker AI 主控台，導覽至網域，然後執行下列其中一項操作。

- 使用[組織設定](#)建立新的 SageMaker Studio 網域。

選擇為組織設定，然後執行下列動作：

- 選擇 AWS Identity Center 作為身分驗證方法。
- 選取為此網域上的所有使用者啟用受信任身分傳播核取方塊。
- 修改現有的 SageMaker Studio 網域。
- 選取使用 IAM Identity Center 進行身分驗證的現有網域。

Important

只有使用 IAM Identity Center 進行身分驗證的 SageMaker Studio 網域才支援信任的身分傳播。如果網域使用 IAM 進行身分驗證，則您無法變更身分驗證方法，因此無法啟用信任的身分傳播。

- [編輯網域設定](#)。編輯身分驗證和許可設定，以啟用信任的身分傳播。

2. 繼續進行[步驟 2：設定預設網域執行角色](#)。SageMaker Studio 網域的使用者需要此角色才能存取其他 AWS 服務，例如 Amazon S3。

步驟 2：設定預設網域執行角色和角色信任政策

網域執行角色是 SageMaker Studio 網域代表網域中的所有使用者擔任的 [IAM 角色](#)。您指派給此角色的許可決定 SageMaker Studio 可執行的動作。

1. 若要建立或選取網域執行角色，請執行下列其中一項操作：

- 使用 [組織的設定](#) 來建立或選取角色。
- 開啟 SageMaker AI 主控台，並遵循步驟 2：設定角色和 ML 活動中的主控台指導，以建立新的網域執行角色或選取現有角色。
- 完成其餘的設定步驟，以建立 SageMaker Studio 網域。

- 手動建立執行角色。
 - 開啟 IAM 主控台並[自行建立執行角色](#)。
2. [更新連接至網域執行角色的信任政策](#)，使其包含下列兩個動作：[sts:AssumeRole](#)和[sts:SetContext](#)。如需有關如何尋找 SageMaker Studio 網域執行角色的資訊，請參閱[取得網域執行角色](#)。

信任政策會指定可擔任角色的身分。此政策是允許 SageMaker Studio 服務擔任網域執行角色的必要政策。新增這兩個動作，使其在您的政策中顯示如下。

```
{

  "Version": "2012-10-17",

  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "sagemaker.amazonaws.com"
        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

步驟 3：驗證網域執行角色所需的 Amazon S3 Access Grant 許可

若要使用 Amazon S3 Access Grants，您必須將許可政策（做為內嵌政策或客戶受管政策）連接至包含下列許可的 SageMaker Studio 網域執行角色。

```
{

  "Version": "2012-10-17",

  "Statement": [
```

```
{
  "Effect": "Allow",
  "Action": [
    "s3:GetDataAccess",
    "s3:GetAccessGrantsInstanceForPrefix"
  ],
  "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
}
```

如果您沒有包含這些許可的政策，請遵循AWS Identity and Access Management 《使用者指南》中的[新增和移除 IAM 身分許可](#)中的指示。

步驟 4：將群組和使用者指派給網域

遵循[新增群組和使用者中的步驟](#)，將群組和使用者指派給 SageMaker Studio 網域。

步驟 5：設定 Amazon S3 Access Grants

若要設定 Amazon S3 Access Grants，請遵循[透過 IAM Identity Center 為受信任身分傳播設定 Amazon S3 Access Grants](#)中的步驟。使用step-by-step說明來完成下列任務：

1. 建立 Amazon S3 Access Grants 執行個體。
2. 在該執行個體中註冊位置。
3. 建立授予，以允許特定 IAM Identity Center 使用者或群組存取這些位置中指定的 Amazon S3 位置或子集（例如特定字首）。

步驟 6：提交 SageMaker 訓練任務並檢視使用者背景工作階段詳細資訊

在 SageMaker Studio 中，啟動新的 Jupyter 筆記本並提交訓練任務。任務執行時，請完成下列步驟以檢視工作階段資訊，並確認使用者背景工作階段內容處於作用中狀態。

1. 開啟 IAM Identity Center 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的使用者名稱。這會帶您前往包含使用者資訊的頁面。
4. 在使用者頁面上，選擇作用中工作階段索引標籤。作用中工作階段旁的括號中的數字表示此使用者的作用中工作階段數量。
5. 若要依使用工作階段之任務的 Amazon Resource Name (ARN) 搜尋工作階段，請在工作階段類型清單中，選擇使用者背景工作階段，然後在搜尋方塊中輸入任務 ARN。

以下是使用使用者背景工作階段的訓練任務如何在使用者的 Active 工作階段索引標籤中顯示的範例。

The screenshot shows the 'Active sessions (5)' page in the AWS IAM Identity Center console. At the top, there are tabs for Profile, Groups (0), AWS accounts, Applications, MFA devices (1), and Active sessions (5). Below the tabs, there's a section titled 'Active sessions (5)' with a refresh icon and an 'End sessions' button. A message states: 'You can end any of the active sessions in this list. The list shows all active sessions initiated by wei_zhang. [Learn more](#)'. Below this is a search bar with the placeholder 'Find sessions by client or used by' and a 'Session type' dropdown menu set to 'All'. A table with the following columns is displayed: Client, Session type, Used by, and IP address. One session is listed with a client of '-', session type of 'User background se...', and a 'Used by' value of 'arn:aws:sagemaker:us-west-2:777788889999:training-job/trustedidprop-trjob-12345a6b'.

步驟 7：檢視 CloudTrail 日誌以驗證 CloudTrail 中信任的身分傳播

啟用信任的身分傳播時，動作會顯示在 onBehalfOf 元素下的 CloudTrail 事件日誌中。userId 反映啟動訓練任務的 IAM Identity Center 使用者的 ID。下列 CloudTrail 事件會擷取信任身分傳播的程序。

```

      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AR0A123456789EXAMPLE:SageMaker",
        "arn": "arn:aws:sts::111122223333:assumed-role/SageMaker-
ExecutionRole-20250728T125817/SageMaker",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AR0A123456789EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/service-role/SageMaker-
ExecutionRole-20250728T125817",
            "accountId": "111122223333",
            "userName": "SageMaker-ExecutionRole-20250728T125817"
          },
          "attributes": {
            "creationDate": "2025-07-29T17:17:10Z",
            "mfaAuthenticated": "false"
          }
        },
        "onBehalfOf": {
          "userId": "2801d3e0-f0e1-707f-54e8-f558b19f0a10",
          "identityStoreArn": "arn:aws:identitystore::777788889999:identitystore/
d-1234567890"
        }
      },
    ],
  }

```

執行時期考量

如果管理員為長時間執行的訓練或處理任務設定了 `MaxRuntimeInSeconds`，而該任務低於使用者背景工作階段持續時間，則 SageMaker Studio 會執行任務至少為 `MaxRuntimeInSeconds` 或使用者背景工作階段持續時間。

如需 `MaxRuntimeInSeconds` 的詳細資訊，請參閱《Amazon SageMaker API 參考》中的 `CreateTrainingJob` [StoppingCondition](#) 參數指南。

授權服務

在所有[分析和資料湖使用案例中](#)，您可以使用下列方式實現精細存取控制：

- AWS Lake Formation - 如需指引，請參閱 [AWS Lake Formation 使用 IAM Identity Center 設定](#)。
- Amazon S3 Access Grants - 如需指引，請參閱 [使用 IAM Identity Center 設定 Amazon S3 Access Grants](#)。

AWS Lake Formation 使用 IAM Identity Center 設定

[AWS Lake Formation](#) 是一種受管服務，可簡化上資料湖的建立和管理 AWS。它可自動化資料收集、分類和安全性，提供集中式儲存庫來存放和分析各種資料類型。Lake Formation 提供精細的存取控制，並與各種 AWS 分析服務整合，讓組織能夠有效率地設定、保護並從其資料湖衍生洞見。

請依照下列步驟，使用 IAM Identity Center 和信任的身分傳播，讓 Lake Formation 根據使用者身分授予資料許可。

先決條件

您必須先設定下列項目，才能開始使用本教學課程：

- [啟用 IAM Identity Center](#)。建議使用[組織執行個體](#)。如需詳細資訊，請參閱[先決條件和考量事項](#)。

設定受信任身分傳播的步驟

1. 將 IAM Identity Center 與 整合 AWS Lake Formation，並遵循[將 Lake Formation 與 IAM Identity Center](#) 連接中的指引。

⚠ Important

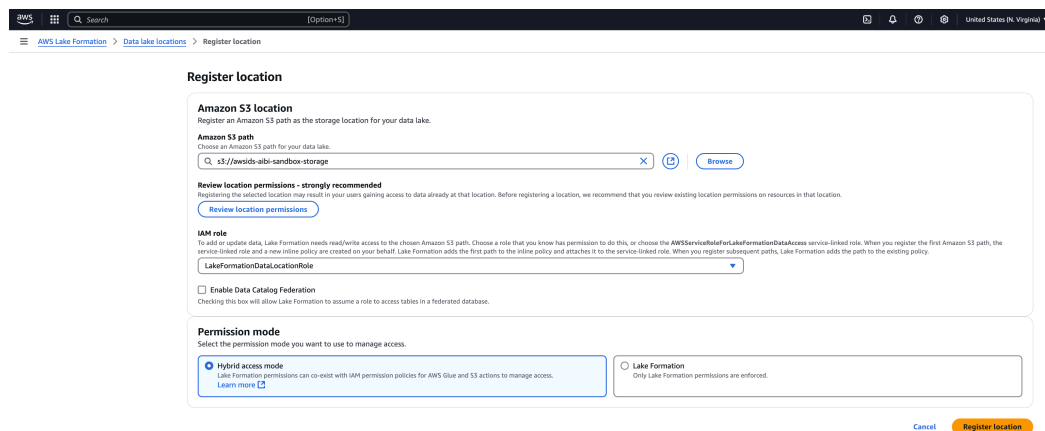
如果您沒有 AWS Glue Data Catalog 資料表，您必須建立這些資料表，才能使用 AWS Lake Formation 將存取權授予 IAM Identity Center 使用者和群組。如需詳細資訊，請參閱在 [中建立物件 AWS Glue Data Catalog](#)。

2. 註冊資料湖位置。

[註冊存放 Glue 資料表資料的 S3 位置](#)。藉由執行此操作，Lake Formation 將在查詢資料表時佈建對所需 S3 位置的臨時存取權，無需在服務角色（例如 WorkGroup 上設定的 Athena 服務角色）中包含 S3 許可。

- a. 在 AWS Lake Formation 主控台的導覽窗格中，導覽至管理區段下方的資料湖位置。選取註冊位置。

這將允許 Lake Formation 佈建具有存取 S3 資料位置必要許可的臨時 IAM 登入資料。



- b. 在 Amazon S3 路徑欄位中輸入資料表資料位置的 AWS Glue S3 路徑。Amazon S3
- c. 在 IAM 角色區段中，如果您想要搭配信任的身分傳播使用服務連結角色，請勿選取該角色。建立具有下列許可的個別角色。

若要使用這些政策，請以您自己的資訊取代範例政策中的#####。如需其他指示，請參閱[建立政策](#)或[編輯政策](#)。許可政策應授予路徑中指定之 S3 位置的存取權：

- i. 許可政策：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket/*"
      ]
    },
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3ListBucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket"
      ]
    },
    {
      "Sid": "LakeFormationDataAccessServiceRolePolicy",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

- ii. 信任關係：這應該包含 `sts:SectContext`，這是信任身分傳播的必要項目。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

 Note

精靈建立的 IAM 角色是服務連結角色，不包含 sts:SetContext。

- d. 建立 IAM 角色後，選取註冊位置。

使用 Lake Formation 跨 進行信任的身分傳播 AWS 帳戶

AWS Lake Formation 支援使用 [AWS Resource Access Manager \(RAM\)](#) 跨 共用資料表，AWS 帳戶並在授予者帳戶和承授者帳戶位於相同 AWS 區域、相同 中，並共用相同的 IAM Identity Center 組織執行個體時 AWS Organizations，使用受信任的身分傳播。如需詳細資訊，請參閱 [Lake Formation 中的跨帳戶資料共用](#)。

使用 IAM Identity Center 設定 Amazon S3 Access Grants

[Amazon S3 Access Grants](#) 提供將身分型精細存取控制授予 S3 位置的彈性。您可以使用 Amazon S3 Access Grants 將 Amazon S3 儲存貯體存取權直接授予公司使用者和群組。請依照下列步驟，Access Grants使用 IAM Identity Center 啟用 S3，並實現受信任的身分傳播。

先決條件

您必須先設定下列項目，才能開始使用本教學課程：

- [啟用 IAM Identity Center](#)。建議使用[組織執行個體](#)。如需詳細資訊，請參閱[先決條件和考量事項](#)。

透過 IAM Identity Center 設定受信任身分傳播的 S3 存取授權

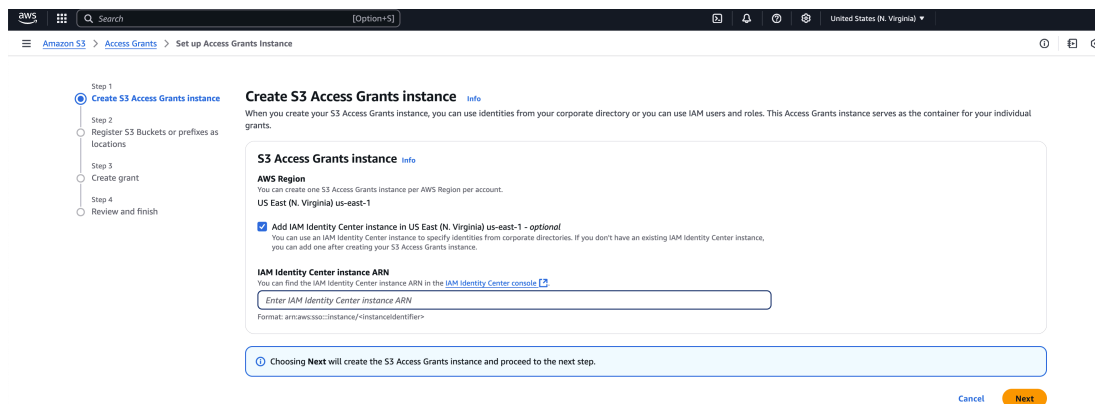
如果您已有已註冊位置的 Amazon S3 Access Grants執行個體，請依照下列步驟執行：

1. [建立 IAM Identity Center 執行個體的關聯](#)。
2. [建立授予](#)。

如果您Access Grants尚未建立 Amazon S3，請遵循下列步驟：

1. [建立 S3 Access Grants執行個體](#) - 您可以為每個執行個體建立一個 S3 Access Grants執行個體 AWS 區域。當您建立 S3 Access Grants執行個體時，請務必勾選新增 IAM Identity Center 執行個體方塊，並提供 IAM Identity Center 執行個體的 ARN。選取下一步。

下圖顯示 Amazon S3 Access Grants主控台中的建立 S3 Access Grants執行個體頁面：Amazon S3



2. 註冊位置 - 在帳戶中的 AWS 區域中[建立 Amazon S3 Access Grants執行個體](#)後，您會在該執行個體中[註冊 S3 位置](#)。S3 Access Grants位置會將預設 S3 區域 (S3://)、儲存貯體或字首映射至 IAM 角色。S3 Access Grants會擔任此 Amazon S3 角色，將臨時登入資料提供給存取該特定位置的承授者。您必須先在 S3 Access Grants執行個體中註冊至少一個位置，才能建立存取授權。

針對位置範圍，指定 `s3://`，其中包含該區域中的所有儲存貯體。這是大多數使用案例的建議位置範圍。如果您有進階存取管理使用案例，您可以將位置範圍設定為儲存貯體中的特定儲

存貯體 `s3://bucket` 或字首 `s3://bucket/prefix-with-path`。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[註冊位置](#)。

 Note

請確定您要授予存取權之 AWS Glue 資料表的 S3 位置包含在此路徑中。

此程序需要您設定位置的 IAM 角色。此角色應包含存取位置範圍的許可。您可以使用 S3 主控台精靈來建立角色。您需要在此 IAM 角色的政策中指定 S3 Access Grants 執行個體 ARN。S3 Access Grants 執行個體 ARN 的預設值為 `arn:aws:s3:Your-Region:Your-AWS-Account-ID:access-grants/default`。

下列範例許可政策會將 Amazon S3 許可授予您建立的 IAM 角色。之後的範例信任政策允許 S3 Access Grants 服務主體擔任 IAM 角色。

a. 許可政策

若要使用這些政策，請以您自己的資訊取代範例政策中的 `#####`。如需其他指示，請參閱[建立政策](#)或[編輯政策](#)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ],
      "Condition": {
```

```

        "StringEquals": {
            "aws:ResourceAccount": "111122223333"
        },
        "ArnEquals": {
            "s3:AccessGrantsInstanceArn": [
                "arn:aws:s3:::access-grants/instance-id"
            ]
        }
    },
    {
        "Sid": "ObjectLevelWritePermissions",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:PutObjectVersionAcl",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:AbortMultipartUpload"
        ],
        "Resource": [
            "arn:aws:s3:::*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceAccount": "111122223333"
            },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                ]
            }
        }
    },
    {
        "Sid": "BucketLevelReadPermissions",
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::*"
        ],
    },

```

```

        "Condition": {
            "StringEquals": {
                "aws:ResourceAccount": "111122223333"
            },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": [
                    "arn:aws:s3:::access-grants/instance-id"
                ]
            }
        },
        {
            "Sid": "OptionalKMSPermissionsForSSEEncryption",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}

```

b. 信任政策

在 IAM 角色信任政策中，授予 S3 存取授權服務 (access-grants.s3.amazonaws.com) 主體對您建立之 IAM 角色的存取權。若要完成此操作，您可以建立包含下列陳述式的 JSON 檔案。若要將信任政策新增至您的帳戶，請參閱[使用自訂信任政策建立角色](#)。

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567891011",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole",
                "sts:SetSourceIdentity"
            ]
        }
    ]
}

```

```

    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "111122223333",
        "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
      }
    }
  },
  {
    "Sid": "Stmt1234567891012",
    "Effect": "Allow",
    "Action": "sts:SetContext",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "111122223333",
        "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
      },
      "ForAllValues:ArnEquals": {
        "sts:RequestContextProviders":
        "arn:aws:iam::aws:contextProvider/IdentityCenter"
      }
    }
  }
]
}

```

建立 Amazon S3 存取授權

如果您有已註冊位置的 Amazon S3 Access Grants 執行個體，且已將 IAM Identity Center 執行個體與其建立關聯，則可以[建立授權](#)。在 S3 主控台建立授予頁面中，完成下列操作：

建立授與

1. 選取在上一個步驟中建立的位置。您可以新增子字首，以減少授予的範圍。子字首可以是 bucket、bucket/prefix 或 儲存貯體中的物件。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的 [Subprefix](#)。
2. 在許可和存取下，根據您的需求選取讀取和或寫入。

3. 在授予者類型中，選擇目錄身分表單 IAM Identity Center。
4. 提供 IAM Identity Center 使用者或群組 ID。您可以在 IAM Identity Center 主控台的使用者和群組 [區段下找到使用者和群組](#) IDs。選取下一步。
5. 在檢閱和完成頁面上，檢閱 S3 的設定，Access Grant 然後選取建立授予。

下圖顯示 Amazon S3 Access Grants 主控台內的建立授予頁面：

設定您自己的 OAuth 2.0 應用程式

信任的身分傳播可讓客戶受管應用程式代表使用者請求存取 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的現有使用者和群組成員資格授予存取權。使用者的身分、代表他們執行的動作和其他事件都會記錄在服務特定的日誌和 CloudTrail 事件中。

透過信任的身分傳播，使用者可以登入客戶受管應用程式，且該應用程式可以在存取資料的請求中傳遞使用者的身分 AWS 服務。

Important

若要存取 AWS 服務，客戶受管應用程式必須從 IAM Identity Center 外部的受信任權杖發行者取得權杖。信任的權杖發行者是建立簽章權杖的 OAuth 2.0 授權伺服器。這些字符授權應用程式啟動存取 AWS 服務（接收應用程式）的請求。如需詳細資訊，請參閱[使用具有受信任權杖發行者的應用程式](#)。

主題

- [設定客戶受管 OAuth 2.0 應用程式以進行受信任身分傳播](#)
- [指定信任的應用程式](#)
- [使用具有受信任權杖發行者的應用程式](#)

設定客戶受管 OAuth 2.0 應用程式以進行受信任身分傳播

若要設定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 Identity Center。使用下列程序將您的應用程式新增至 IAM Identity Center。

主題

- [步驟 1：選取應用程式類型](#)
- [步驟 2：指定應用程式詳細資訊](#)
- [步驟 3：指定身分驗證設定](#)
- [步驟 4：指定應用程式登入資料](#)
- [步驟 5：檢閱和設定](#)

步驟 1：選取應用程式類型

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Applications (應用程式)。
3. 選擇客戶管理索引標籤。
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下，選擇我有想要設定的應用程式。
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：指定應用程式詳細資訊](#)。

步驟 2：指定應用程式詳細資訊

1. 在指定應用程式詳細資訊頁面的應用程式名稱和描述下，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 Identity Center 使用者和群組存取應用程式。

應用程式圖磚可見性 – 只有直接或透過群組指派給應用程式的使用者，才能在 AWS 存取入口網站中檢視應用程式圖磚，前提是 AWS 存取入口網站中的應用程式可見性設定為可見。

- 不需要指派 – 允許所有授權的 IAM Identity Center 使用者和群組存取此應用程式。

應用程式圖磚可見性 – 除非 AWS 存取入口網站中的應用程式可見性設定為不可見，否則登入 AWS 存取入口網站的所有使用者都可看見應用程式圖磚。

3. 在 AWS 存取入口網站下，輸入使用者可存取應用程式的 URL，並指定應用程式圖磚是否會顯示在 AWS 存取入口網站中。如果您選擇不可見，則甚至沒有指派的使用者都可以檢視應用程式圖磚。
4. 在標籤（選用）下，選擇新增標籤，然後指定索引鍵和值的值（選用）。

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，然後繼續前往下一頁 [步驟 3：指定身分驗證設定](#)。

步驟 3：指定身分驗證設定

若要將支援 OAuth 2.0 的客戶受管應用程式新增至 IAM Identity Center，您必須指定信任的權杖發行者。受信任字符發行者是能建立簽章字符的 OAuth 2.0 授權伺服器。這些字符授權發起請求的應用程式 (請求應用程式) 存取 AWS 受管應用程式 (接收應用程式)。

1. 在指定身分驗證設定頁面的信任字符發行者下，執行下列其中一項操作：

- 若要使用現有的受信任權杖發行者：

選取您要使用的受信任權杖發行者名稱旁的核取方塊。

- 若要新增受信任權杖發行者：

1. 選擇建立信任的權杖發行者。
2. 新的瀏覽器索引標籤隨即開啟。請遵循 中的步驟 5 到 8 [如何將受信任權杖發行者新增至 IAM Identity Center 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，然後選取您剛新增的信任權杖發行者。
4. 在信任權杖發行者清單中，選取您剛新增之信任權杖發行者名稱旁的核取方塊。

選取信任的權杖發行者之後，即會顯示設定選取的信任權杖發行者區段。

2. 在設定選取的受信任權杖發行者下，輸入 Aud 宣告。Aud 宣告會識別受信任字符發行者所產生字符的目標對象（收件人）。如需詳細資訊，請參閱[Aud 宣告](#)。

- 若要防止使用者在使用此應用程式時重新驗證身分，請選取啟用重新整理字串授予。選取後，此選項會每 60 分鐘重新整理工作階段的存取字串，直到工作階段過期或使用者結束工作階段為止。
- 選擇下一步，然後繼續前往下一頁 [步驟 4：指定應用程式登入資料](#)。

步驟 4：指定應用程式登入資料

完成此程序中的步驟，以指定您的應用程式用來與信任的應用程式執行權杖交換動作的登入資料。這些登入資料用於以資源為基礎的政策。政策要求您指定具有執行政策中指定動作之許可的委託人。即使信任的應用程式位於相同的 中，您也必須指定委託人 AWS 帳戶。

Note

當您使用 政策設定許可時，只會授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。

此政策需要 [CreateTokenWithIAM](#) API 動作。如需此政策的詳細資訊，以及您可以視需要針對環境進行調整的範例，請參閱 [IAM Identity Center IAM Identity Center 的資源型政策範例](#)。

- 在指定應用程式登入資料頁面上，執行下列其中一項操作：
 - 若要快速指定一或多個 IAM 角色：
 - 選擇輸入一或多個 IAM 角色。
 - 在輸入 IAM 角色下，指定現有 IAM 角色的 Amazon Resource Name (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AWS Identity and Access Management 《使用者指南》中的[使用資源型政策和 IAM ARN 進行跨帳戶存取](#)。 [ARNs](#)

- 若要手動編輯政策（如果您指定非AWS 憑證則為必要）：
 - 選取編輯應用程式政策。
 - 在 JSON 文字方塊中輸入或貼上文字，以修改您的政策。
 - 解決政策驗證期間產生的任何安全警告、錯誤或一般警告。如需詳細資訊，請參閱 [《使用者指南》中的驗證 IAM 政策](#)。AWS Identity and Access Management
- 選擇下一頁並繼續前往下一頁 [步驟 5：檢閱和設定](#)。

步驟 5：檢閱和設定

1. 在檢閱和設定頁面上，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，然後進行必要的變更。
2. 完成後，請選擇新增應用程式。
3. 您新增的應用程式會出現在客戶受管應用程式清單中。
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 服務或信任的應用程式。這可讓使用者登入您的客戶受管應用程式，並存取信任應用程式中的資料。

如需詳細資訊，請參閱[指定信任的應用程式](#)。

指定信任的應用程式

[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信任 AWS 的服務或信任的應用程式。指定具有客戶受管應用程式使用者需要存取之資料 AWS 的服務。當您的使用者登入客戶受管應用程式時，該應用程式會將您的使用者身分傳遞給信任的應用程式。

使用下列程序來選取服務，然後為該服務指定要信任的個別應用程式。

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Applications (應用程式)。
3. 選擇客戶管理索引標籤。
4. 在客戶受管應用程式清單中，選取您要啟動存取請求的 OAuth 2.0 應用程式。這是您的使用者登入的應用程式。
5. 在詳細資訊頁面的用於身分傳播的可信應用程式下，選擇指定信任的應用程式。
6. 在設定類型下，選取個別應用程式並指定存取權，然後選擇下一步。
7. 在選取服務頁面上，選擇 AWS 具有客戶受管應用程式可信任之應用程式的服務，以進行身分傳播，然後選擇下一步。

您選取的服務會定義可信任的應用程式。您將在下一個步驟中選取應用程式。

8. 在選取應用程式頁面上，選擇個別應用程式，選取可接收存取請求之每個應用程式的核取方塊，然後選擇下一步。
9. 在設定存取頁面的組態方法下，執行下列其中一項操作：

- 選取每個應用程式的存取權 – 選取此選項，為每個應用程式設定不同的存取層級。選擇您要為其設定存取層級的應用程式，然後選擇編輯存取權。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。
- 將相同層級的存取套用至所有應用程式 – 如果您不需要為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，請選擇信任應用程式。

使用具有受信任權杖發行者的應用程式

受信任權杖發行者可讓您將受信任身分傳播與在 外部驗證的應用程式搭配使用 AWS。透過信任的權杖發行者，您可以授權這些應用程式代表其使用者提出請求，以存取 AWS 受管應用程式。

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

- [受信任權杖發行者概觀](#)
- [受信任權杖發行者的先決條件和考量事項](#)
- [JTI 宣告詳細資訊](#)
- [受信任權杖發行者組態設定](#)
- [設定信任的權杖發行者](#)
- [身分增強的 IAM 角色工作階段](#)

受信任權杖發行者概觀

受信任身分傳播提供一種機制，可讓在 外部驗證的應用程式使用受信任字符發行者，代表其使用者 AWS 提出請求。信任的權杖發行者是建立簽章權杖的 OAuth 2.0 授權伺服器。這些字符授權啟動請求（請求應用程式）的應用程式存取 AWS 服務（接收應用程式）。請求應用程式代表受信任字符發行者驗證的使用者啟動存取請求。信任的字符發行者和 IAM Identity Center 都知道這些使用者。

AWS 服務 接收請求會根據其使用者和群組成員資格管理對其資源的精細授權，如 Identity Center 目錄所示。AWS 服務 無法直接使用外部字符發行者的字符。

為了解決此問題，IAM Identity Center 為請求應用程式或請求應用程式使用的 AWS 驅動程式提供了一種方法，以將受信任字符發行者發出的字符交換為 IAM Identity Center 產生的字符。IAM Identity Center 產生的權杖是指對應的 IAM Identity Center 使用者。請求應用程式或驅動程式會使用新的字符來起始對接收應用程式的請求。由於新字符參考 IAM Identity Center 中的對應使用者，因此接收應用程式可以根據使用者或其群組成員資格來授權請求的存取權，如 IAM Identity Center 所示。

Important

選擇將 OAuth 2.0 授權伺服器新增為信任的權杖發行者是需要仔細考量的安全決策。僅選擇您信任的受信任權杖發行者來執行下列任務：

- 驗證字符中指定的使用者。
- 授權該使用者存取接收應用程式。
- 產生權杖，IAM Identity Center 可以交換 IAM Identity Center 建立的權杖。

受信任權杖發行者的先決條件和考量事項

在您設定信任的權杖發行者之前，請檢閱下列先決條件和考量事項。

- 受信任權杖發行者組態

您必須設定 OAuth 2.0 授權伺服器（信任的權杖發行者）。雖然信任的權杖發行者通常是您用來做為 IAM Identity Center 身分來源的身分提供者，但它不一定是。如需有關如何設定信任權杖發行者的資訊，請參閱相關身分提供者的文件。

Note

您最多可以設定 10 個受信任權杖發行者，以搭配 IAM Identity Center 使用，只要您將受信任權杖發行者中的每個使用者身分映射至 IAM Identity Center 中的對應使用者。

- 建立權杖的 OAuth 2.0 授權伺服器（受信任權杖發行者）必須具有 [OpenID Connect \(OIDC\)](#) 探索端點，IAM Identity Center 可用來取得公有金鑰來驗證權杖簽章。如需詳細資訊，請參閱 [OIDC 探索端點 URL（發行者 URL）](#)。
- 受信任權杖發行者發行的權杖

來自信任權杖發行者的權杖必須符合下列要求：

- 權杖必須使用 RS256 演算法以 [JSON Web 權杖 \(JWT\)](#) 格式簽署。

- 字符必須包含下列宣告：
 - [發行者](#) (iss) – 發行權杖的實體。此值必須與信任字符發行者 OIDC 探索端點 (發行者 URL) 中設定的值一致。
 - [主旨](#) (子) – 已驗證的使用者。
 - [對象](#) (aud) – 字符的預期收件人。這是權杖從 AWS 服務 IAM Identity Center 交換權杖後將會存取的。如需詳細資訊，請參閱[Aud 宣告](#)。
 - [過期時間](#) (exp) – 字符過期的時間。
- 字符可以是身分字符或存取字符。
- 字符必須具有可以唯一映射到一個 IAM Identity Center 使用者的屬性。

Note

Microsoft Entra ID 不支援將自訂簽署金鑰用於來自 JWTs。為了 Microsoft Entra ID 搭配信任的權杖發行者使用來自的權杖，您無法使用自訂簽署金鑰。

• 選用宣告

IAM Identity Center 支援 RFC 7523 中定義的所有選用宣告。如需詳細資訊，請參閱此 RFC [的第 3 節：JWT 格式和處理需求](#)。

例如，字符可以包含 [JTI \(JWT ID\) 宣告](#)。此宣告存在時，可防止具有相同 JTI 的權杖重複使用於權杖交換。如需 JTI 宣告的詳細資訊，請參閱 [JTI 宣告詳細資訊](#)。

• 使用受信任字符發行者的 IAM Identity Center 組態

您也必須啟用 IAM Identity Center、設定 IAM Identity Center 的身分來源，以及佈建對應至信任字符發行者目錄中使用者的使用者。

若要這樣做，您必須執行下列其中一項操作：

- 使用跨網域身分管理 (SCIM) 2.0 通訊協定，將使用者同步至 IAM Identity Center。
- 直接在 IAM Identity Center 中建立使用者。

JTI 宣告詳細資訊

如果 IAM Identity Center 收到交換 IAM Identity Center 已交換權杖的請求，則請求會失敗。若要偵測和防止權杖交換重複使用權杖，您可以包含 JTI 宣告。IAM Identity Center 會根據權杖中的宣告來防止權杖的重播。

並非所有 OAuth 2.0 授權伺服器都會將 JTI 宣告新增至權杖。有些 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限身分字符、僅限存取字符或兩者。如需詳細資訊，請參閱 OAuth 2.0 授權伺服器的文件。

如需有關建置交換字符的應用程式的資訊，請參閱 IAM Identity Center API 文件。如需有關設定客戶受管應用程式以取得和交換正確字符的資訊，請參閱應用程式的文件。

受信任權杖發行者組態設定

下列各節說明設定和使用信任權杖發行者所需的設定。

主題

- [OIDC 探索端點 URL \(發行者 URL\)](#)
- [屬性對應](#)
- [Aud 宣告](#)

OIDC 探索端點 URL (發行者 URL)

當您將受信任權杖發行者新增至 IAM Identity Center 主控台時，您必須指定 OIDC 探索端點 URL。此 URL 通常由其相對 URL 所參考 `/.well-known/openid-configuration`。在 IAM Identity Center 主控台中，此 URL 稱為發行者 URL。

Note

您必須貼上探索端點的 URL，直到 且不含 為止 `/.well-known/openid-configuration`。如果 URL `/.well-known/openid-configuration` 中包含 ，信任的字符發行者組態將無法運作。由於 IAM Identity Center 不會驗證此 URL，如果 URL 的格式不正確，信任的權杖發行者設定將會失敗，恕不另行通知。

OIDC 探索端點 URL 只能透過連接埠 80 和 443 存取。

IAM Identity Center 使用此 URL 來取得受信任字符發行者的其他資訊。例如，IAM Identity Center 使用此 URL 來取得驗證受信任字符發行者產生的字符所需的資訊。當您將受信任權杖發行者新增至 IAM Identity Center 時，您必須指定此 URL。若要尋找 URL，請參閱您用來為應用程式產生字符的 OAuth 2.0 授權伺服器提供者文件，或直接聯絡提供者尋求協助。

屬性對應

屬性映射可讓 IAM Identity Center 將信任字符發行者發出的字符中表示的使用者與 IAM Identity Center 中的單一使用者進行比對。當您將信任的字符發行者新增至 IAM Identity Center 時，必須指定屬性映射。此屬性映射用於由受信任權杖發行者產生的權杖中的宣告。宣告中的值用於搜尋 IAM Identity Center。搜尋使用指定的屬性來擷取 IAM Identity Center 中的單一使用者，該使用者將做為中的使用者。AWS 您選擇的宣告必須對應至 IAM Identity Center 身分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 Identity Center 身分存放區屬性：使用者名稱、電子郵件和外部 ID。您在 IAM Identity Center 中指定的屬性值對於每個使用者必須是唯一的。

Aud 宣告

aud 宣告會識別要為其指定權杖的對象（收件人）。當請求存取的應用程式透過未聯合 IAM Identity Center 的身分提供者進行身分驗證時，該身分提供者必須設定為信任的字符發行者。接收存取請求的應用程式（接收應用程式）必須將受信任字符發行者產生的字符交換為 IAM Identity Center 產生的字符。

如需如何在受信任權杖發行者註冊接收應用程式時取得 aud 宣告值的相關資訊，請參閱受信任權杖發行者的文件，或聯絡受信任權杖發行者管理員尋求協助。

設定信任的權杖發行者

若要為向 IAM Identity Center 外部驗證的應用程式啟用受信任身分傳播，一或多個管理員必須設定受信任權杖發行者。信任的權杖發行者是 OAuth 2.0 授權伺服器，會向啟動請求的應用程式（請求應用程式）發出權杖。這些字符授權這些應用程式代表其使用者向接收應用程式 (an) 發出請求 AWS 服務。

主題

- [協調管理角色和責任](#)
- [設定受信任權杖發行者的任務](#)
- [如何將受信任權杖發行者新增至 IAM Identity Center 主控台](#)
- [如何在 IAM Identity Center 主控台中檢視或編輯受信任權杖發行者設定](#)
- [使用受信任字符發行者的應用程式的設定程序和請求流程](#)

協調管理角色和責任

在某些情況下，單一管理員可能會執行設定信任字符發行者所需的所有必要任務。如果多個管理員執行這些任務，則需要密切協調。下表說明多個管理員如何協調以設定信任的字符發行者，並設定 AWS 服務來使用它。

Note

應用程式可以是與 IAM Identity Center 整合並支援受信任身分傳播的任何 AWS 服務。

如需詳細資訊，請參閱[設定受信任權杖發行者的任務](#)。

Role	執行這些任務	與 的座標
IAM Identity Center 管理員	將外部 IdP 做為信任的權杖發行者新增至 IAM Identity Center 主控台。 協助設定 IAM Identity Center 與外部 IdP 之間的正確屬性映射。 當信任的字符發行者新增至 IAM Identity Center 主控台時，通知 AWS 服務管理員。	外部 IdP (受信任字符發行者) 管理員 AWS 服務管理員
外部 IdP (受信任字符發行者) 管理員	設定外部 IdP 以發出權杖。 協助設定 IAM Identity Center 與外部 IdP 之間的正確屬性映射。 提供對象名稱 (Aud 宣告) 給 AWS 服務管理員。	IAM Identity Center 管理員 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權杖發行者。IAM Identity Center 管理員將其新增至 IAM Identity Center 主控台後，可在 AWS 服務主控台中看到信任的權杖發行者。 將 AWS 服務設定為使用信任的字符發行者。	IAM Identity Center 管理員 外部 IdP (受信任字符發行者) 管理員

設定受信任權杖發行者的任務

若要設定受信任權杖發行者，IAM Identity Center 管理員、外部 IdP（受信任權杖發行者）管理員和應用程式管理員必須完成下列任務。

Note

應用程式可以是與 IAM Identity Center 整合並支援受信任身分傳播的任何 AWS 服務。

1. 將信任權杖發行者新增至 IAM Identity Center – IAM Identity Center 管理員會使用 [IAM Identity Center 主控台或 API 新增信任權杖發行者](#)。APIs 此組態需要指定下列項目：
 - 受信任權杖發行者的名稱。
 - OIDC 探索端點 URL（在 IAM Identity Center 主控台中，此 URL 稱為發行者 URL）。探索端點只能透過連接埠 80 和 443 存取。
 - 使用者查詢的屬性映射。此屬性映射用於由受信任權杖發行者產生的權杖中的宣告。宣告中的值用於搜尋 IAM Identity Center。搜尋會使用指定的屬性來擷取 IAM Identity Center 中的單一使用者。
2. 將 AWS 服務連線至 IAM Identity Center – AWS 服務管理員必須使用應用程式或應用程式 APIs 的主控台，將應用程式連線至 IAM Identity Center。

將信任的字符發行者新增至 IAM Identity Center 主控台後，它也會在 AWS 服務主控台中顯示，並可供 AWS 服務管理員選取。

3. 設定權杖交換的使用 – 在 AWS 服務主控台中，AWS 服務管理員會將 AWS 服務設定為接受信任權杖發行者發行的權杖。這些字符會交換為 IAM Identity Center 產生的字符。這需要從步驟 1 指定受信任權杖發行者的名稱，以及對應至 AWS 服務的 Aud 宣告值。

信任的權杖發行者會將 Aud 宣告值放在其發行的權杖中，以表示權杖旨在供 AWS 服務使用。若要取得此值，請聯絡信任權杖發行者的管理員。

如何將受信任權杖發行者新增至 IAM Identity Center 主控台

在具有多個管理員的組織中，此任務是由 IAM Identity Center 管理員執行。如果您是 IAM Identity Center 管理員，您必須選擇要用作信任字符發行者的外部 IdP。

將受信任權杖發行者新增至 IAM Identity Center 主控台

1. 開啟 [IAM Identity Center 主控台](#)。

2. 選擇設定。
3. 在設定頁面上，選擇身分驗證索引標籤。
4. 在信任權杖發行者下，選擇建立信任權杖發行者。
5. 在設定外部 IdP 以發出信任權杖頁面上，在信任權杖發行者詳細資訊下，執行下列動作：
 - 對於發行者 URL，請指定外部 IdP 的 [OIDC 探索 URL](#)，該 IdP 將發行受信任身分傳播的權杖。IdP 您必須指定探索端點的 URL，直到 且不含 為止 `.well-known/openid-configuration`。外部 IdP 的管理員可以提供此 URL。

 Note

注意 此 URL 必須符合發行者 (iss) 宣告中針對受信任身分傳播發出的字符中的 URL。

- 針對受信任權杖發行者名稱，在 IAM Identity Center 和應用程式主控台中輸入名稱以識別此受信任權杖發行者。
6. 在映射屬性下，執行下列動作：
 - 針對身分提供者屬性，從清單中選擇屬性，以對應至 IAM Identity Center 身分存放區中的屬性。
 - 針對 IAM Identity Center 屬性，選取屬性映射的對應屬性。
 7. 在標籤（選用）下，選擇新增標籤、為金鑰指定值，以及為值選擇性指定值。

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. 完成建立信任的權杖發行者之後，請聯絡應用程式管理員，讓他們知道信任的權杖發行者名稱，以便確認信任的權杖發行者顯示在適當的主控台中。
 10. 應用程式管理員必須在適用的主控台中選取此受信任權杖發行者，以讓使用者從設定為受信任身分傳播的應用程式存取應用程式。

如何在 IAM Identity Center 主控台中檢視或編輯受信任權杖發行者設定

將受信任權杖發行者新增至 IAM Identity Center 主控台後，您可以檢視和編輯相關設定。

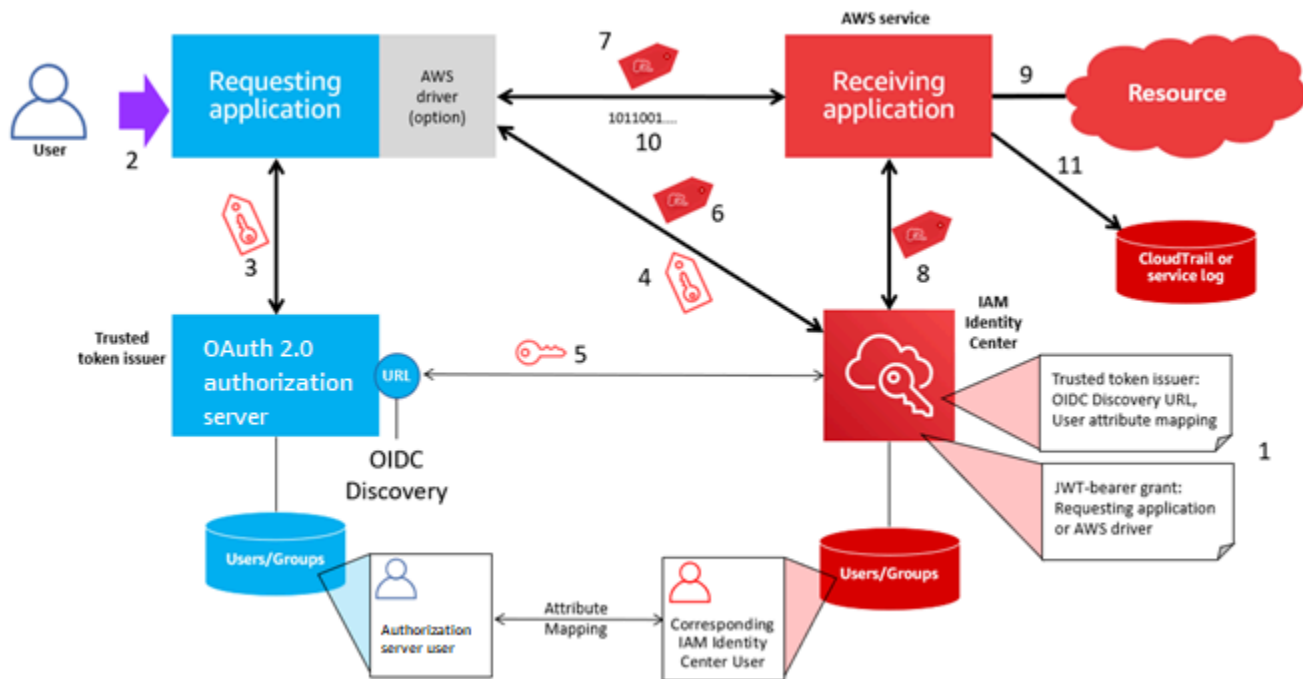
如果您打算編輯信任的權杖發行者設定，請記住，這樣做可能會導致使用者無法存取任何設定為使用信任權杖發行者的應用程式。為了避免中斷使用者存取，建議您在編輯設定之前，先針對設定為使用信任字串發行者的任何應用程式，與管理員進行協調。

在 IAM Identity Center 主控台中檢視或編輯受信任權杖發行者設定

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分驗證索引標籤。
4. 在信任權杖發行者下，選取您要檢視或編輯的信任權杖發行者。
5. 選擇動作，然後選擇編輯。
6. 在編輯信任的字符發行者頁面上，視需要檢視或編輯設定。您可以編輯信任的權杖發行者名稱、屬性映射和標籤。
7. 選擇儲存變更。
8. 在編輯信任的字符發行者對話方塊中，系統會提示您確認是否要進行變更。選擇確認。

使用受信任字符發行者的應用程式的設定程序和請求流程

本節說明使用受信任權杖發行者進行受信任身分傳播的應用程式的設定程序和請求流程。下圖提供此程序的概觀。



下列步驟提供此程序的其他資訊。

1. 設定 IAM Identity Center 和接收 AWS 受管應用程式，以使用信任的權杖發行者。如需相關資訊，請參閱[設定受信任權杖發行者的任務](#)。

2. 請求流程會在使用者開啟請求應用程式時開始。
3. 請求應用程式會向信任的權杖發行者請求權杖，以起始對接收 AWS 受管應用程式的請求。如果使用者尚未進行身分驗證，此程序會觸發身分驗證流程。字符包含下列資訊：
 - 使用者的主體 (Sub)。
 - IAM Identity Center 用來在 IAM Identity Center 中查詢對應使用者的屬性。
 - 對象（對象）宣告，其中包含信任權杖發行者與接收 AWS 受管應用程式相關聯的值。如果有其他宣告，IAM Identity Center 不會使用這些宣告。
4. 請求應用程式或其使用的 AWS 驅動程式會將字符傳遞給 IAM Identity Center，並請求將字符交換為 IAM Identity Center 產生的字符。如果您使用 AWS 驅動程式，您可能需要為此使用案例設定驅動程式。如需詳細資訊，請參閱相關 AWS 受管應用程式的文件。
5. IAM Identity Center 使用 OIDC Discovery 端點來取得可用於驗證字符真實性的公有金鑰。IAM Identity Center 接著會執行下列動作：
 - 驗證權杖。
 - 搜尋 Identity Center 目錄。若要這樣做，IAM Identity Center 會使用字符中指定的映射屬性。
 - 驗證使用者是否有權存取接收應用程式。如果 AWS 受管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以群組為基礎的指派，否則請求會被拒絕。如果 AWS 受管應用程式設定為不需要使用者和群組指派，則處理會繼續進行。

 Note

AWS 服務具有預設設定組態，可判斷使用者和群組是否需要指派。如果您打算將它們與信任的身分傳播搭配使用，建議您不要修改這些應用程式的需要指派設定。即使您已設定允許使用者存取特定應用程式資源的精細許可，修改需要指派設定仍可能導致意外行為，包括中斷使用者存取這些資源。

- 確認請求應用程式已設定為使用接收 AWS 受管應用程式的有效範圍。
6. 如果先前的驗證步驟成功，IAM Identity Center 會建立新的權杖。新權杖是不透明（加密）權杖，其中包含 IAM Identity Center 中對應使用者的身分、接收 AWS 受管應用程式的對象 (Aud)，以及請求應用程式在向接收 AWS 受管應用程式提出請求時可以使用的範圍。
 7. 請求應用程式或其使用的驅動程式會啟動資源請求給接收應用程式，並將 IAM Identity Center 產生的字符傳遞給接收應用程式。
 8. 接收應用程式會呼叫 IAM Identity Center，以取得使用者身分和字符中編碼的範圍。它也可能請求從 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請求的應用程式資源。

10.如果使用者有權存取請求的應用程式資源，接收應用程式會回應請求。

11.使用者的身分、代表他們執行的動作和其他事件都會記錄在接收應用程式日誌和 CloudTrail 事件中。記錄此資訊的特定方式會根據應用程式而有所不同。

身分增強的 IAM 角色工作階段

[AWS Security Token Service \(STS\)](#) 可讓應用程式取得身分增強的 IAM 角色工作階段。身分增強型角色工作階段具有新增的身分內容，可將使用者識別符帶到 AWS 服務 其呼叫的。AWS 服務 可以在 IAM Identity Center 中查詢使用者的群組成員資格和屬性，並使用它們來授權使用者存取 資源。

AWS 應用程式透過向 AWS STS [AssumeRole](#) API 動作提出請求，並在請求的 `ProvidedContexts` 參數中將內容聲明與使用者的識別符 (`userId`) 傳遞給，來取得身分增強型角色工作階段 `AssumeRole`。內容聲明是從回應 SSO OIDC 對 的請求而收到的 `idToken` 宣告中取得 [CreateTokenWithIAM](#)。當 AWS 應用程式使用身分增強型角色工作階段來存取資源時，CloudTrail 會記錄 `userId`、起始工作階段和採取的動作。如需詳細資訊，請參閱 [身分增強 IAM 角色工作階段記錄](#)。

主題

- [身分增強型 IAM 角色工作階段的類型](#)
- [身分增強 IAM 角色工作階段記錄](#)

身分增強型 IAM 角色工作階段的類型

AWS STS 可以建立兩種不同類型的身分增強 IAM 角色工作階段，取決於提供給 `AssumeRole` 請求的內容聲明。從 IAM Identity Center 取得 ID 字符的應用程式可以將 `sts:identity_context` (建議) 或 `sts:audit_context` (支援回溯相容性) 新增至 IAM 角色工作階段。身分增強的 IAM 角色工作階段只能具有其中一個內容聲明，不能同時具有兩者。

使用 建立的身分增強 IAM 角色工作階段 `sts:identity_context`

當身分增強型角色工作階段包含稱為 `sts:identity_context` AWS 服務的時，會判斷資源授權是以角色工作階段中代表的使用者為基礎，還是以角色為基礎。AWS 服務 支援以使用者為基礎的授權提供應用程式的管理員控制項，以將存取權指派給使用者或使用者為成員的群組。

AWS 服務 不支援使用者型授權的 會忽略 `sts:identity_context`。CloudTrail 會使用角色採取的所有動作來記錄 IAM Identity Center 使用者的 `userId`。如需詳細資訊，請參閱 [身分增強 IAM 角色工作階段記錄](#)。

若要從中取得這種類型的身分增強型角色工作階段 AWS STS，應用程式會使用 請求參數，在 [AssumeRole](#) `ProvidedContexts` 請求中提供 `sts:identity_context` 欄位的值。使用 `arn:aws:iam::aws:contextProvider/IdentityCenter` 做為 的值 `ProviderArn`。

如需授權行為的詳細資訊，請參閱接收的文件 AWS 服務。

使用 建立的身分增強 IAM 角色工作階段 `sts:audit_context`

在過去，`sts:audit_context` 用來讓 AWS 服務 記錄使用者身分，而不用它來做出授權決策。AWS 服務 現在可以使用單一內容 - `sts:identity_context` - 來達成此目的，以及做出授權決策。我們建議在所有信任身分傳播的新部署 `sts:identity_context` 中使用。

身分增強 IAM 角色工作階段記錄

AWS 服務 使用身分增強 IAM 角色工作階段向 提出請求時，使用者的 IAM Identity Center `userId` 會記錄在 `OnBehalfOf` 元素中的 `CloudTrail`。CloudTrail 中記錄事件的方式會根據 而有所不同 AWS 服務。並非所有 都會 AWS 服務 記錄 `onBehalfOf` 元素。

以下是如何使用身分增強型角色工作階段向 AWS 服務 提出的請求在 `CloudTrail` 中記錄的範例。

```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROEXAMPLE:MyRole",
  "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
  "accountId": "111111111111",
  "accessKeyId": "ASIAEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROEXAMPLE",
      "arn": "arn:aws:iam::111111111111:role/MyRole",
      "accountId": "111111111111",
      "userName": "MyRole"
    },
    "attributes": {
      "creationDate": "2023-12-12T13:55:22Z",
      "mfaAuthenticated": "false"
    }
  },
  "onBehalfOf": {
    "userId": "11111111-1111-1111-1111-111111111111",
    "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/d-1111111111"
```

```
}  
}
```

輪換 IAM Identity Center 憑證

IAM Identity Center 使用憑證來設定 IAM Identity Center 與您應用程式服務提供者之間的 SAML 信任關係。當您在 IAM Identity Center 中新增應用程式時，會自動建立 IAM Identity Center 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 Identity Center 憑證有效期為五年。

身為 IAM Identity Center 管理員，有時您需要將較舊的憑證取代為指定應用程式較新的憑證。例如，您可能需要在憑證上的過期日期接近時取代憑證。使用較新的憑證取代較舊憑證的程序稱為憑證輪換。

輪換憑證之前的考量事項

在您開始在 IAM Identity Center 中輪換憑證的程序之前，請考慮下列事項：

- 認證輪換程序需要您重新建立 IAM Identity Center 與服務提供者之間的信任。若要重新建立信任，請使用 中提供的程序[輪換 IAM Identity Center 憑證](#)。
- 使用服務供應商更新憑證可能會對您的使用者造成暫時性服務中斷，直到成功重新建立信任為止。如果可能，請在尖峰時段仔細規劃此操作。

輪換 IAM Identity Center 憑證

輪換 IAM Identity Center 憑證是一個包含下列項目的多步驟程序：

- 產生新憑證
- 將新憑證新增至服務提供者的網站
- 將新憑證設定為作用中
- 刪除非作用中憑證

依照下列順序使用下列所有程序，以完成指定應用程式的憑證輪換程序。

步驟 1：產生新的憑證

您產生的新 IAM Identity Center 憑證可以設定為使用下列屬性：

- 有效期間 – 指定新 IAM Identity Center 憑證過期之前分配的時間（以月為單位）。
- 金鑰大小 – 決定金鑰必須搭配其密碼編譯演算法使用的位元數。您可以將此值設定為 1024 位元 RSA 或 2048 位元 RSA。如需金鑰大小如何在密碼編譯中運作的一般資訊，請參閱[金鑰大小](#)。
- 演算法 – 指定 IAM Identity Center 在簽署 SAML 聲明/回應時所使用的演算法。您可以盡可能使用 SHA-256 將此值設定為 SHA-1 或 SHA-256。AWS recommends，除非您的服務供應商需要 SHA-1。SHA-256 如需密碼編譯演算法運作方式的一般資訊，請參閱[公有金鑰密碼編譯](#)。

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Applications (應用程式)。
3. 在應用程式清單中，選擇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 Identity Center 中繼資料下，選擇管理憑證。如果您沒有組態索引標籤或組態設定不可用，則不需要輪換此應用程式的憑證。
5. 在 IAM Identity Center 憑證頁面上，選擇產生新憑證。
6. 在產生新的 IAM Identity Center 憑證對話方塊中，指定有效期間、演算法和金鑰大小的適當值。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

當您將新憑證上傳到服務提供者時，您的使用者可能無法進行身分驗證。若要修正這種情況，請將新憑證設定為作用中，如下一個步驟所述。

1. 在 [IAM Identity Center 主控台](#) 中，選擇您剛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，然後遵循特定應用程式服務供應商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

應用程式最多可以指派兩個憑證給它。IAM Identity Center 將使用設定為作用中的憑證來簽署所有 SAML 聲明。

1. 開啟 [IAM Identity Center 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 Identity Center 中繼資料下，選擇管理憑證。
5. 在 IAM Identity Center 憑證頁面上，選取您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. 在將選取的憑證設為作用中對話方塊中，確認您了解將憑證設定為作用中可能需要您重新建立信任，然後選擇設為作用中。

步驟 4：刪除舊憑證

使用下列程序來完成應用程式的憑證輪換程序。您只能刪除處於非作用中狀態的憑證。

1. 開啟 [IAM Identity Center 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 Identity Center 中繼資料下，選擇管理憑證。
5. 在 IAM Identity Center 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。

憑證過期狀態指示燈

在 IAM Identity Center 主控台中，應用程式頁面會在每個應用程式的屬性中顯示狀態指示燈圖示。這些圖示會顯示在清單中每個憑證旁的過期日期欄中。以下說明 IAM Identity Center 用來判斷每個憑證顯示哪些圖示的條件。

- 紅色 – 表示憑證目前已過期。
- 黃色 – 表示憑證將在 90 天內過期。
- 綠色 - 表示憑證目前有效，並將再維持有效至少 90 天。

檢查憑證的狀態

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇 Applications (應用程式)。
3. 在應用程式清單中，檢閱清單中憑證的狀態，如 上的過期資料欄所示。

了解 IAM Identity Center 主控台中的應用程式屬性

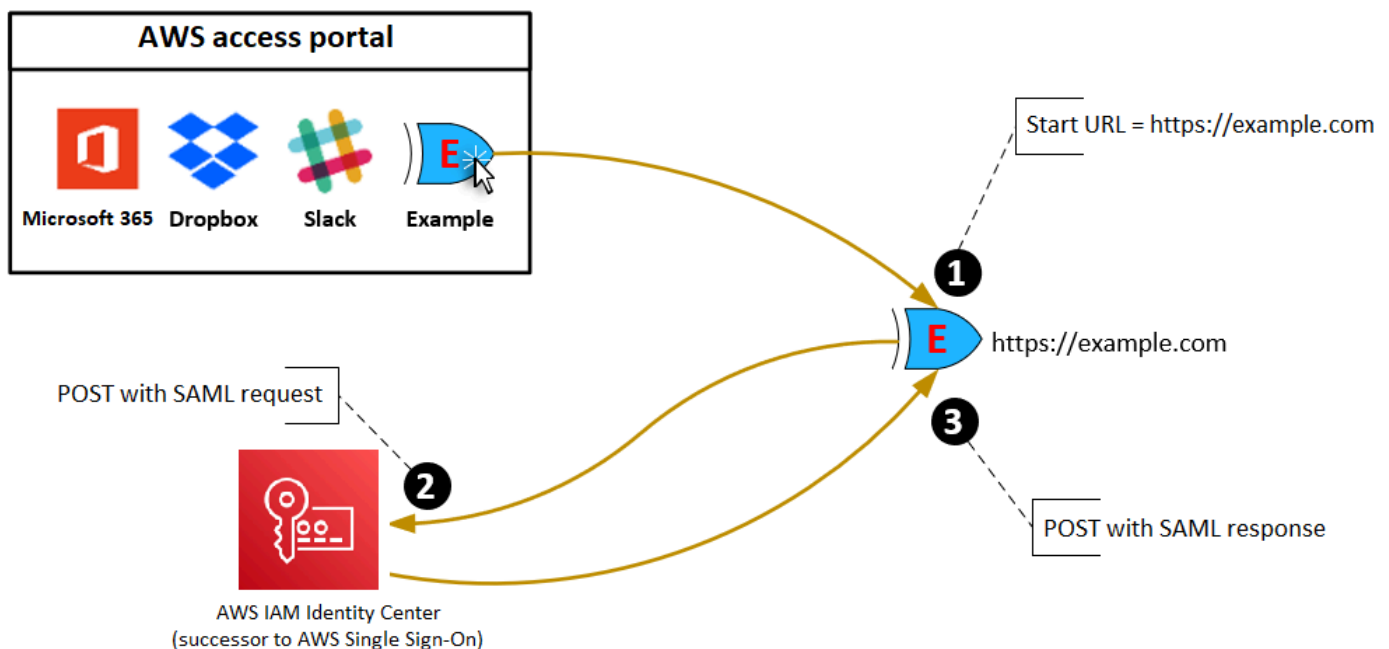
在 IAM Identity Center 中，您可以透過設定應用程式啟動 URL、轉送狀態和工作階段持續時間來自訂使用者體驗。

應用程式啟動 URL

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。

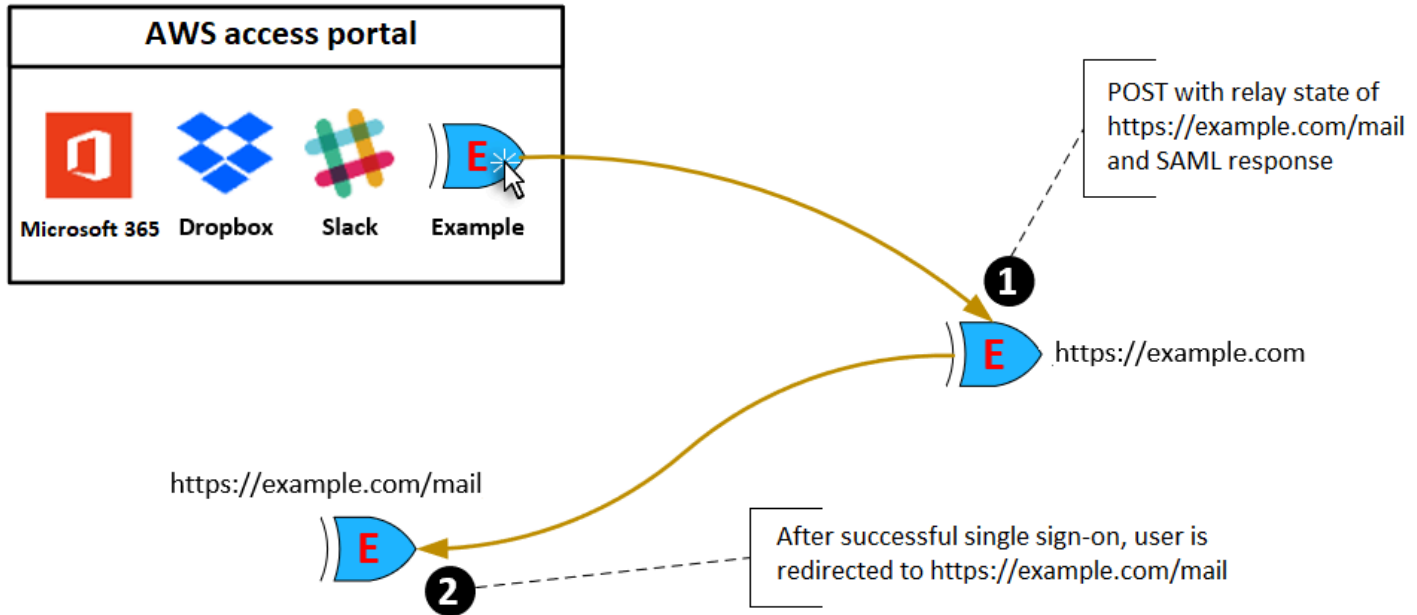
下列步驟和圖表說明當使用者在 AWS 存取入口網站中選擇應用程式時，應用程式啟動 URL 身分驗證工作流程：

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. 應用程式會將 HTML POST 具有的 SAMLRequest 傳送至 IAM Identity Center。
3. 然後，IAM Identity Center 會將 HTML POST 具有 SAMLResponse 的 傳回應用程式。



轉送狀態

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。設定應用程式屬性後，IAM Identity Center 會將轉送狀態值與 SAML 回應一起傳送至應用程式。



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 聲明的元素 `SessionNotOnOrAfter` 的日期。 `saml2:AuthNStatement`

應用程式可以透過下列其中一種方式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。應用程式可能會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 Identity Center 主控台中指派使用者對應用程式的存取權

您可以將使用者單一登入存取權指派給應用程式目錄中的 SAML 2.0 應用程式或自訂 SAML 2.0 應用程式。

群組指派的考量事項：

- 將存取權直接指派給群組。為了協助簡化存取許可的管理，建議您將存取權直接指派給群組，而非個別使用者。使用群組，您可以將許可授予或拒絕給使用者群組，而不是將這些許可套用至每個人。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。然後，使用者會自動接收新組織所需的許可。
- 不支援巢狀群組。將使用者存取權指派給應用程式時，IAM Identity Center 不支援將使用者新增至巢狀群組。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。必須針對使用者為成員的立即群組進行指派。

將使用者或群組存取權指派給應用程式

Important

對於 AWS 受管應用程式，您必須直接從相關應用程式主控台或透過 APIs 新增使用者。

1. 開啟 [IAM Identity Center 主控台](#)。

Note

如果您在 中管理使用者 AWS Managed Microsoft AD，請確定 IAM Identity Center 主控台正在使用 AWS Managed Microsoft AD 目錄所在的 AWS 區域，然後再執行下一個步驟。

2. 選擇 Applications (應用程式)。
3. 在應用程式清單中，選擇您要為其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，輸入使用者顯示名稱或群組名稱。您可以透過選取出現在搜尋結果中的適用帳戶來指定多個使用者或群組。
6. 選擇 Assign users (指派使用者)。

移除使用者對 SAML 2.0 應用程式的存取權

使用此程序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。如需身分驗證工作階段和持續時間的詳細資訊，請參閱[了解 IAM Identity Center 中的身分驗證工作階段](#)。

移除使用者對應用程式的存取權

1. 開啟 [IAM Identity Center 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映射至 IAM Identity Center 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 中的對應屬性。

將應用程式屬性映射至 IAM Identity Center 中的屬性

1. 開啟 [IAM Identity Center 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，然後選擇編輯屬性映射。
5. 選擇新增屬性映射。
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，輸入您要映射至應用程式屬性的 IAM Identity Center 屬性。例如，您可能想要將應用程式屬性映射 **Username** 至 IAM Identity Center 使用者屬性 **email**。若要查看 IAM Identity Center 中允許的使用者屬性清單，請參閱 中的表格[IAM Identity Center 與外部身分提供者目錄之間的屬性映射](#)。
8. 在資料表的第三欄中，從選單中選擇屬性的適當格式。
9. 選擇儲存變更。

設定 的存取權 AWS 帳戶

AWS IAM Identity Center 與 整合 AWS Organizations，可讓您集中管理多個 的許可，AWS 帳戶 而無需手動設定每個帳戶。您可以定義許可，並將這些許可指派給人力資源使用者，以 AWS 帳戶 使用 IAM Identity Center [的組織執行個體](#) 控制對特定 的存取。IAM Identity Center [的帳戶執行個體](#) 不支援帳戶存取。

AWS 帳戶 類型

在 AWS 帳戶 中有兩種類型 AWS Organizations：

- 管理帳戶 - AWS 帳戶 用來建立組織的。
- 成員帳戶 - AWS 帳戶 屬於組織的其餘。

如需 AWS 帳戶 類型的詳細資訊，請參閱AWS Organizations 《使用者指南[AWS Organizations](#)》中的[術語和概念](#)。

您也可以選擇將成員帳戶註冊為 IAM Identity Center 的委派管理員。此帳戶中的使用者可執行大多數 IAM Identity Center 管理任務。如需詳細資訊，請參閱[委派的管理](#)。

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 Identity Center 管理任務。

IAM Identity Center 管理任務	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
啟用或停用使用者存取	✘ 否	✔ 是	✔ 是
啟用、停用或管理傳入屬性	✘ 否	✔ 是	✔ 是

IAM Identity Center 管理任務	成員帳戶	委派管理員帳戶	管理帳戶
變更或管理身分來源	⊗ 否	☑ 是	☑ 是
建立、編輯或刪除客戶受管應用程式	⊗ 否	☑ 是	☑ 是
建立、編輯或刪除 AWS 受管應用程式	☑ 是	☑ 是	☑ 是
設定 MFA	⊗ 否	☑ 是	☑ 是
管理管理帳戶中未佈建的許可集	⊗ 否	☑ 是	☑ 是
管理管理帳戶中佈建的許可集	⊗ 否	⊗ 否	☑ 是
啟用 IAM Identity Center	⊗ 否	⊗ 否	☑ 是
刪除 IAM Identity Center 組態	⊗ 否	⊗ 否	☑ 是
在管理帳戶中啟用或停用使用者存取	⊗ 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

*請參閱有關將使用者和群組指派至管理帳戶之委派管理的最佳實務。

指派 AWS 帳戶 存取權

您可以使用許可集來簡化如何指派組織中的使用者和群組存取權 AWS 帳戶。許可集存放在 IAM Identity Center 中，並定義使用者和群組對的存取層級 AWS 帳戶。您可以建立單一許可集，並將其指派給組織內 AWS 帳戶的多個。您也可以將多個許可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、管理和刪除許可集](#)。

Note

您也可以將使用者單一登入存取指派給應用程式。如需相關資訊，請參閱[設定對應用程式的存取](#)。

最終使用者體驗

AWS 存取入口網站透過 Web 入口網站，為 IAM Identity Center 使用者提供其所有指派 AWS 帳戶和應用程式的單一登入存取權。AWS 存取入口網站不同於 [AWS 管理主控台](#)，這是用於管理 AWS 資源的服務主控台集合。

當您建立許可集時，您為許可集指定的名稱會在 AWS 存取入口網站中顯示為可用角色。使用者登入 AWS 存取入口網站，選擇 AWS 帳戶，然後選擇角色。選擇角色後，他們可以使用 AWS 管理主控台或擷取臨時登入資料來以程式設計方式存取 AWS AWS 服務。

若要開啟 AWS 管理主控台 或擷取臨時登入資料以程式設計方式存取 AWS，使用者請完成下列步驟：

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. 他們使用其目錄登入資料登入 AWS 存取入口網站。
3. 身分驗證後，在 AWS 存取入口網站頁面上，他們選擇帳戶索引標籤，以顯示他們有權存取 AWS 帳戶的清單。
4. 然後，使用者選擇他們要使用 AWS 帳戶的。
5. 在的名稱下方 AWS 帳戶，指派給使用者的任何許可集都會顯示為可用角色。例如，如果您john_styles將使用者指派給PowerUser許可集，該角色會在 AWS 存取入口網站中顯示為PowerUser/john_styles。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 管理主控台。
6. 除了角色之外，AWS 存取入口網站使用者可以選擇存取金鑰，擷取命令列或程式設計存取的臨時憑證。

如需您可以提供給人力資源使用者的step-by-step指引，請參閱 [設定和使用 AWS 存取入口網站](#)和 [取得 AWS CLI AWS SDKs 的 IAM Identity Center 使用者憑證](#)。

強制執行和限制存取

當您啟用 IAM Identity Center 時，IAM Identity Center 會建立服務連結角色。您也可以使用服務控制政策 (SCPs)。

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 Identity Center 之後，IAM Identity Center 可以在 AWS 帳戶 組織中的每個 中建立服務連結角色。此角色提供預先定義的許可，允許 IAM Identity Center 委派和強制執行哪些使用者具有組織中特定 AWS 帳戶 的單一登入存取權 AWS Organizations。您需要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[了解 IAM Identity Center 中的服務連結角色](#)及[使用 IAM Identity Center 的服務連結角色](#)。

限制從成員帳戶存取身分存放區

對於 IAM Identity Center 使用的身分存放區服務，有權存取成員帳戶的使用者可以使用需要讀取許可的 API 動作。成員帳戶可以存取 sso-directory 和 Identitystore 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的[AWS IAM Identity Center 目錄的動作、資源和條件索引鍵](#)，以及[AWS Identity Store 的動作、資源和條件索引鍵](#)。

若要防止成員帳戶中的使用者在身分存放區中使用 API 操作，您可以[連接服務控制政策 \(SCP\)](#)。SCP 是一種組織政策，可用來管理組織中的許可。下列範例 SCP 可防止成員帳戶中的使用者存取身分存放區中的任何 API 操作。

```
{
  "Sid": "ExplicitlyBlockIdentityStoreAccess",
  "Effect": "Deny",
  "Action": ["identitystore:*", "sso-directory:*"],
  "Resource": "*"
}
```

Note

為了確保受 AWS 管應用程式能與 IAM Identity Center 正常運作，您應該避免將此 SCP 套用至 AWS 帳戶 部署這些應用程式的。此外，如果您使用委派的管理，則應避免將此 SCP 套用至委派的管理帳戶。如需詳細資訊，請參閱[最佳實務](#)。

如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[服務控制政策 \(SCP\)](#)。

委派的管理

委派的管理為已註冊成員帳戶中的指派使用者提供方便的方式，以執行大多數 IAM Identity Center 管理任務。當您啟用 IAM Identity Center 時，您的 IAM Identity Center 執行個體 AWS Organizations 預設會在 的管理帳戶中建立。最初以這種方式設計，讓 IAM Identity Center 可以跨組織的所有成員帳戶佈建、取消佈建和更新角色。雖然您的 IAM Identity Center 執行個體必須一律位於管理帳戶中，但您可以選擇將 IAM Identity Center 的管理委派給其中的成員帳戶 AWS Organizations，藉此擴展從管理帳戶外部管理 IAM Identity Center 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以協助緩解安全問題的人數降至最低
- 允許選取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 Identity Center 如何使用 的詳細資訊 AWS Organizations，請參閱 [設定 的存取權 AWS 帳戶](#)。如需詳細資訊並檢閱示範如何設定委派管理的範例公司案例，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](#)
- [先決條件](#)
- [註冊成員帳戶](#)
- [取消註冊成員帳戶](#)
- [檢視哪些成員帳戶已註冊為委派管理員](#)

最佳實務

以下是設定委派管理之前需要考慮的一些最佳實務：

- 授予管理帳戶最低權限 – 知道管理帳戶是高權限帳戶，並且為了遵守最低權限的委託人，強烈建議您將管理帳戶的存取權限制為盡可能少的人員。委派管理員功能旨在將需要存取管理帳戶的人員數量降至最低。您也可以考慮使用[暫時提升的存取權](#)，僅在需要時才授予此存取權。
- 管理帳戶的專用許可集 – 使用管理帳戶的專用許可集。基於安全考量，用於存取管理帳戶的許可集只能由管理帳戶的 IAM Identity Center 管理員修改。委派管理員無法變更管理帳戶中佈建的許可集。

- 僅將使用者（而非群組）指派給管理帳戶中的許可集 – 由於管理帳戶具有特殊權限，因此在主控台或 AWS Command Line Interface (CLI) 中將存取權指派給此帳戶時必須小心。如果您將群組指派給具有管理帳戶存取權的許可集，則具有修改這些群組中成員資格許可的任何人都可以新增/移除這些群組的使用者，進而影響有權存取管理帳戶的人員。這是控制您的身分來源的任何群組管理員，包括您的身分提供者 (IdP) 管理員、Microsoft Active Directory Domain Service (AD DS) 管理員或 IAM Identity Center 管理員。因此，您應該將使用者直接指派給許可集，以授予管理帳戶中的存取權，並避免群組。如果您確實使用群組來管理管理帳戶的存取權，請確定 IdP 中具有適當的控制，以限制誰能夠修改這些群組，並確保這些群組的變更（或管理帳戶中使用者的登入資料變更）會視需要記錄和檢閱。
- 考慮您的 Active Directory 位置 – 如果您打算使用 Active Directory 做為 IAM Identity Center 身分來源，請在已啟用 IAM Identity Center 委派管理員功能的成員帳戶中尋找目錄。如果您決定將 IAM Identity Center 身分來源從任何其他來源變更為 Active Directory，或從 Active Directory 變更為任何其他來源，則目錄必須位於 IAM Identity Center 委派管理員成員帳戶中。如果您希望 Active Directory 位於管理帳戶中，您必須在管理帳戶中執行設定，因為委派管理員不會擁有完成它的必要許可。

在具有外部身分來源的委派管理帳戶中限制 IAM Identity Center 身分存放區動作

如果您使用外部身分來源，例如 IdP 或 Directory Service，您應該實作政策來限制 IAM Identity Center 管理員可以從委派管理帳戶內採取的身分存放區動作。應仔細考慮寫入和刪除操作。一般而言，外部身分來源是使用者及其屬性以及群組成員資格的事實來源。如果您使用身分存放區 APIs 或主控台修改這些項目，您的變更將在正常同步週期期間遭到覆寫。最好讓這些操作專屬控制您的身分真相來源。這也可防止 IAM Identity Center 管理員修改群組成員資格，以授予群組指派許可集或應用程式的存取權，而不是將群組成員資格控制保留給您的 IdP 管理員。您也應該保護誰可以從委派的管理帳戶建立 SCIM 承載字符，因為這些字符可讓成員帳戶管理員透過 SCIM 用戶端修改群組和使用者。

有時，寫入或刪除操作可能適合委派的管理員帳戶。例如，您可以建立群組而不新增成員，然後對許可集進行指派，而不必等待 IdP 管理員建立群組。在 IdP 管理員佈建群組且 IdP 同步程序建立群組成員之前，沒有人可以存取該指派。當您無法等待 IdP 同步程序移除使用者或群組的存取權時，也可以刪除使用者或群組以防止登入或授權。不過，濫用此許可可能會對使用者造成干擾。指派身分存放區許可時，您應該使用最低權限原則。您可以使用服務控制政策 (SCP) 控制委派管理帳戶管理員允許的身分存放區動作。

以下範例 SCP 可防止透過 Identity Store API 和將使用者指派給群組 AWS 管理主控台，這在您的身分來源為外部時建議使用。這不會影響 Directory Service 來自外部 IdP 的使用者同步（透過 SCIM）。

 Note

雖然您使用外部身分來源，但您的組織仍可能完全或部分依賴 Identity Store APIs 來佈建使用者和群組。因此，在啟用此 SCP 之前，您應該確認您的使用者佈建程序不會使用此 Identity Store API 操作。此外，請參閱下一節，了解如何將群組成員資格的管理限制在特定群組。

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ "*" ] }
  ]
}
```

如果您想要避免僅將使用者新增至授予管理帳戶存取權的群組，您可以使用群組 ARN 以下列格式參考這些特定群組：arn:\${Partition}:identitystore:::group/\${GroupId}。Identity Store 中可用的此和其他資源類型記錄在服務授權參考中 [AWS Identity Store 定義的資源類型](#) 中。您也可以考慮在 SCP 中包含其他 Identity Store APIs。如需詳細資訊，請參閱 Identity Store API 參考中的 [動作](#)。

透過將下列政策陳述式新增至 SCP，您可以防止委派管理員建立 SCIM 承載字符。您可以將此套用到兩個外部身分來源。

 Note

如果您的委派管理員需要使用 SCIM 設定使用者佈建，或執行定期 SCIM 承載字符輪換，您將需要暫時允許存取此 API，以允許委派管理員完成這些任務。

```
{ "Effect": "Deny",
  "Action": ["sso-directory:CreateBearerToken"],
  "Resource": [ "*" ]
}
```

為本機受管使用者限制委派管理帳戶中的 IAM Identity Center 身分存放區動作

如果您直接在 IAM Identity Center 中建立使用者和群組，而不是使用外部 IdP 或 Directory Service，則您應該針對誰可以建立使用者、重設密碼和控制群組成員資格採取預防措施。這些動作為管理員提供了強大的能力，讓誰可以登入，以及誰可以透過群組中的成員資格獲得存取權。這些政策最好實作為您用於 IAM Identity Center 管理員的許可集中的內嵌政策，而不是做為 SCPs。下列內嵌政策範例有兩個目標。首先，它可防止將使用者新增至特定群組。您可以使用此功能來防止委派管理員將使用者新增至授予管理帳戶存取權的群組。其次，可防止發行 SCIM 承載字符。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [
        arn:${Partition}:identitystore:::group/${GroupId1},
        arn:${Partition}:identitystore:::group/${GroupId2}
      ]
    },
    {
      "Effect": "Deny",
      "Action": ["sso-directory:CreateBearerToken"],
      "Resource": [ "*" ]
    }
  ]
}
```

將 IAM Identity Center 組態管理與 PermissionSet 管理隔離

從您的管理帳戶建立不同的管理員許可集，以區隔管理任務，包括修改外部身分來源、SCIM 字符管理、工作階段逾時組態與建立、修改和指派許可集。

限制發行 SCIM 承載字符

當 IAM Identity Center 的身分來源為 Okta 或 Entra ID 等外部 IdP 時，SCIM 承載字符可讓外部身分來源透過 SCIM 通訊協定佈建使用者、群組和群組成員資格。您可以設定下列 SCP，以防止委派管理員建立 SCIM 承載字符。如果您的委派管理員需要使用 SCIM 設定使用者佈建，或執行定期 SCIM 承載字符輪換，您將需要暫時允許存取此 API，以允許委派管理員完成這些任務。

```
{ "Effect": "Deny",  
  "Action": ["sso-directory:CreateBearerToken"],  
  "Resource": [ "*" ]  
}
```

使用許可集標籤和帳戶清單來委派特定帳戶的管理

您可以建立指派給 IAM Identity Center 管理員的許可集，以委派誰可以建立許可集，以及誰可以指派哪些許可集在哪些帳戶中。這可透過標記許可集並使用您指派給管理員的許可集中的政策條件來完成。例如，您可以建立許可集，讓使用者能夠建立許可集，前提是以特定方式標記許可集。您也可以建立政策，讓管理員指派在指定帳戶中具有特定標籤的許可集。這可協助您透過 帳戶委派管理，而不會授予管理員修改其對委派管理帳戶之存取權和權限的權限。例如，透過標記只在委派管理帳戶中使用的許可集，您可以指定僅授予特定人員許可的政策，以修改影響委派管理帳戶的權限集和指派。您也可以授予其他人管理委派管理帳戶以外帳戶清單的許可。若要進一步了解，請參閱 AWS 安全部落格中的在 [中委派許可集管理和帳戶指派 AWS IAM Identity Center](#)。

先決條件

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，還必須啟用和設定至少一個成員帳戶。
- 如果您的身分來源設定為 Active Directory，則必須啟用[IAM Identity Center 可設定的 AD 同步](#)此功能。

註冊成員帳戶

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管理員。該成員帳戶中具有足夠許可的使用者將具有 IAM Identity Center 的管理存取權。成員帳戶成功註冊委派管理後，即稱為委派管理員帳戶。若要進一步了解委派管理員帳戶可執行的任務，請參閱 [AWS 帳戶 類型](#)。

IAM Identity Center 支援一次僅將一個成員帳戶註冊為委派管理員。您只能在使用來自管理帳戶的登入資料登入時註冊成員帳戶。

使用下列程序，將 AWS 組織中的特定成員帳戶註冊為委派管理員，以授予 IAM Identity Center 的管理存取權。

Important

此操作會將 IAM Identity Center 管理存取權委派給此成員帳戶中的管理員使用者。擁有此委派管理員帳戶足夠許可的所有使用者可以從帳戶執行所有 IAM Identity Center 管理任務，但以下除外：

- 啟用 IAM Identity Center
- 刪除 IAM Identity Center 組態
- 管理管理帳戶中佈建的許可集
- 將其他成員帳戶註冊或取消註冊為委派管理員
- 在管理帳戶中啟用或停用使用者存取權

委派管理員可以編輯群組成員資格。

註冊成員帳戶

1. AWS 管理主控台 使用 管理帳戶的登入資料登入 AWS Organizations。執行 [RegisterDelegatedAdministrator](#) API 需要管理帳戶登入資料。
2. 選取啟用 IAM Identity Center 的區域，然後開啟 [IAM Identity Center 主控台](#)。
3. 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

您只能在使用來自管理帳戶的登入資料登入時取消註冊成員帳戶。

使用下列程序取消註冊先前指定為委派管理員 AWS 的組織成員帳戶，以從 IAM Identity Center 移除管理存取權。

Important

當您取消註冊帳戶時，您可以有效地移除所有管理員使用者從該帳戶管理 IAM Identity Center 的能力。因此，他們無法再從此帳戶管理 IAM Identity Center 身分、存取管理、身分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，因此不會影響

您的最終使用者，因為他們將繼續存取其應用程式，以及 AWS 帳戶 從 AWS 存取入口網站存取。

取消註冊成員帳戶

1. AWS 管理主控台 使用 管理帳戶的登入資料登入 AWS Organizations。執行 [DeregisterDelegatedAdministrator](#) API 需要管理帳戶憑證。
2. 選取啟用 IAM Identity Center 的區域，然後開啟 [IAM Identity Center 主控台](#)。
3. 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，檢閱安全性影響，然後輸入成員帳戶的名稱以確認您了解。
6. 選擇取消註冊帳戶。

檢視哪些成員帳戶已註冊為委派管理員

使用下列程序來尋找 中哪個成員帳戶 AWS Organizations 已設定為 IAM Identity Center 的委派管理員。

檢視已註冊的成員帳戶

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在詳細資訊區段中，找到委派管理員下的註冊帳戶名稱。您也可以選取管理索引標籤，並在委派管理員區段下檢視，以找出此資訊。

暫時提升對 的存取 AWS 帳戶

對 的所有存取 AWS 帳戶 都涉及一定層級的權限。敏感操作，例如變更生產環境的組態，由於範圍和潛在影響，需要特殊處理。暫時提升存取（也稱為just-in-time存取）是一種請求、核准和追蹤在指定時間內執行特定任務之許可的使用方式。暫時提升的存取可補充其他形式的存取控制，例如許可集和多重要素驗證。

Note

為了確保業務連續性，我們建議您[設定](#)的緊急存取 AWS 管理主控台。

為了滿足客戶的各種需求，會與 AWS 安全能力合作夥伴的解決方案 AWS IAM Identity Center 整合。會 AWS 驗證這些解決方案可解決一組常見的暫時提升存取需求。我們建議您仔細檢閱每個合作夥伴解決方案，以便選擇最適合您獨特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。

已驗證的解決方案包括 [Apono Access 管理平台](#)、[CyberArk 安全雲端存取](#)、[Okta 存取請求](#)和 [Tensor](#) (先前為 Ermetic)。

合作夥伴可以使用 Partner Center 中的 AWS 安全能力應用程式來指定解決方案。如需詳細資訊，請參閱[AWS 安全能力合作夥伴](#)。

Note

如果您使用以資源為基礎的 Amazon Elastic Kubernetes Service 或 AWS Key Management Service，請參閱在選擇just-in-time解決方案之前，[參考資源政策](#)、[Amazon EKS 叢集組態映射](#)和 [AWS KMS 金鑰政策中的許可集](#)。

對的單一登入存取 AWS 帳戶

您可以 AWS Organizations 根據[常見的任務函數](#)，將連線目錄許可中的使用者指派給 中的管理帳戶或成員帳戶。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，您可以授予資料庫管理員開發帳戶中 Amazon RDS 的廣泛許可，但限制他們在生產帳戶中的許可。IAM Identity Center 會自動在 AWS 帳戶 中設定所有必要的使用者許可。

Note

您可能需要授予使用者或群組在 AWS Organizations 管理帳戶中操作的許可。因為這是高權限帳戶，所以額外的安全限制需要您擁有 [IAMFullAccess](#) 政策或同等許可，才能進行設定。您 AWS 組織中的任何成員帳戶不需要這些額外的安全限制。

主題

- [將使用者或群組存取權指派給 AWS 帳戶](#)

- [移除的使用者和群組存取權 AWS 帳戶](#)
- [撤銷由許可集建立的作用中 IAM 角色工作階段](#)
- [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](#)

將使用者或群組存取權指派給 AWS 帳戶

使用下列程序將單一登入存取指派給連線目錄中的使用者和群組，並使用許可集來判斷其存取層級。

若要檢查現有的使用者和群組存取權，請參閱 [檢視和變更許可集](#)。

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。

將使用者或群組存取權指派給 AWS 帳戶

1. 開啟 [IAM Identity Center 主控台](#)。

Note

請確定 IAM Identity Center 主控台正在使用 AWS Managed Microsoft AD 目錄所在的區域，然後再移至下一個步驟。

2. 在導覽窗格中的多帳戶許可下，選擇 AWS 帳戶。
3. 在 AWS 帳戶頁面上，會顯示組織的樹狀檢視清單。選取您要 AWS 帳戶 為其指派存取權之 旁的核取方塊。如果您要設定 IAM Identity Center 的管理存取權，請選取管理帳戶 旁的核取方塊。

Note

當您將單一登入存取權指派給使用者和群組時，每個許可集一次最多可以選取 AWS 帳戶 10 個。若要將超過 10 AWS 帳戶 個指派給同一組使用者和群組，請視需要為其他帳戶重複此程序。出現提示時，選取相同的使用者、群組和許可集。

4. 選擇指派使用者或群組。

5. 針對步驟 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，執行下列動作：
 1. 在使用者索引標籤上，選取要授予單一登入存取權的一或多個使用者。

若要篩選結果，請在搜尋方塊中開始輸入您想要的使用者名稱。
 2. 在群組索引標籤上，選取要授予單一登入存取權的一或多個群組。

若要篩選結果，請在搜尋方塊中開始輸入您想要的群組名稱。
 3. 若要顯示您選取的使用者和群組，請選擇所選使用者和群組旁的邊三角形。
 4. 在您確認已選取正確的使用者和群組之後，請選擇下一步。
6. 針對步驟 2：選取許可集，在將許可集指派給 "**AWS-account-name**" 頁面上，執行下列動作：
 1. 選取一或多個許可集。如果需要，您可以建立和選取新的許可集。
 - 若要選取一或多個現有的許可集，請在許可集下，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許可集。
 - 若要建立一或多個新的許可集，請選擇建立許可集，然後遵循 中的步驟[建立許可集](#)。在您建立要套用的許可集之後，在 IAM Identity Center 主控台中，返回 AWS 帳戶 並遵循指示，直到您達到步驟 2：選取許可集為止。當您到達此步驟時，請選取您建立的新許可集，然後繼續進行此程序的下一個步驟。
 2. 在您確認已選取正確的許可集之後，請選擇下一步。
7. 針對步驟 3：檢閱和提交，在檢閱和提交指派至 "**AWS-account-name**" 頁面上，執行下列動作：
 1. 檢閱選取的使用者、群組和許可集。
 2. 在您確認已選取正確的使用者、群組和許可集之後，請選擇提交。

考量事項

- 使用者和群組指派程序可能需要幾分鐘的時間才能完成。保持開啟此頁面，直到程序成功完成為止。

Note

您可能需要授予使用者或群組在 AWS Organizations 管理帳戶中操作的許可。因為這是高權限帳戶，所以額外的安全限制需要您擁有 [IAMFullAccess](#) 政策或同等許可，才能進行設定。您 AWS 組織中的任何成員帳戶不需要這些額外的安全限制。

8. 如果下列任一情況適用，請依照 中的步驟[MFA 提示使用者](#)啟用 IAM Identity Center 的 MFA：
- 您使用預設的 Identity Center 目錄做為身分來源。
 - 您正在使用 Active Directory 中的 AWS Managed Microsoft AD 目錄或自我管理目錄做為身分來源，而且沒有搭配使用 RADIUS MFA AWS Directory Service。

 Note

如果您使用的是外部身分提供者，請注意，外部 IdP 而非 IAM Identity Center 會管理 MFA 設定。外部 IdPs 不支援在 IAM Identity Center 中使用 MFA。

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 Identity Center 控制，在相關 中建立 AWS 帳戶，且許可集中指定的政策會連接到角色。

或者，您可以使用 [AWS CloudFormation](#) 來建立和指派許可集，並將使用者指派給這些許可集。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。

移除的使用者和群組存取權 AWS 帳戶

使用此程序為連線目錄中的一或多個使用者和群組移除對 AWS 帳戶 的單一登入存取權。或者，您可以使用 [delete-account-assignment](#) AWS CLI。

 Note

當您需要取消佈建 IAM Identity Center 使用者或群組時，應先從使用者和群組[移除許可集的任何指派](#)，再刪除使用者和群組。

移除的使用者和群組存取權 AWS 帳戶

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在導覽窗格中的多帳戶許可下，選擇 AWS 帳戶。
3. 在 AWS 帳戶頁面上，會顯示組織的樹狀檢視清單。選取 AWS 帳戶 包含您要移除單一登入存取之使用者和群組的名稱。
4. 在 概觀頁面的已指派使用者和群組 AWS 帳戶下，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。

撤銷由許可集建立的作用中 IAM 角色工作階段

以下是撤銷 IAM Identity Center 使用者作用中許可集工作階段的一般程序。此程序假設您想要移除已洩露登入資料之使用者或系統中不良演員的所有存取權。先決條件是遵循 [中的指引準備撤銷由許可集建立的作用中 IAM 角色工作階段](#)。我們假設拒絕所有政策都存在於服務控制政策 (SCP) 中。

Note

AWS 建議您建置自動化來處理僅限主控台操作以外的所有步驟。

1. 取得您必須撤銷其存取權之人員的使用者 ID。您可以使用身分存放區 APIs 依使用者名稱尋找使用者。
2. 更新拒絕政策，以新增服務控制政策 (SCP) 中步驟 1 的使用者 ID。完成此步驟後，目標使用者將失去存取權，且無法對政策影響的任何角色採取動作。
3. 移除使用者的所有許可集指派。如果透過群組成員資格指派存取權，請從所有群組和所有直接許可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。如果使用者有作用中的 AWS 存取入口網站工作階段，且您停用該使用者，則他們可以繼續擔任新角色，直到您移除其存取權為止。
4. 如果您使用身分提供者 (IdP) 或 Microsoft Active Directory 做為身分來源，請停用身分來源中的使用者。停用使用者可防止建立其他 AWS 存取入口網站工作階段。使用您的 IdP 或 Microsoft Active Directory API 文件，了解如何自動化此步驟。如果您使用 IAM Identity Center 目錄做為身分來源，請勿停用使用者存取。您將在步驟 6 中停用使用者存取。
5. 在 IAM Identity Center 主控台中，尋找使用者並刪除其作用中工作階段。
 - a. 選擇 Users (使用者)。
 - b. 選擇您要刪除其作用中工作階段的使用者。
 - c. 在使用者的詳細資訊頁面上，選擇作用中工作階段索引標籤。
 - d. 選取您要刪除之工作階段旁的核取方塊，然後選擇刪除工作階段。

刪除使用者工作階段後，使用者將立即失去 AWS 存取入口網站的存取權。了解[工作階段持續時間](#)。

6. 在 IAM Identity Center 主控台中，停用使用者存取。

- 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. 將拒絕政策保留至少 12 小時。否則，具有作用中 IAM 角色工作階段的使用者將還原具有 IAM 角色的動作。如果您等待 12 小時，作用中工作階段會過期，使用者將無法再次存取 IAM 角色。

Important

如果您在停止使用者工作階段之前停用使用者的存取權（您已完成步驟 6 但未完成步驟 5），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，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。

如果使用者的密碼遭到入侵並[還原其指派](#)，您現在可以變更使用者的登入資料。

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 Identity Center 主控台將單一登入存取權指派給管理帳戶是一項特殊權限動作。根據預設，只有已連接 AWSSSOMasterAccountAdministrator 和 IAMFullAccess AWS 受管政策的 AWS 帳戶根使用者 或 使用者可以將單一登入存取權指派給 管理帳戶。AWSSSOMasterAccountAdministrator 和 IAMFullAccess 政策會管理 AWS Organizations 組織中管理帳戶的單一登入存取權。

或者，您可以使用 AWS CLI 來建立、連接政策，以及指派許可集。下列列出每個步驟的命令：

- 若要建立許可集：[create-permission-set](#)
- 若要連接至 AWS Managed Policy 許可集：[attach-managed-policy-to-permission-set](#)
- 若要將客戶受管政策連接至許可集：[attach-customer-managed-policy-to-permission-set](#)
- 將許可集指派給委託人：[create-account-assignment](#)

使用下列步驟將管理單一登入存取的許可委派給您目錄中的使用者和群組。

授予許可，以管理您目錄中使用者和群組的單一登入存取

1. 以管理帳戶的根使用者或其他具有管理帳戶管理員許可的使用者身分登入 IAM Identity Center 主控台。
2. 依照 中的步驟[建立許可集](#)建立許可集，然後執行下列動作：
 1. 在建立新的許可集頁面上，選取建立自訂許可集核取方塊，然後選擇下一步：詳細資訊。
 2. 在建立新的許可集頁面上，指定自訂許可集的名稱，以及選擇性的描述。如有需要，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 中的 URL AWS 管理主控台。例如：

<https://console.aws.amazon.com/ec2/>

如需詳細資訊，請參閱[設定轉送狀態以快速存取 AWS 管理主控台](#)。

3. 在您想要在許可集中包含哪些政策？下，選取連接 AWS 受管政策核取方塊。
4. 在 IAM 政策清單中，選擇 AWSSSOMasterAccountAdministrator 和 IAMFullAccess AWS 受管政策。這些政策會將許可授予未來獲指派存取此許可集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，指定金鑰和值的值（選用），然後選擇下一步：檢閱。如需標籤的詳細資訊，請參閱[標記 AWS IAM Identity Center 資源](#)。
7. 檢閱您所做的選擇，然後選擇建立。
3. 請依照 中的步驟[將使用者或群組存取權指派給 AWS 帳戶](#)，將適當的使用者和群組指派給您剛建立的許可集。
4. 向指派的使用者傳達以下內容：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，以您剛委派的許可進行身分驗證。

AWS 帳戶 使用許可集管理

許可集是您建立和維護的範本，可定義一或多個 [IAM 政策](#) 的集合。許可集可簡化組織中使用者和群組的 AWS 帳戶 存取指派。例如，您可以建立資料庫管理員許可集，其中包含管理 AWS RDS、DynamoDB 和 Aurora 服務的政策，並使用該單一許可集為資料庫管理員授予對 [AWS Organization](#) AWS 帳戶 內目標清單的存取權。

IAM Identity Center AWS 帳戶 會使用許可集，將存取權指派給一或多個 中的使用者或群組。當您指派許可集時，IAM Identity Center 會在每個帳戶中建立對應的 IAM Identity Center 控制 IAM 角色，並將許可集中指定的政策連接到這些角色。IAM Identity Center 會使用 IAM Identity Center 使用者入口網站或 AWS CLI 來管理角色，並允許您定義的授權使用者擔任角色。當您修改許可集時，IAM Identity Center 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](#)、[客戶受管政策](#)、[內嵌政策](#)和[AWS 任務職能的受管政策](#)新增至許可集。您也可以將 AWS 受管政策或客戶受管政策指派為[許可界限](#)。

若要建立許可集，請參閱 [建立、管理和刪除許可集](#)。

建立套用最低權限許可的許可集

若要遵循套用最低權限許可的最佳實務，請在建立管理許可集之後，建立更嚴格的許可集，並將其指派給一或多個使用者。在先前程序中建立的許可集為您提供起點，以評估使用者所需資源的存取量。若要切換到最低權限許可，您可以執行 IAM Access Analyzer 以使用 AWS 受管政策監控主體。了解他們正在使用哪些許可後，您可以撰寫自訂政策或產生僅具有團隊所需許可的政策。

使用 IAM Identity Center，您可以將多個許可集指派給相同的使用者。您的管理使用者也應獲指派額外、更嚴格的許可集。如此一來，他們只能 AWS 帳戶 使用所需的許可存取您的，而不是一律使用其管理許可。

例如，如果您是開發人員，在 IAM Identity Center 中建立管理使用者之後，您可以建立新的許可集，以授予PowerUserAccess許可，然後將該許可集指派給您自己。與使用 AdministratorAccess 許可的管理許可集不同，PowerUserAccess 許可集不允許管理 IAM 使用者和群組。當您登入 AWS 存取入口網站以存取 AWS 您的帳戶時，您可以選擇 PowerUserAccess 而非 AdministratorAccess 在帳戶中執行開發任務。

請謹記以下幾點考量：

- 若要快速開始建立更嚴格的許可集，請使用預先定義的許可集，而不是自訂許可集。

透過使用[預先定義許可](#)的預先定義許可集，您可以從可用政策清單中選擇單一 AWS 受管政策。每個政策會授予特定層級的存取權，以存取常見任務函數 AWS 的服務和資源或許可。如需這些政策的詳細資訊，請參閱 [AWS 任務函數的 受管政策](#)。

- 您可以設定許可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。

當使用者聯合到他們的 AWS 帳戶 並使用 AWS 管理主控台或 AWS 命令列界面 (AWS CLI) 時，IAM Identity Center 會使用許可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

工作階段持續時間的值會決定使用者在 AWS 將使用者登出工作階段 AWS 帳戶 之前可登入 的時間長度，設定為一小時。您可以指定最大值 12 小時。如需詳細資訊，請參閱[設定 的工作階段持續時間 AWS 帳戶](#)。

- 您也可以設定 AWS 存取入口網站工作階段持續時間，以控制人力資源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為 8 小時，此值決定人力使用者在必須重新驗證之前可以登入 AWS 存取入口網站的時間長度。您可以指定最大值 90 天。如需詳細資訊，請參閱[在 IAM Identity Center 中設定工作階段持續時間](#)。

- 當您登入 AWS 存取入口網站時，請選擇提供最低權限許可的角色。

您建立並指派給使用者的每個許可集都會在 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，請選擇對應至您可用來在帳戶中執行任務之最嚴格許可集的角色，而非 AdministratorAccess。

- 您可以將其他使用者新增至 IAM Identity Center，並將現有或新的許可集指派給這些使用者。

如需詳細資訊，請參閱 [將使用者或群組存取權指派給 AWS 帳戶](#)。

主題

- [AWS 受管政策的預先定義許可](#)
- [AWS 受管和客戶受管政策的自訂許可](#)
- [建立、管理和刪除許可集](#)
- [設定許可集屬性](#)

AWS 受管政策的預先定義許可

您可以使用 AWS 受管政策建立預先定義的許可集。

當您建立具有預先定義許可的許可集時，您可以從 AWS 受管政策清單中選擇一個政策。在可用的政策中，您可以從常見許可政策和任務函數政策中進行選擇。

常見許可政策

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政策：

- AdministratorAccess

- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

任務函數政策

從 AWS 受管政策清單中選擇，這些政策可讓您存取中 AWS 帳戶可能與組織內任務相關的資源。您可以新增下列其中一個政策：

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

如需可用常見許可政策和任務職能政策的詳細說明，請參閱《AWS Identity and Access Management 使用者指南》中的[AWS 任務職能的受管政策](#)。

如需如何建立許可集的說明，請參閱[建立、管理和刪除許可集](#)。

AWS 受管和客戶受管政策的自訂許可

您可以建立具有自訂許可的許可集，結合您在 AWS Identity and Access Management (IAM) 中擁有的任何 AWS 受管和客戶受管政策以及內嵌政策。您也可以包含許可界限，設定其他政策可授予許可集使用者的最大可能許可。

如需如何建立許可集的說明，請參閱[建立、管理和刪除許可集](#)。

您可以連接到許可集的政策類型

主題

- [內嵌政策](#)
- [AWS 受管政策](#)
- [客戶管理政策](#)
- [許可界限](#)

內嵌政策

您可以將內嵌政策連接至許可集。內嵌政策是格式化為您直接新增至許可集之 IAM 政策的文字區塊。當您建立新的許可集時，您可以在 IAM Identity Center 主控台中貼上政策，或使用政策建立工具產生新的政策。您也可以使用政策[AWS 產生器建立 IAM 政策](#)。

當您部署具有內嵌政策的許可集時，IAM Identity Center 會在您指派許可集 AWS 帳戶的 中建立 IAM 政策。當您將許可集指派給帳戶時，IAM Identity Center 會建立政策。然後，政策會連接到 AWS 帳戶使用者所擔任之 中的 IAM 角色。

當您建立內嵌政策並指派許可集時，IAM Identity Center 會 AWS 帳戶 為您在 中設定政策。當您使用建置許可集時[客戶管理政策](#)，您必須先在 AWS 帳戶 自己的 中建立政策，才能指派許可集。

AWS 受管政策

您可以將AWS 受管政策連接至您的許可 set。AWS managed 政策是 AWS 維護的 IAM 政策。相反地，[客戶管理政策](#)是您帳戶中建立和維護的 IAM 政策。AWS 受管政策可解決您 中常見的最低權限使用案例 AWS 帳戶。您可以指派 AWS 受管政策做為 IAM Identity Center 建立之角色的許可，或做為[許可界限](#)。

AWS 會維護[AWS 任務函數的受管政策](#)，將任務特定的存取許可指派給您的 AWS 資源。當您選擇將預先定義的許可與許可集搭配使用時，可以新增一個任務函數政策。選擇自訂許可時，您可以新增多個任務函數政策。

您的 AWS 帳戶 也包含適用於特定 AWS 服務 和 組合的大量 AWS 受管 IAM 政策 AWS 服務。當您建立具有自訂許可的許可集時，您可以從許多其他 AWS 受管政策中選擇要指派給許可集。

AWS AWS 帳戶 會以 AWS 受管政策填入每個 。若要部署具有 AWS 受管政策的許可集，您不需要先在 中建立政策 AWS 帳戶。當您使用 建置許可集時[客戶管理政策](#)，您必須先在 AWS 帳戶 自己的 中建立政策，才能指派許可集。

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](#)。

客戶管理政策

您可以將客戶受管政策連接至您的許可集。客戶受管政策是您建立和維護的帳戶中的 IAM 政策。相反地，[AWS 受管政策](#)是您帳戶中 AWS 維護的 IAM 政策。您可以指派客戶受管政策做為 IAM Identity Center 建立之角色的許可，或做為[許可界限](#)。

當您使用客戶受管政策建立許可集時，您必須在 IAM Identity Center 指派許可集 AWS 帳戶 的每個 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 Identity Center 會將 IAM 政策連接至其在 中建立的 IAM 角色 AWS 帳戶。最佳實務是將相同的許可套用至您指派許可集的每個帳戶中的政策。如需詳細資訊，請參閱[在許可集中使用 IAM 政策](#)。

Note

當客戶受管政策連接到許可集時，政策的名稱不區分大小寫。

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

您可以將許可界限連接至您的許可集。許可界限是 AWS 受管或客戶受管 IAM 政策，可設定身分型政策可授予 IAM 主體的最大許可。當您套用許可界限时，您的 [內嵌政策](#)、[客戶管理政策](#) 和 [AWS 受管政策](#) 無法授予超出許可界限所授予許可的任何許可。許可界限不會授予任何許可，而是讓 IAM 忽略超出界限的所有許可。

當您使用客戶受管政策建立許可集做為許可界限时，您必須在 IAM Identity Center 指派許可集 AWS 帳戶的每個 中建立具有相同名稱的 IAM 政策。IAM Identity Center 會將 IAM 政策做為許可界限連接至其在 中建立的 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、管理和刪除許可集

許可集定義使用者和群組對 的存取層級 AWS 帳戶。許可集存放在 IAM Identity Center 中，並可佈建至一或多個 AWS 帳戶。您可以為使用者指派多個許可集合。如需許可集及其在 IAM Identity Center 中的使用方式的詳細資訊，請參閱 [AWS 帳戶 使用許可集管理](#)。

Note

您可以在 IAM Identity Center 主控台中依名稱搜尋和排序許可集。

建立許可集時，請謹記下列考量事項：

- 組織執行個體

若要使用許可集，您需要使用 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱[IAM Identity Center 的組織和帳戶執行個體](#)。

- 從預先定義的許可集開始

透過使用預先定義[許可的預先定義](#)許可集，您可以從可用政策清單中選擇單一 AWS 受管政策。每個政策會授予特定層級的存取權，以存取常見任務函數 AWS 的服務和資源或許可。如需這些政策的詳細資訊，請參閱 [AWS 任務函數的 受管政策](#)。收集用量資料後，您可以將許可集精簡為更具限制性。

- 將管理工作階段持續時間限制在合理的工作期間

當使用者聯合到他們的 AWS 帳戶 並使用 AWS 管理主控台 或 AWS 命令列界面 (AWS CLI) 時，IAM Identity Center 會使用許可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，他們會登出主控台並要求 再次登入。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。根據預設，工作階段持續時間的值為一小時。您可以指定最大值 12 小時。如需詳細資訊，請參閱[設定 的工作階段持續時間 AWS 帳戶](#)。

- 限制人力資源使用者入口網站工作階段持續時間

人力使用者使用入口網站工作階段來選擇角色和存取應用程式。根據預設，工作階段持續時間上限的值為 8 小時，此值決定人力使用者在必須重新驗證之前可以登入 AWS 存取入口網站的時間長度。您可以指定最大值 90 天。如需詳細資訊，請參閱[在 IAM Identity Center 中設定工作階段持續時間](#)。

- 使用提供最低權限許可的角色

您建立並指派給使用者的每個許可集都會在 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，請選擇對應至您可用來在帳戶中執行任務之最嚴格許可集的角色，而非 AdministratorAccess。在傳送使用者邀請之前，測試您的許可集以確認其提供必要的存取權。

Note

您也可以使用 [AWS CloudFormation](#) 來建立和指派許可集，並將使用者指派給這些許可集。

主題

- [建立許可集](#)
- [檢視和變更許可集](#)
- [委派許可集管理](#)
- [在許可集中使用 IAM 政策](#)
- [在 IAM Identity Center 中移除許可集](#)

- [在 IAM Identity Center 中刪除許可集](#)

建立許可集

使用此程序來建立使用單一 AWS 受管政策的預先定義許可集，或使用最多 10 AWS 個受管或客戶受管政策和內嵌政策的自訂許可集。您可以在 [Service Quotas 主控台](#) 中請求調整 IAM 的 10 個政策數目上限。您可以在 IAM Identity Center 主控台中建立許可集。

Note

若要使用許可集，您需要使用 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱 [IAM Identity Center 的組織和帳戶執行個體](#)。

建立許可集合

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在多帳戶許可下，選擇許可集。
3. 選擇 Create permission set (建立許可集合)。
4. 在選取許可集類型頁面的許可集類型下，選取許可集類型。
5. 根據許可集類型，選擇您要用於許可集的一或多個政策：
 - 預先定義的許可集
 1. 在預先定義許可集的政策下，選取清單中的其中一個 IAM 任務函數政策或常見許可政策，然後選擇下一步。如需詳細資訊，請參閱AWS Identity and Access Management 《使用者指南》中的[AWS 任務函數的 受管政策](#)和 [AWS 受管政策](#)。
 2. 前往步驟 6 以完成指定許可集詳細資訊頁面。
 - 自訂許可集
 1. 選擇下一步。
 2. 在指定政策和許可界限頁面上，選擇要套用至新許可集的 IAM 政策類型。根據預設，您可以將最多 10 個AWS 受管政策和客戶受管政策的任意組合新增至您的許可集。此配額由 IAM 設定。若要提高配額，AWS 帳戶 請在您要指派許可集的每個 中的 Service Quotas 主控台中，請求增加連接到 IAM 角色的 IAM 配額受管政策。
 - 展開AWS 受管政策，從 AWS 建立和維護的 IAM 新增政策。如需詳細資訊，請參閱[AWS 受管政策](#)。
 - a. 在許可集中搜尋並選擇您要套用至使用者的AWS 受管政策。

- b. 如果您想要新增其他類型的政策，請選擇其容器並進行選擇。當您已選擇您要套用的所有政策時，請選擇下一步。前往步驟 6 以完成指定許可集詳細資訊頁面。
- 展開客戶受管政策，從您建置和維護的 IAM 新增政策。如需詳細資訊，請參閱[客戶管理政策](#)。
 - a. 選擇連接政策，然後輸入您要新增至許可集的政策名稱。在您要指派許可集的每個帳戶中，使用您輸入的名稱建立政策。最佳實務是將相同的許可指派給每個帳戶中的政策。
 - b. 選擇連接更多以新增其他政策。
 - c. 如果您想要新增其他類型的政策，請選擇其容器並進行選擇。當您已選擇您要套用的所有政策時，請選擇下一步。前往步驟 6 以完成指定許可集詳細資訊頁面。
- 展開內嵌政策以新增自訂 JSON 格式的政策文字。內嵌政策不會對應至現有的 IAM 資源。若要建立內嵌政策，請在提供的表單中輸入自訂政策語言。IAM Identity Center 會將政策新增至其在成員帳戶中建立的 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。您可以使用新增陳述式來新增其他陳述式。
 - b. 如果您想要新增其他類型的政策，請選擇其容器並進行選擇。當您已選擇您要套用的所有政策時，請選擇下一步。前往步驟 6 以完成指定許可集詳細資訊頁面。
- 展開許可界限，將 AWS 受管或客戶受管 IAM 政策新增為許可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. 選擇使用許可界限來控制許可上限。
 - b. 選擇 AWS 受管政策，從 IAM 設定政策，以 AWS 建置和維護 做為您的許可界限。選擇客戶受管政策，從您建置和維護的 IAM 設定政策作為許可界限。
 - c. 如果您想要新增其他類型的政策，請選擇其容器並進行選擇。當您已選擇您要套用的所有政策時，請選擇下一步。前往步驟 6 以完成指定許可集詳細資訊頁面。

6. 在指定許可集詳細資訊頁面上，執行下列動作：

1. 在許可集名稱下，輸入名稱以在 IAM Identity Center 中識別此許可集。您為此許可集指定的名稱會在 AWS 存取入口網站中顯示為可用角色。使用者登入 AWS 存取入口網站，選擇 AWS 帳戶，然後選擇 角色。

 Note

許可集名稱在您的 IAM Identity Center 執行個體中必須是唯一的。

2. (選用) 您也可以輸入描述。描述只會出現在 IAM Identity Center 主控台中，而不會出現在 AWS 存取入口網站中。

3. (選用) 指定工作階段持續時間的值。此值決定在主控台將使用者登出其工作階段之前，使用者可登入的時間長度。如需詳細資訊，請參閱[設定工作階段持續時間 AWS 帳戶](#)。
4. (選用) 指定轉送狀態的值。此值用於聯合程序，以重新導向帳戶內的使用者。如需詳細資訊，請參閱[設定轉送狀態以快速存取 AWS 管理主控台](#)。

 Note

轉送狀態 URL 必須在內 AWS 管理主控台。例如：

`https://console.aws.amazon.com/ec2/`

5. 展開標籤 (選用)，選擇新增標籤，然後指定金鑰和值的值 (選用)。

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. 在檢閱和建立頁面上，檢閱您所做的選擇，然後選擇建立。
8. 根據預設，當您建立許可集時，不會佈建許可集 (用於任何 AWS 帳戶)。若要在中佈建許可集 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，然後將許可集套用到這些使用者和群組。如需詳細資訊，請參閱[將使用者或群組存取權指派給 AWS 帳戶](#)。

檢視和變更許可集

您可以使用許可集來授予使用者對的存取權 AWS 帳戶。您可以使用 AWS IAM Identity Center 主控台檢視和變更許可集。您可以在 IAM Identity Center 主控台中依名稱搜尋和排序許可集。如需許可集及其在 IAM Identity Center 中的使用方式的詳細資訊，請參閱 [the section called “許可集”](#)。

管理使用者存取應用程式不需要許可集。

 Note

若要使用許可集，您需要使用 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱[IAM Identity Center 的組織和帳戶執行個體](#)。

檢視許可集指派

使用此程序在 主控台中檢視套用的 AWS IAM Identity Center 許可集。

All AWS 帳戶 where a permission set is provisioned

若要檢視許可集的所有指派，請使用下列程序：

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/singlesignon/> 開啟 AWS IAM Identity Center 主控台。
2. 在多帳戶許可下，選擇許可集。
3. 在許可集頁面上，選取您要檢視的許可集。
4. 在選取的許可集頁面上，在帳戶索引標籤下，您可以查看使用許可集的帳戶。您可以選取帳戶，以查看如何在帳戶中佈建許可集。您可以[刪除](#)、編輯政策，並將政策連接到許可集。

All permission sets for an AWS 帳戶

若要檢視許可集的所有指派，請使用下列程序：

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/singlesignon/> 開啟 AWS IAM Identity Center 主控台。
2. 在多帳戶許可下，選擇 AWS 帳戶。選取您要檢視已佈建許可集的帳戶。
3. 在所選 AWS 帳戶 頁面上的許可集索引標籤下，您可以檢視指派給所選 的不同許可集 AWS 帳戶。您可以選取許可集超連結，以進一步了解許可集。

All applied permission sets to users and groups

若要檢視指派給使用者或群組的所有許可集，請使用下列程序：

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/singlesignon/> 開啟 AWS IAM Identity Center 主控台。
2. 在儀表板下選取使用者或群組，以檢視 IAM Identity Center 使用者或群組。
 - a. 在使用者頁面上，選取要查看其套用許可集的使用者。接著，選取 AWS 帳戶 標籤和 AWS 帳戶 存取區段 AWS 帳戶 下的。您將能夠查看 AWS 帳戶 所選使用者的套用許可集和。
 - b. 在群組頁面上，選取要檢視已套用許可集的群組。接著，選取 AWS 帳戶 標籤和 AWS 帳戶 存取區段 AWS 帳戶 下的。您將能夠查看所套用的許可集，以及所選群組 AWS 帳戶 的。

變更許可集

使用此程序來使用 IAM Identity Center 主控台變更[許可集](#)。您可以從使用者或群組新增或移除許可集。

1. 登入 AWS 管理主控台 並開啟位於 <https://console.aws.amazon.com/singlesignon/> 的 AWS IAM Identity Center 主控台。
2. 在多帳戶許可下，選擇 AWS 帳戶。
3. 在 AWS 帳戶頁面上，會顯示組織的樹狀檢視清單。選取您要 AWS 帳戶 從中變更許可集的名稱。
4. 在 的概觀頁面的已指派使用者和群組 AWS 帳戶下，選取您要變更之許可集的使用者名稱或群組名稱。然後選擇變更許可集。
5. 對許可集進行所需的變更，然後選擇儲存變更。
6. 導覽至許可集索引標籤，然後選取最近變更的許可集，然後選擇更新。
7. 在更新許可頁面上，選擇更新。

委派許可集管理

IAM Identity Center 可讓您透過建立參考 IAM Identity Center 資源 [Amazon Resource Name \(ARNs\) 的 IAM 政策](#)，委派帳戶中許可集和指派的管理。例如，您可以建立政策，讓不同的管理員針對具有特定標籤的許可集，管理指定帳戶中的指派。

Note

若要使用許可集，您需要使用 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱[IAM Identity Center 的組織和帳戶執行個體](#)。

您可以使用下列其中一種方法來建立這些類型的政策。

- （建議）在 IAM Identity Center 中建立[許可集](#)，每個都具有不同的政策，並將許可集指派給不同的使用者或群組。這可讓您管理使用所選 [IAM Identity Center 身分來源](#) 登入之使用者的管理許可。
- 在 IAM 中建立自訂政策，然後將它們連接到管理員擔任的 IAM 角色。如需角色的資訊，請參閱 [IAM 角色](#) 以取得其指派的 IAM Identity Center 管理許可。

⚠ Important

IAM Identity Center 資源 ARNs 區分大小寫。

以下顯示參考 IAM Identity Center 許可集和帳戶資源類型的適當案例。

資源類型	ARN	內容金鑰
PermissionSet	arn:\${Partition}:sso::permissionSet/\${InstanceId}/\${PermissionSetId}	aws:ResourceTag/\${TagKey}
帳戶	arn:\${Partition}:sso::account/\${AccountId}	不適用

在許可集中使用 IAM 政策

在 [中建立許可集](#)，您已了解如何將政策新增至許可集，包括客戶受管政策和許可界限。當您將客戶受管政策和許可新增至許可集時，IAM Identity Center 不會在任何 [中](#) 建立政策 AWS 帳戶。您必須改為在您要指派許可集的每個帳戶中事先建立這些政策，並將其與許可集的名稱和路徑規格相符。當您將許可集指派給組織中 AWS 帳戶 的 時，IAM Identity Center 會建立 [AWS Identity and Access Management \(IAM\) 角色](#)，並將您的 [IAM 政策](#) 連接至該角色。

考量事項

- 若要使用許可集，您需要使用 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱 [IAM Identity Center 的組織和帳戶執行個體](#)。
- 使用 IAM 政策指派許可集之前，您必須準備您的成員帳戶。成員帳戶中的 IAM 政策名稱必須與管理帳戶中的政策名稱相符。如果您的成員帳戶中不存在政策，IAM Identity Center 無法指派許可集。

📘 Note

當客戶受管政策連接到許可集時，政策的名稱不區分大小寫。

- 政策授予的許可不必完全符合帳戶。

將 IAM 政策指派給許可集

1. 在 AWS 帳戶 您要指派許可集的每個 中建立 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許可。為了獲得一致的體驗，請在每個政策中設定和維護相同的許可。您可以使用 AWS CloudFormation StackSets 等自動化資源，在每個成員帳戶中建立具有相同名稱和許可的 IAM 政策複本。如需 CloudFormation StackSets 的詳細資訊，請參閱《AWS CloudFormation 使用者指南》中的[使用 AWS CloudFormation StackSets](#)。
3. 在管理帳戶中建立許可集，並在客戶受管政策或許可界限下新增 IAM 政策。如需如何建立許可集的詳細資訊，請參閱 [建立許可集](#)。
4. 新增任何內嵌政策、AWS 受管政策或您已準備的其他 IAM 政策。
5. 建立並指派您的許可集。

在 IAM Identity Center 中移除許可集

您可以在 IAM Identity Center 主控台中移除 IAM Identity Center 使用者和群組的許可集。您也可以從 移除許可集 AWS 帳戶。如需許可集及其在 IAM Identity Center 中的使用方式的詳細資訊，請參閱 [AWS 帳戶 使用許可集管理](#)。

Note

若要使用許可集，您需要使用 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱 [IAM Identity Center 的組織和帳戶執行個體](#)。

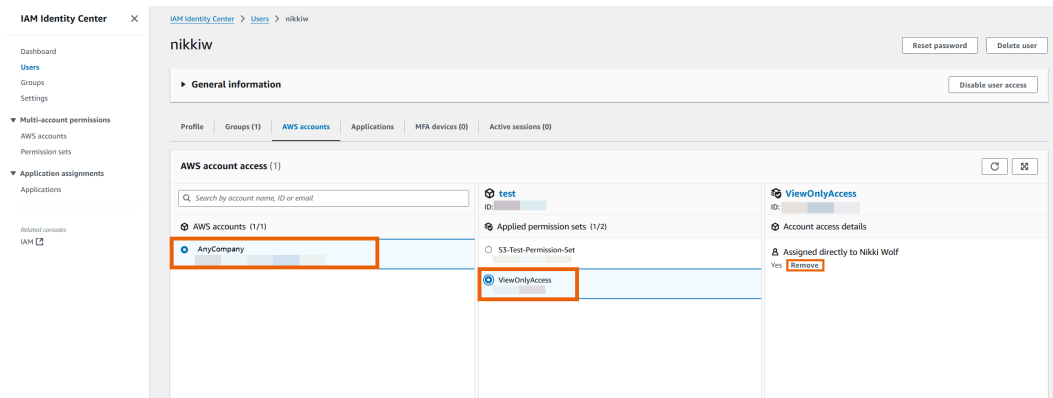
Remove permission set from a user

從使用者移除許可集

使用此程序從具有 IAM Identity Center 主控台的使用者移除許可集。

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/singlesignon/> 開啟 AWS IAM Identity Center 主控台。
2. 在 IAM Identity Center 下，選取使用者。
3. 選取您要從中移除許可集的使用者名稱。
4. 在使用者詳細資訊頁面上，選取AWS 帳戶標籤。在AWS 帳戶 存取下，選取您的 AWS 帳戶。

5. 在右窗格中，會顯示所選使用者的套用許可。選取您要移除的許可集。在帳戶存取詳細資訊下，選取移除。
6. 隨即出現對話方塊，詢問您是否要移除此許可集。選取 Remove (移除)。

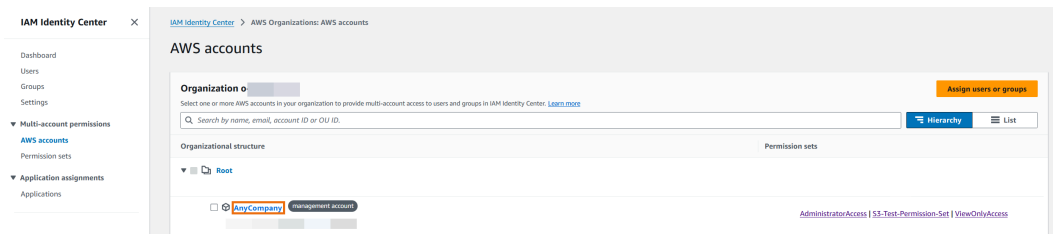


Remove permission set from a group

從群組移除許可集

使用此程序從具有 IAM Identity Center 主控台的群組中移除許可集。

1. 登入 AWS 管理主控台 並在 <https://console.aws.amazon.com/singlesignon/> 開啟 AWS IAM Identity Center 主控台。
2. 在多帳戶許可下，選取 AWS 帳戶。選取您管理帳戶的連結。



3. 在指派的使用者和群組索引標籤下，選取您要從中移除許可集的群組，然後選取變更許可集。
4. 在變更許可集頁面上，清除您要移除的許可集，然後選取儲存變更。

Remove permission set from an AWS 帳戶

使用此程序，透過 IAM Identity Center AWS 帳戶 主控台從 移除許可集。

1. 登入 AWS 管理主控台，並在 <https://console.aws.amazon.com/singlesignon/> 開啟 AWS IAM Identity Center 主控台。

2. 在多帳戶許可下，選取 AWS 帳戶。選取您要 AWS 帳戶 從中移除許可集的 名稱。
3. 在 的概觀頁面上 AWS 帳戶，選擇許可集索引標籤。選取您要移除的許可集。然後選取移除。
4. 在移除許可集對話方塊中，確認已選取正確的許可集，輸入 **Delete** 以確認移除，然後選擇移除存取權。

在 IAM Identity Center 中刪除許可集

在從 IAM Identity Center 刪除許可集之前，您應該將其從使用該許可集的所有 AWS 帳戶 [中移除](#)。若要檢查現有的使用者和群組存取權，請參閱 [檢視和變更許可集](#)。

考量事項

- 若要使用許可集，您需要使用 IAM Identity Center 的組織執行個體。如需詳細資訊，請參閱 [IAM Identity Center 的組織和帳戶執行個體](#)。
- 如果您想要撤銷作用中的許可集工作階段，請參閱 [the section called “結束人力使用者的作用中工作階段”](#)。
- 您應該從要刪除的使用者或群組中移除許可集和應用程式指派，然後再刪除它們。否則，您會在 IAM Identity Center 中擁有未指派和未使用的許可集和應用程式。

使用下列程序刪除一或多個許可集，讓 AWS 帳戶 組織中的任何 都無法使用這些許可集。

Important

所有已指派此許可集的使用者和群組，無論其 AWS 帳戶 使用方式為何，都無法再登入。若要檢查現有的使用者和群組存取權，請參閱 [檢視和變更許可集](#)。

從 刪除許可集 AWS 帳戶

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在多帳戶許可下，選擇許可集。
3. 選取您要刪除的許可集，然後選擇刪除。
4. 在刪除許可集對話方塊中，輸入許可集的名稱以確認刪除，然後選擇刪除。名稱區分大小寫。

設定許可集屬性

在 IAM Identity Center 中，管理員可以完成下列組態和管理任務，以控制使用者存取和工作階段持續時間。

任務	進一步了解
透過 IAM Identity Center 存取 AWS 資源時，管理員可以設定使用者工作階段的最長持續時間。	設定的工作階段持續時間 AWS 帳戶
管理員可以透過 IAM Identity Center 成功驗證後，自訂使用者看到的登陸頁面。	設定轉送狀態以快速存取 AWS 管理主控台
確保使用者在撤銷許可時不再能夠存取 AWS 資源。	使用拒絕政策撤銷作用中的使用者許可

設定的工作階段持續時間 AWS 帳戶

對於每個[許可集](#)，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。經過指定的持續時間後，會將使用者 AWS 登出工作階段。

當您建立新的許可集時，工作階段持續時間預設為 1 小時（以秒為單位）。最短工作階段持續時間為 1 小時，最多可設定為 12 小時。IAM Identity Center 會自動為每個許可集在每個指派的帳戶中建立 IAM 角色，並設定這些角色的工作階段持續時間上限為 12 小時。

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 會使用許可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，IAM Identity Center 針對許可集產生的 IAM 角色只能由 IAM Identity Center 使用者擔任，以確保強制執行 IAM Identity Center 許可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。

建立許可集之後，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許可集的工作階段持續時間長度。

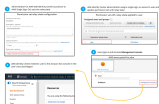
設定工作階段持續時間

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在多帳戶許可下，選擇許可集。
3. 選擇您要變更工作階段持續時間的許可集名稱。
4. 在許可集的詳細資訊頁面上，於一般設定區段標題右側，選擇編輯。
5. 在編輯一般許可集設定頁面上，選擇工作階段持續時間的新值。
6. 如果許可集佈建在任何 中 AWS 帳戶，帳戶的名稱會顯示在 下AWS 帳戶，以自動重新佈建。更新許可集的工作階段持續時間值後，AWS 帳戶 使用許可集的所有 都會重新佈建。這表示此設定的新值會套用至使用該許可集的所有 AWS 帳戶。
7. 選擇儲存變更。
8. AWS 帳戶 頁面頂端會出現通知。
 - 如果在一或多個 中佈建許可集 AWS 帳戶，則通知會確認已成功 AWS 帳戶 重新佈建，且已更新的許可集已套用至帳戶。
 - 如果未在 中佈建許可集 AWS 帳戶，通知會確認許可集的設定已更新。

設定轉送狀態以快速存取 AWS 管理主控台

根據預設，當使用者登入 AWS 存取入口網站、選擇帳戶，然後選擇從指派的許可集 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 管理主控台。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/>)，以在使用者選擇 Amazon EC2 管理員角色時將使用者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，如果使用者在歐洲（斯德哥爾摩）區域 (eu-north-1) 結束其最後一個主控台工作階段，則會將該使用者重新導向至該區域的 Amazon EC2 主控台。



若要設定 IAM Identity Center 將使用者重新導向至特定 中的主控台 AWS 區域，請在 URL 中包含區域規格。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) 中的 Amazon EC2 主控台，請在該區域 () 中指定 Amazon EC2 主控台的 URL <https://us-east-2.console.aws.amazon.com/ec2/>

east-2.console.aws.amazon.com/ec2/。如果您在美國西部（奧勒岡）區域 (us-west-2) 區域中啟用 IAM Identity Center，並且想要將使用者導向該區域，請指定 **https://us-west-2.console.aws.amazon.com**。

設定轉送狀態

使用下列程序來設定許可集的轉送狀態 URL。

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在多帳戶許可下，選擇許可集。
3. 選擇您要為其設定新轉送狀態 URL 的許可集名稱。
4. 在許可集的詳細資訊頁面上，於一般設定區段標題右側，選擇編輯。
5. 在編輯一般許可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 必須在 內 AWS 管理主控台。

6. 如果許可集佈建在任何 中 AWS 帳戶，帳戶的名稱會顯示在 下AWS 帳戶，以自動重新佈建。更新許可集的轉送狀態 URL 後，AWS 帳戶 使用許可集的所有 都會重新佈建。這表示此設定的新值會套用至使用該許可集的所有 AWS 帳戶。
7. 選擇儲存變更。
8. AWS 組織頁面頂端會顯示通知。
 - 如果在一或多個 中佈建許可集 AWS 帳戶，則通知會確認已成功 AWS 帳戶 重新佈建，且已更新的許可集已套用至帳戶。
 - 如果未在 中佈建許可集 AWS 帳戶，通知會確認許可集的設定已更新。

Note

您可以使用 AWS API、AWS SDK 或 AWS Command Line Interface() 來自動化此程序AWS CLI。如需詳細資訊，請參閱：

- [IAM Identity Center API 參考](#)中的 CreatePermissionSet 或 UpdatePermissionSet 動作

- `update-permission-set` 命令參考 [sso-admin](#) 區段中的 `create-permission-set` 或命令。AWS CLI

使用拒絕政策撤銷作用中的使用者許可

當使用者正在使用許可集 AWS 帳戶 時，您可能需要撤銷 IAM Identity Center 使用者對 的存取權。您可以事先為未指定的使用者實作拒絕政策，以移除他們使用其作用中 IAM 角色工作階段的能力，然後視需要更新拒絕政策，以指定您要封鎖其存取權的使用者。本主題說明如何建立拒絕政策，以及如何部署政策的考量事項。

準備撤銷由許可集建立的作用中 IAM 角色工作階段

您可以藉由使用服務控制政策，為特定使用者套用拒絕所有政策，防止使用者對其正在使用的 IAM 角色採取動作。您也可以防止使用者使用任何許可集，直到您變更其密碼為止，這會移除惡意行為者主動濫用遭竊的登入資料。如果您需要廣泛拒絕存取，並防止使用者重新輸入許可集或存取其他許可集，您也可以移除所有使用者存取、停止作用中的 AWS 存取入口網站工作階段，以及停用使用者登入。請參閱 [以 the section called “結束人力使用者的作用中工作階段”](#) 了解如何使用拒絕政策搭配其他動作，進行更廣泛的存取撤銷。

拒絕政策

您可以使用拒絕政策搭配符合 IAM Identity Center UserID 身分存放區中使用者 的條件，以防止使用者正在使用的 IAM 角色採取進一步動作。當您部署拒絕政策時，使用此政策可避免對可能使用相同許可集的其他使用者造成影響。此政策使用預留位置使用者 ID，針對 `"identitystore:userId"` *Add user ID here*，您會使用要撤銷存取權的使用者 ID 進行更新。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "*"
      ],
      "Resource": "*",
      "Condition": {
```

```

        "StringEquals": {
            "identitystore:userId": "Add user ID here"
        }
    }
}

```

雖然您可以使用其他條件金鑰，例如 `aws:userId`，但 `identitystore:userId` 是確定的，因為它是與一個人相關聯的全域唯一值。在條件 `aws:userId` 中使用可能會受到使用者屬性從您的身分來源同步方式的影響，如果使用者的使用者名稱或電子郵件地址變更，可能會變更。

從 IAM Identity Center 主控台，您可以透過導覽至使用者、依名稱搜尋使用者、展開一般資訊區段，以及複製使用者 ID `identitystore:userId` 來尋找使用者的。搜尋使用者 ID 時，也可輕鬆停止使用者的 AWS 存取入口網站工作階段，並在相同區段中停用其登入存取。您可以透過查詢身分存放區 APIs 來取得使用者的使用者 ID，以自動化建立拒絕政策的程序。

部署拒絕政策

您可以使用無效預留位置使用者 ID，例如 *Add user ID here*，預先使用您連接至 AWS 帳戶使用者可能有權存取的服務控制政策 (SCP) 部署拒絕政策。這是建議的方法來實現其輕鬆性和影響速度。當您使用拒絕政策撤銷使用者的存取權時，您將編輯政策，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。這可防止使用者對您連接 SCP 的每個帳戶中設定的任何許可採取任何動作。即使使用者使用其作用中的 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，也會封鎖使用者的動作。透過 SCP 完全封鎖使用者的存取權，您就可以停用其登入、撤銷其指派，並視需要停止其 AWS 存取入口網站工作階段的能力。

除了使用 SCPs 之外，您也可以在此許可集的內嵌政策中包含拒絕政策，以及在使用者可存取的許可集所使用的客戶受管政策中包含拒絕政策。

如果您必須撤銷多個人的存取權，您可以使用條件區塊中的值清單，例如：

```

    "Condition": {
        "StringEquals": {
            "identitystore:userId": [" user1 userId", "user2 userId"...]
        }
    }

```

⚠ Important

無論您使用何種方法，您都必須採取任何其他修正動作，並將使用者的使用者 ID 保留在政策中至少 12 小時。之後，使用者擔任的任何角色都會過期，然後您可以從拒絕政策中移除其使用者 ID。

在資源政策、Amazon EKS 叢集組態映射和 AWS KMS 金鑰政策中參考許可集

當您將許可集指派給 AWS 帳戶時，IAM Identity Center 會建立名稱開頭為 的角色AWSReservedSSO_。

角色的完整名稱和 Amazon Resource Name (ARN) 使用以下格式：

名稱	ARN
AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/ <i>aws-region</i> /AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>

如果 IAM Identity Center 中的身分來源託管於 us-east-1，則 ARN 中沒有 *aws-region*。角色的完整名稱和 ARN 使用以下格式：

名稱	ARN
AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>

例如，如果您建立將 AWS 帳戶存取權授予資料庫管理員的許可集，則會使用下列名稱和 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 帳戶中此許可集的所有指派，IAM Identity Center 建立的對應角色也會一併刪除。如果您稍後對相同的許可集進行新的指派，IAM Identity Center 會為許可集建立新的角色。新角色的名稱和 ARN 包含不同的唯一尾碼。在此範例中，唯一的尾碼是 abcdef0123456789。

名稱	ARN
AWSReservedSSO_DatabaseAdministrator_ abcdef0123456789	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ abcdef0123456789

角色新名稱和 ARN 中的尾碼變更會導致任何參考原始名稱和 ARN 的政策 out-of-date，這會中斷使用對應許可集之個人的存取。例如，如果在下列組態中參考原始 ARN，角色的 ARN 變更會中斷許可集使用者的存取權：

- 當您使用 進行叢集存取時，在 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集 aws-auth ConfigMap 的 aws-auth ConfigMap 檔案中。
- 在 AWS Key Management Service (AWS KMS) 金鑰的資源型政策中。此政策也稱為金鑰政策。

Note

我們建議您使用 [Amazon EKS 存取項目](#) 來管理對 Amazon EKS 叢集的存取。這可讓您使用 IAM 許可來管理有權存取 Amazon EKS 叢集的主體。透過使用 Amazon EKS 存取項目，您可以使用具有 Amazon EKS 許可的 IAM 主體來重新取得叢集的存取權，而無需聯絡 支援。

雖然您可以更新大多數 AWS 服務的資源型政策，以參考對應至許可集之角色的新 ARN，但您必須擁有在 IAM 中為 Amazon EKS 建立的備份角色，以及 ARN AWS KMS 變更時。對於 Amazon EKS，備份 IAM 角色必須存在於 `aws-auth ConfigMap`。對於 AWS KMS，它必須存在於您的金鑰政策中。如果您沒有具有更新 `aws-auth ConfigMap` 或 AWS KMS 金鑰政策許可的備份 IAM 角色，請聯絡支援以重新取得這些資源的存取權。

避免存取中斷的建議

為了避免因對應至許可集之角色的 ARN 變更而導致存取中斷，建議您執行下列動作。

- 維護至少一個許可集指派。

在包含您在 `aws-auth ConfigMap` Amazon EKS 的中參考的角色、中的金鑰政策 AWS KMS 或其他資源型政策的 AWS 帳戶中維護此指派 AWS 服務。

例如，如果您建立 `EKSAccess` 許可集並參考來自 AWS 帳戶的對應角色 ARN `111122223333`，則請將管理群組永久指派給該帳戶中的許可集。由於指派是永久的，IAM Identity Center 不會刪除對應的角色，這會消除重新命名風險。管理群組一律可以存取，而不會有權限提升的風險。

- 對於使用 **`aws-auth ConfigMap`** 和的 Amazon EKS 叢集 AWS KMS：包含在 IAM 中建立的角色。

如果您在適用於 Amazon EKS `aws-auth ConfigMap` 叢集的中或在 AWS KMS 金鑰的金鑰政策中參考許可集的角色 ARNs，我們建議您也包含至少一個您在 IAM 中建立的角色。角色必須允許您存取 Amazon EKS 叢集或管理 AWS KMS 金鑰政策。許可集必須能夠擔任此角色。如此一來，如果許可集的角色 ARN 變更，您可以在 `aws-auth ConfigMap` 或 AWS KMS 金鑰政策中更新 ARN 的參考。下一節提供如何為在 IAM 中建立的角色建立信任政策的範例。角色只能由 `AdministratorAccess` 許可集擔任。

自訂信任政策範例

以下是自訂信任政策的範例，該政策提供 `AdministratorAccess` 許可集，可存取在 IAM 中建立的角色。此政策的關鍵元素包括：

- 此信任政策的主體元素會指定 AWS 帳戶主體。在此政策中，AWS 帳戶中 `111122223333` 具有 `sts:AssumeRole` 許可的主體可以擔任在 IAM 中建立的角色。
- 此信任政策 `Condition element` 的會為可擔任在 IAM 中建立之角色的委託人指定其他需求。在此政策中，具有下列角色 ARN 的許可集可以擔任該角色。

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/  
AWSReservedSSO_AdministratorAccess_*
```

Note

Condition 元素包含 ArnLike 條件運算子，並在許可集角色 ARN 結尾使用萬用字元，而不是唯一的尾碼。這表示即使許可集的角色 ARN 變更，政策仍會允許許可集擔任在 IAM 中建立的角色。

JSON

```
{  
  "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_*"  
        }  
      }  
    }  
  ]  
}
```

如果在這類政策中包含您在 IAM 中建立的角色，將可讓您緊急存取 Amazon EKS 叢集 AWS KMS keys，或如果意外刪除和重新建立許可集或許可集的所有指派的其他 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 Identity Center，AWS 帳戶 使用來自任何 IAM Identity Center 身分來源的使用者屬性，跨多個 管理對 AWS 資源的存

取。在 中 AWS，這些屬性稱為標籤。在 中使用使用者屬性做為標籤，AWS 可協助您簡化在 中建立精細許可的程序，AWS 並確保您的人力資源只能存取具有相符標籤 AWS 的資源。

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 Identity Center 中的相同許可集，然後選取團隊名稱屬性以進行存取控制。當 Bob 和 Sally 登入其時 AWS 帳戶，IAM Identity Center 會在 AWS 工作階段中傳送其團隊名稱屬性，以便 Bob 和 Sally 只有在其團隊名稱屬性符合 AWS 專案資源上的團隊名稱標籤時，才能存取專案資源。如果 Bob 未來移至 Sally 的團隊，您只需在公司目錄中更新他的團隊名稱屬性，即可修改他的存取權。當 Bob 下次登入時，他會自動存取新團隊的專案資源，而不需要更新任何許可 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，因為與相同許可集相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 Identity Center 許可集和資源型政策中使用這些使用者屬性，以實作 ABAC 至 AWS 資源，並大規模簡化許可管理。

優勢

以下是在 IAM Identity Center 中使用 ABAC 的其他優點。

- ABAC 需要較少的許可集 – 由於您不需要為不同的任務函數建立不同的政策，因此您可以建立較少的許可集。這可減少您的許可管理複雜性。
- 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時，會根據屬性自動授予新資源的許可。
- 使用公司目錄中的員工屬性搭配 ABAC – 您可以使用 IAM Identity Center 中設定的任何身分來源的現有員工屬性來做出存取控制決策 AWS。
- 追蹤誰正在存取資源 – 安全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分 AWS。

如需如何使用 IAM Identity Center 主控台設定 ABAC 的資訊，請參閱 [存取控制的屬性](#)。如需有關如何使用 IAM Identity Center APIs 啟用和設定 ABAC 的資訊，請參閱《IAM Identity Center API 參考指南》中的 [CreateInstanceAccessControlAttributeConfiguration](#)。

主題

- [檢查清單：AWS 使用 IAM Identity Center 在 中設定 ABAC](#)
- [存取控制的屬性](#)

檢查清單：AWS 使用 IAM Identity Center 在 中設定 ABAC

此檢查清單包含準備 AWS 資源和設定 IAM Identity Center for ABAC 存取所需的組態任務。依序完成此檢查清單中的任務。當參考連結帶您前往主題時，請返回此主題，以便您可以繼續此檢查清單中的其餘任務。

步驟	任務	參考資料
1	檢閱如何將標籤新增至您的所有 AWS 資源。若要在 IAM Identity Center 中實作 ABAC，您必須先將標籤新增至要實作 ABAC 的所有 AWS 資源。	標記 AWS 資源
2	檢閱如何在 IAM Identity Center 中使用身分存放區中的相關聯使用者身分和屬性來設定身分來源。IAM Identity Center 可讓您從 ABAC in 的任何支援的 IAM Identity Center 身分來源使用使用者屬性 AWS。	管理您的身分來源
3	根據下列條件，決定您要在 中用於做出存取控制決策的屬性 AWS，並將其傳送至 IAM Identity Center。	開始使用
	如果您使用的是外部身分提供者 (IdP)，請決定要使用從 IdP 傳遞的屬性，還是從 IAM Identity Center 中選取屬性。	使用外部身分提供者做為您的身分來源時，選擇屬性
	如果您選擇讓 IdP 傳送屬性，請將 IdP 設定為在 SAML 聲明中傳輸屬性。請參閱特定 IdP 教學課程中的 Optional 章節。	IAM Identity Center 身分來源教學課程
	如果您使用 IdP 做為身分來源，並選擇在 IAM Identity Center 中選取屬性，請調查如何設定 SCIM，讓屬性值來自您的 IdP。如果您無法搭配 IdP 使用 SCIM，請使用 IAM Identity Center 主控台使用者頁面新增使用者及其屬性。	使用 SCIM 從外部身分提供者佈建使用者和群組 支援的外部身分提供者屬性
	如果您使用 Active Directory 或 IAM Identity Center 做為身分來源，或使用 IdP 並選擇在 IAM Identity Center 中選取屬性，請檢閱您可以設定的可用屬性。然後立即跳到步驟 4，開始使用 IAM Identity Center 主控台設定 ABAC 屬性。	使用 IAM Identity Center 做為您的身分來源時選擇屬性

步驟	任務	參考資料
		• 使用 AWS Managed Microsoft AD 做為您的身分來源時選擇屬性 • IAM Identity Center 與 之間的預設映射 Microsoft AD
4	使用 IAM Identity Center 主控台內的存取控制屬性頁面，選取要用於 ABAC 的屬性。從此頁面中，您可以從您在步驟 2 中設定的身分來源選取存取控制的屬性。身分及其屬性位於 IAM Identity Center 之後，您必須建立鍵/值對（映射），並將其傳遞給 AWS 帳戶 以用於存取控制決策。	• 啟用和設定存取控制的屬性
5	在許可集中建立自訂許可政策，並使用存取控制屬性來建立 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 中設定的使用者屬性會做為存取控制決策 AWS 的標籤。您可以使用 <code>aws:PrincipalTag/key</code> 條件參考許可政策中的存取控制屬性。	• 在 IAM Identity Center 中建立 ABAC 的許可政策
6	在各種 AWS 帳戶，將使用者指派給您在步驟 5 中建立的許可集。這樣做可確保當他們聯合到其帳戶並存取 AWS 資源時，他們只會根據相符的標籤取得存取權。	• 將使用者或群組存取權指派給 AWS 帳戶

完成這些步驟後，AWS 帳戶 使用單一登入聯合到 的使用者將根據相符的屬性來存取其 AWS 資源。

存取控制的屬性

存取控制的屬性是 IAM Identity Center 主控台內的頁面名稱，您可以在其中選取要在政策中使用的使用者屬性，以控制對資源的存取。您可以 AWS 根據使用者身分來源中的現有屬性，將使用者指派給中的工作負載。

例如，假設您想要根據部門名稱指派對 S3 儲存貯體的存取權。在存取控制的屬性頁面上，您可以選取要與屬性型存取控制 (ABAC) 搭配使用的部門使用者屬性。在 IAM Identity Center 許可集中，您接著撰寫政策，只有在部門屬性符合您指派給 S3 儲存貯體的部門標籤時，才會授予使用者存取權。IAM Identity Center 會將使用者的部門屬性傳遞給正在存取的帳戶。然後，會使用 屬性來根據政策判斷存取權。當 IAM Identity Center 將這些屬性傳遞給帳戶時，它們會以工作階段標籤的形式傳送，您可

以使用所有相關 IAM AWS 政策類型中的 `aws:PrincipalTag/tag-key` 條件索引鍵來參考。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的屬性，取決於您使用的身分來源。無論您選擇何種身分來源，在選取屬性之後，您需要建立或編輯許可集政策。這些政策必須授予使用者身分對資源的 AWS 存取權。

使用 IAM Identity Center 做為您的身分來源時選擇屬性

當您將 IAM Identity Center 設定為身分來源時，請先新增使用者並設定其屬性。接著，導覽至存取控制的屬性頁面，然後選取您要在政策中使用的屬性。最後，導覽至 AWS 帳戶頁面以建立或編輯許可集，以使用 ABAC 的屬性。

使用 AWS Managed Microsoft AD 做為您的身分來源時選擇屬性

當您將 IAM Identity Center 設定為 AWS Managed Microsoft AD 身分來源時，請先將一組屬性從 Active Directory 映射至 IAM Identity Center 中的使用者屬性。接著，導覽至存取控制的屬性頁面。然後，根據從 Active Directory 映射的現有 SSO 屬性集，選擇要在 ABAC 組態中使用的屬性。最後，使用許可集中的存取控制屬性編寫 ABAC 規則，以授予使用者身分對資源的 AWS 存取權。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映射清單，請參閱 [IAM Identity Center 與之間的預設映射 Microsoft AD](#)。

使用外部身分提供者做為您的身分來源時，選擇屬性

當您使用外部身分提供者 (IdP) 做為身分來源來設定 IAM Identity Center 時，有兩種方式可以使用 ABAC 的屬性。

- 在 IAM Identity Center 主控台中設定屬性映射。您可以將屬性從 IAM Identity Center 目錄映射到 IAM Identity Center 主控台中存取控制屬性頁面上的工作階段標籤。您在此處選擇的屬性值來自 Identity Center 目錄，並透過 SAML 聲明取代來自 IdP 的任何相符屬性值。根據您是否使用 SCIM，請考慮下列事項：
 - 如果使用 SCIM，IdP 會自動將屬性值同步到 IAM Identity Center。然後，您可以在存取控制的屬性頁面上選取這些同步屬性，以將其用作工作階段標籤。
 - 如果您不是使用 SCIM，則必須手動新增使用者並設定其屬性，就像使用 IAM Identity Center 做為身分來源一樣。接著，導覽至存取控制的屬性頁面，然後選擇您要在政策中使用的屬性。
- 透過 SAML 聲明從您的 IdP 傳遞屬性。您可以將 IdP 設定為透過 SAML 聲明將屬性作為工作階段標籤傳送。若要執行此作業，請將 IdP 設定為傳送屬性名稱設為的 SAML 聲明 `https://aws.amazon.com/SAML/Attributes/AccessControl:TagKey`，並將 *TagKey* 取代為您要填入的工作階段標籤金鑰。IAM Identity Center 會將屬性名稱和值從 IdP 傳遞到以進行政策評估。

您不需要針對從外部 IdP 透過 SAML 聲明傳入的屬性，在存取控制屬性頁面上設定 ABAC 屬性映射。不過，如果您在存取控制的屬性頁面上為相同的屬性設定 ABAC 映射，則來自 Identity Center 目錄的映射會優先，並在 SAML 聲明中取代 IdP 傳送的值。

Note

您無法在存取控制的屬性頁面上看到 SAML 聲明中的屬性。您必須事先了解這些屬性，並在撰寫政策時將其新增至存取控制規則。如果您決定信任外部 IdPs 的屬性，則這些屬性一律會在使用者聯合時傳遞 AWS 帳戶。如需如何在 IdP 中為存取控制設定使用者屬性以透過 SAML 聲明傳送的資訊，請參閱 IdP [IAM Identity Center 身分來源教學課程](#)的。

如需 IAM Identity Center 中使用者屬性到外部 IdPs 中使用者屬性的支援屬性完整清單，請參閱 [支援的外部身分提供者屬性](#)。

若要在 IAM Identity Center 中開始使用 ABAC，請參閱下列主題。

主題

- [啟用和設定存取控制的屬性](#)
- [在 IAM Identity Center 中建立 ABAC 的許可政策](#)

啟用和設定存取控制的屬性

若要使用屬性型存取控制 (ABAC)，您必須先在 IAM Identity Center 主控台的設定頁面或 [IAM Identity Center API](#) 中啟用它。無論身分來源為何，您一律可以從身分存放區設定使用者屬性，以便在 ABAC 中使用。在 主控台中，您可以透過導覽至設定頁面上存取控制的屬性索引標籤來執行此操作。如果您使用外部身分提供者 (IdP) 做為身分來源，您也可以選擇從 SAML 聲明中的外部 IdP 接收屬性。在此情況下，您需要設定外部 IdP 以傳送所需的屬性。如果 SAML 聲明中的屬性也在 IAM Identity Center 中定義為 ABAC 屬性，IAM Identity Center 會在登入時將值從其 Identity Store 做為 [工作階段標籤](#) 傳送至 AWS 帳戶。

Note

您無法從 IAM Identity Center 主控台的存取控制屬性頁面檢視外部 IdP 設定和傳送的屬性。如果您要從外部 IdP 傳遞 SAML 聲明中的存取控制屬性，則這些屬性會在使用者聯合 AWS 帳戶時直接傳送至。屬性無法在 IAM Identity Center 中用於映射。

主題

- [啟用存取控制的屬性](#)
- [選取您的屬性以進行存取控制](#)
- [停止以屬性進行存取控制](#)

啟用存取控制的屬性

使用下列程序，使用 IAM Identity Center 主控台啟用存取 (ABAC) 控制功能的屬性。

Note

如果您有現有的許可集，且打算在 IAM Identity Center 執行個體中啟用 ABAC，則其他安全限制會要求您先擁有 `iam:UpdateAssumeRolePolicy` 政策。如果您沒有在帳戶中建立任何許可集，則不需要這些額外的安全限制。

如果您的 IAM Identity Center 執行個體是在 2020 年 12 月之前建立，且您計劃在其中啟用 ABAC，則無論您的帳戶中是否建立許可集，您都必須擁有與 IAM Identity Center 管理角色相關聯的 `iam:UpdateAssumeRolePolicy` 政策。

啟用存取控制的屬性

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定
3. 在設定頁面上，找到存取控制資訊的屬性方塊，然後選擇啟用。繼續下一個程序來設定它。

選取您的屬性以進行存取控制

使用下列程序來設定 ABAC 組態的屬性。

Note

此程序僅適用於您想要從 IAM Identity Center 目錄映射屬性以用作工作階段標籤的情況。如果您要透過 SAML 聲明從外部身分提供者 (IdP) 傳遞屬性，則不需要在此處設定屬性映射。如需詳細資訊，請參閱[使用外部身分提供者做為您的身分來源時，選擇屬性](#)。從 Identity Center 目錄映射中設定的值會覆寫 SAML 聲明中設定的值。

使用 IAM Identity Center 主控台選取屬性

1. 開啟 [IAM Identity Center 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. 在存取控制的屬性頁面上，選擇新增屬性，然後輸入金鑰和值詳細資訊。在這裡，您將將來自身分來源的屬性映射到 IAM Identity Center 作為工作階段標籤傳遞的屬性。

Key ⓘ	Value (optional) ⓘ	Remove
Department	<code>\${path:enterprise.department}</code>	✕
CostCenter	<code>\${path:enterprise.costCenter}</code>	✕
Add new key	Add new value	

索引鍵代表您要提供給屬性的名稱，以用於 政策。這可以是任何任意名稱，但您需要在您撰寫的存取控制政策中指定該確切名稱。例如，假設您使用 Okta (外部 IdP) 作為身分來源，並且需要將組織的成本中心資料作為工作階段標籤傳遞。在金鑰中，您會輸入類似相符的名稱，例如做為金鑰名稱的 CostCenter。請務必注意，您在此處選擇的任何名稱，也必須在 [aws:PrincipalTag #####](#) (即) 中將其命名為完全相同的名稱"ec2:ResourceTag/CostCenter": "\${aws:PrincipalTag/CostCenter}"。

Note

為您的金鑰使用單一值屬性，例如 **Manager**。IAM Identity Center 不支援 ABAC 的多值屬性，例如 **Manager, IT Systems**。

值代表來自您設定之身分來源的屬性內容。在這裡，您可以從 中列出的適當身分來源資料表輸入任何值[IAM Identity Center 與外部身分提供者目錄之間的屬性映射](#)。例如，使用上述範例中提供的內容，您可以檢閱支援的 IdP 屬性清單，並判斷支援屬性最接近的相符項目會是 `${path:enterprise.costCenter}`，然後在值欄位中輸入它。如需參考，請參閱上述提供的螢幕擷取畫面。請注意，除非您使用透過 SAML 聲明傳遞屬性的選項，否則您無法針對 ABAC 使用此清單以外的外部 IdP 屬性值。

5. 選擇儲存變更。

現在您已設定映射存取控制屬性，您需要完成 ABAC 組態程序。若要這樣做，請建立 ABAC 規則，並將其新增至您的許可集和/或資源型政策。這是必要的，以便您可以授予使用者身分對 AWS 資源的存取權。如需詳細資訊，請參閱[在 IAM Identity Center 中建立 ABAC 的許可政策](#)。

停止以屬性進行存取控制

使用下列程序停用 ABAC 功能，並刪除所有已設定的屬性映射。

停用存取控制的屬性

1. 開啟 [IAM Identity Center 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. 在存取控制的管理屬性頁面上，選擇停用。
5. 在停用存取控制的屬性對話方塊中，檢閱資訊和準備就緒時輸入 **DISABLE**，然後選擇確認。

Important

此步驟會刪除所有屬性，並在聯合到時停止使用存取控制的屬性，AWS 帳戶 無論外部身分來源提供者的 SAML 聲明中是否存在任何屬性。

在 IAM Identity Center 中建立 ABAC 的許可政策

您可以建立許可政策，根據設定的屬性值來決定誰可以存取您的 AWS 資源。當您啟用 ABAC 並指定屬性時，IAM Identity Center 會將已驗證使用者的屬性值傳遞至 IAM，以用於政策評估。

aws:PrincipalTag 條件金鑰

您可以使用 `aws:PrincipalTag` 條件索引鍵在許可集中使用存取控制屬性來建立存取控制規則。例如，在以下政策中，您可以使用其各自的成本中心標記組織中的所有資源。您也可以使用單一許可集，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，他們只能存取其各自成本中心中的資源。當團隊為其專案新增更多開發人員和資源時，您只需使用正確的成本中心標記資源。然後在開發人員聯合時，在 AWS 工作階段中傳遞成本中心資訊 AWS 帳戶。因此，隨著組織將新資源和開發人員新增至成本中心，開發人員可以管理與其成本中心一致的資源，而不需要任何許可更新。

JSON

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

當使用者 AWS 帳戶 透過 IAM Identity Center 聯合到 時，設定的存取控制屬性會以工作階段標籤的形式傳遞。您可以使用 `aws:PrincipalTag/tag-key` 條件金鑰，在政策中參考這些工作階段標籤。您可以在其中使用條件的所有相關 AWS IAM 政策類型中支援此條件金鑰，包括身分型政策、資源型政策、許可界限、服務控制政策 (SCPs) 和 VPC 端點政策。這可讓您根據整個 AWS 環境中的使用者屬性，做出精細的存取控制決策。

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](#)。

如果政策在其條件中包含無效的屬性，則政策條件將會失敗並拒絕存取。如需詳細資訊，請參閱[錯誤「使用者嘗試使用外部身分提供者登入時發生非預期錯誤」](#)。

了解 IAM Identity Center 中的服務連結角色

[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具有組織中特定 AWS 帳戶的單一登入存取權 AWS Organizations。服務透過 AWS 帳戶在其組織內的每個中佈建服務連結角色來啟用此功能。然後，該服務允許 IAM Identity Center AWS 等其他服務利用這些角色來執行服務相關任務。如需詳細資訊，請參閱 [AWS Organizations](#) 和 [服務連結角色](#)。

當您啟用 IAM Identity Center 時，IAM Identity Center 會在組織中的所有帳戶中建立服務連結角色 AWS Organizations。IAM Identity Center 也會在每個帳戶中建立相同的服務連結角色，該角色隨後會新增至您的組織。此角色允許 IAM Identity Center 代表您存取每個帳戶的資源。如需詳細資訊，請參閱 [設定 的存取權 AWS 帳戶](#)。

在每個中建立的服務連結角色命名 AWS 帳戶為 `AWSServiceRoleForSSO`。如需詳細資訊，請參閱 [使用 IAM Identity Center 的服務連結角色](#)。

備註

- 如果您登入 AWS Organizations 管理帳戶，它會使用您目前登入的角色，而不是服務連結角色。這可防止權限升級。
- 當 IAM Identity Center 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。這可讓 CloudTrail 中的日誌提供誰在管理帳戶中進行所有權限變更的可見性。

設定和使用 AWS 存取入口網站

AWS 存取入口網站會透過 IAM Identity Center 將您的人力資源連線至 AWS 帳戶 和雲端應用程式。管理員設定入口網站和管理使用者存取，而最終使用者登入一次，無縫存取其所有授權的資源。

AWS 存取入口網站提供單一登入存取：

- AWS 帳戶 在您的組織中。
- AWS 受管應用程式，例如 Amazon Quick 和 Kiro。
- Office 365、Concur、Salesforce 等雲端應用程式。

當使用者登入入口網站時，他們會找到他們獲授權存取的 AWS 帳戶 和 應用程式，而無需額外的登入。

AWS 存取入口網站入門

對於管理員：

您需要對[組織執行個體](#)或 IAM Identity Center [帳戶執行個體](#)的管理存取權，才能設定 AWS 存取入口網站和管理使用者存取權。

1. 選擇性地自訂 AWS 存取入口網站 URL。
2. 指派使用者存取 AWS 帳戶 和 應用程式。入口網站中會顯示指派 AWS 的資源。

對於最終使用者：

您的管理員必須已完成 AWS 存取入口網站設定，並為您提供入口網站 URL 和登入憑證。

1. 從您的管理員取得入口網站 URL（通常是 `https://your-company.awsapps.com/start`）。
2. 使用管理員提供的登入資料登入。
3. 存取入口網站中的資源。

設定 AWS 存取入口網站

身為管理員，您可以自訂 AWS 存取入口網站以符合組織的需求，並確保使用者可以輕鬆存取其授權的資源。

您可以設定的內容

AWS 存取入口網站啟用：設定 AWS 存取入口網站的初始使用者存取，包括使用者憑證啟用和首次登入程序。

自訂 AWS 存取入口網站 URL（選用）：將組織的 AWS 存取入口網站 URL 從預設格式 (d-xxxxxxxxxx.awsapps.com/start) 個人化為可辨識的子網域 (your-company.awsapps.com/start)。

開始之前

確定您擁有 IAM Identity Center 的管理存取權、確認 IAM Identity Center 已設定為[組織執行個體](#)或[帳戶執行個體](#)，並規劃您的自訂子網域名稱（此為一次性組態，稍後無法變更）。

設定完成後，使用者可以使用自訂 URL 存取 AWS 存取入口網站，並遵循您為組織建立的啟用程序。

主題

- [為第一次 IAM Identity Center 使用者啟用 AWS 存取入口網站](#)
- [自訂 AWS 存取入口網站 URL](#)
- [確認使用者可以登入 AWS 存取入口網站](#)

為第一次 IAM Identity Center 使用者啟用 AWS 存取入口網站

如果這是您第一次嘗試登入 AWS 存取入口網站，請檢查您的電子郵件，以取得如何啟用使用者登入資料的指示。

啟用您的使用者登入資料

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登入資料，以便您可以開始使用 AWS 存取入口網站。
 - a. 如果您收到一封電子郵件，其中包含加入 AWS IAM Identity Center 的邀請主旨，請開啟並選擇接受邀請。在新增使用者註冊頁面上，輸入並確認密碼，然後選擇設定新密碼。每次您登入入口網站時，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，請遵循他們提供的指示來啟用您的使用者登入資料。
2. 在您提供新密碼來啟用使用者登入資料後，AWS 存取入口網站會自動登入。如果未發生這種情況，您可以使用 中提供的指示手動登入 AWS 存取入口網站[登入 AWS 存取入口網站](#)。

自訂 AWS 存取入口網站 URL

根據預設，您可以使用遵循此格式的 URL 來存取 AWS 存取入口網站：d-xxxxxxxxxx.awsapps.com/start。您可以自訂 URL，如下所示：*your_subdomain*.awsapps.com/start。

Important

如果您變更 AWS 存取入口網站 URL，您稍後就無法編輯。

自訂您的 URL

1. 在 <https://console.aws.amazon.com/singlesignon/> 開啟 AWS IAM Identity Center 主控台。
2. 在 IAM Identity Center 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

如果未顯示自訂按鈕，表示已自訂 AWS 存取入口網站。自訂 AWS 存取入口網站 URL 是無法反轉的一次性操作。

4. 輸入所需的子網域名稱，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。

確認使用者可以登入 AWS 存取入口網站

下列步驟適用於 IAM Identity Center 管理員，以確認 IAM Identity Center 使用者可以登入 AWS 存取入口網站並存取 AWS 帳戶。

登入 AWS 存取入口網站

1. 執行下列其中一項操作來登入 AWS 管理主控台。
 - 新使用者 AWS（根使用者）– 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者的身分登入。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，然後選取管理員角色。

2. 開啟 [IAM Identity Center 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. 使用下列其中一項登入：
 - 如果您使用 Active Directory 或外部身分提供者 (IdP) 做為身分來源，請使用 Active Directory 或 IdP 使用者的登入資料登入。
 - 如果您使用預設的 Identity Center 目錄做為身分來源，請使用您在建立使用者時指定的使用者名稱，以及您為使用者指定的新密碼來登入。
6. 在帳戶索引標籤中，找到 AWS 帳戶 並展開您的。
7. 隨即顯示您可用的角色。例如，如果您同時獲指派 AdministratorAccess 許可集和 Billing 許可集，這些角色會顯示在 AWS 存取入口網站中。選擇您要用於工作階段的 IAM 角色名稱。
8. 如果您被重新導向至 AWS 管理主控台，您已成功完成對 的存取設定 AWS 帳戶。

Note

如果您未看到任何 AWS 帳戶列出的項目，則使用者可能尚未指派給該帳戶的許可集。如需將使用者指派給許可集的指示，請參閱 [將使用者或群組存取權指派給 AWS 帳戶](#)。

現在您已確認可以使用 IAM Identity Center 登入資料登入，請切換到用來登入 的瀏覽器，AWS 管理主控台 並從根使用者或 IAM 使用者登入資料登出。

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任務，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 Identity Center，請僅透過 IAM Identity Center 建立和指派許可集。

使用 AWS 存取入口網站

您可以在入口網站中選擇 AWS 帳戶 或 應用程式索引標籤來啟動多個應用程式。AWS 存取入口網站中存在應用程式圖示，表示您公司的管理員已授予您存取這些 AWS 帳戶 或 應用程式的權限。這也表示您可以從存取入口網站 AWS 存取所有這些帳戶或應用程式，而無需額外的登入提示。

如何使用 AWS 存取入口網站

若要使用 AWS 存取入口網站：

1. 從您的管理員取得入口網站 URL（通常看起來像 `https://your-company.awsapps.com/start`）。
2. 使用管理員提供的登入資料登入。
3. 在入口網站中選擇您要存取的帳戶和應用程式。

您的管理員會根據您的角色和許可，控制您在入口網站中看到的內容。在這些情況下，請聯絡您的管理員以請求額外的存取權：

- 您看不到需要存取的 AWS 帳戶 或 應用程式。
- 您對指定帳戶或應用程式的存取不符合您的預期。

主題

- [登入 AWS 存取入口網站](#)
- [重設您的 AWS 存取入口網站使用者密碼](#)
- [取得 AWS CLI AWS SDKs 的 IAM Identity Center 使用者憑證](#)
- [建立 AWS 管理主控台 目的地的捷徑連結](#)
- [為您的裝置註冊 MFA](#)
- [檢視和結束作用中工作階段](#)

登入 AWS 存取入口網站

AWS 存取入口網站透過 Web 入口網站，為 IAM Identity Center 使用者提供其所有指派 AWS 帳戶 和 應用程式的單一登入存取權。以下概述如何登入 AWS 存取入口網站、登入提示，以及如何登出 AWS 存取入口網站。

先決條件

必須啟用 IAM Identity Center 才能使用 AWS 存取入口網站。如需詳細資訊，請參閱[啟用 IAM Identity Center](#)。

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](#)。

登入 AWS 存取入口網站

登入 AWS 存取入口網站

1. 在瀏覽器視窗中，貼上您提供的登入 URL，然後選擇 Enter。URL 看起來像 d-xxxxxxxxxx.awsapps.com/start 或 *your_subdomain*.awsapps.com/start。我們建議您立即將此入口網站的連結設定成書籤，以便日後可以快速存取。
2. 使用您的標準公司登入憑證登入。

Note

如果您的管理員傳送電子郵件一次性密碼 (OTP)，而這是您第一次登入，請輸入該密碼。登入後，您必須為未來的登入建立新密碼。

如果系統提示您輸入驗證碼，請檢查您的電子郵件，然後將程式碼複製並貼到登入頁面。

Note

驗證碼通常透過電子郵件傳送，但交付方法可能有所不同。如需詳細資訊，請洽詢您的管理員。

3. 登入後，您可以存取入口網站中顯示的任何 AWS 帳戶 和 應用程式。

信任的裝置

當您選擇 選項 這是來自登入頁面的受信任裝置時，IAM Identity Center 會將該裝置的所有未來登入視為已授權。這表示只要您使用該受信任裝置，IAM Identity Center 就不會顯示在 MFA 代碼中輸入的選項。不過，有一些例外狀況，包括從新瀏覽器登入，或您的裝置獲發不明 IP 地址。

AWS 存取入口網站的登入提示

以下是一些可協助您管理 AWS 存取入口網站體驗的秘訣。

- 有時，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來開啟入口網站中列出的任何應用程式。使用應用程式完成後，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都會保持開啟並執行。
- 您必須先登出 AWS 存取入口網站，才能以不同的使用者身分登入。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。切換角色會暫時保留原始使用者許可，並改為給予您指派給角色的許可。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](#)。

登出 AWS 存取入口網站

- 在 AWS 存取入口網站中，從導覽列中選擇登出。

Note

如果您想要以不同使用者身分登入，您必須先登出 AWS 存取入口網站。

重設您的 AWS 存取入口網站使用者密碼

AWS 存取入口網站可讓 [IAM Identity Center](#) 使用者透過 Web 入口網站，透過單一登入存取其所有指派 AWS 的帳戶和雲端應用程式。AWS 存取入口網站不同於 [AWS 管理主控台](#)，這是用於管理 AWS 資源的服務主控台集合。

使用此程序來重設 AWS 存取入口網站的 IAM Identity Center 使用者密碼。請參閱 [《使用者指南》](#)，[進一步了解 使用者類型](#)。AWS 登入

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](#)做為其身分來源的 Identity Center 執行個體使用者。如果您的使用者連接到外部身分提供者或 [AD Connector](#)，則必須從外部身分提供者或連接的 完成使用者密碼重設Active Directory。

- 如果您的身分來源是 IAM Identity Center 目錄，請參閱 [在 IAM Identity Center 中管理身分時的密碼需求](#)。
- 如果您的身分來源是 AWS Managed Microsoft AD，請參閱[在中重設密碼時的密碼要求 AWS Managed Microsoft AD](#)。

將密碼重設為 AWS 存取入口網站

1. 開啟 Web 瀏覽器，並前往 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。您應該已透過電子郵件收到加入 AWS IAM Identity Center 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為您提供一次性密碼和 AWS 存取入口網站 URL。如果您找不到此資訊，請要求管理員將其傳送給您。

如需登入 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。

驗證您的使用者名稱，並輸入所提供影像的字元，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程式軟體。

4. 隨即出現一則訊息，確認已傳送重設密碼電子郵件。選擇繼續。
5. 您會收到來自 的電子郵件，no-reply@signin.aws其中包含請求的主體密碼重設。在電子郵件中，選擇重設密碼。
6. 在重設密碼頁面上，驗證您的使用者名稱，為 AWS 存取入口網站指定新密碼，然後選擇設定新密碼。
7. 您會收到來自 的電子郵件no-reply@signin.aws，主旨行密碼已更新。

Note

管理員可以透過傳送電子郵件給您來重設密碼，或產生一次性密碼並與您共用。如果您是管理員，請參閱[重設最終使用者的 IAM Identity Center 使用者密碼](#)。

取得 AWS CLI AWS SDKs 的 IAM Identity Center 使用者憑證

您可以使用 AWS Command Line Interface 或 AWS 軟體開發套件 (SDKs) 搭配 IAM Identity Center 的使用者憑證，以程式設計方式存取 AWS 服務。本主題說明如何在 IAM Identity Center 中取得使用者的臨時登入資料。

AWS 存取入口網站為 IAM Identity Center 使用者提供存取其 AWS 帳戶 和雲端應用程式的單一登入。以 IAM Identity Center 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，您可以在 AWS CLI AWS SDKs 中使用登入資料，也稱為 IAM Identity Center 使用者登入資料，以存取中的資源 AWS 帳戶。

如果您使用 AWS CLI 以程式設計方式存取 AWS 服務，您可以使用本主題中的程序來啟動對的存取 AWS CLI。如需的詳細資訊 AWS CLI，請參閱[AWS Command Line Interface 《使用者指南》](#)。

如果您使用 AWS SDKs 以程式設計方式存取 AWS 服務，遵循本主題中的程序也會直接建立 AWS SDKs 的身分驗證。如需 AWS SDKs 的相關資訊，請參閱[AWS SDKs和工具參考指南](#)。

Note

IAM Identity Center 中的使用者與 [IAM 使用者](#) 不同。IAM 使用者會獲得 AWS 資源的長期登入資料。IAM Identity Center 中的使用者會獲得臨時登入資料。我們建議您使用暫時登入資料做為存取的安全最佳實務，AWS 帳戶 因為這些登入資料會在每次登入時產生。

先決條件

若要取得 IAM Identity Center 使用者的臨時登入資料，您需要下列項目：

- IAM Identity Center 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 Identity Center 並建立 IAM Identity Center 使用者的詳細資訊，請參閱 [透過 IAM Identity Center 開始使用](#)。
- 使用者存取 AWS 帳戶- 若要授予 IAM Identity Center 使用者擷取其臨時憑證的許可，您或管理員必須將 IAM Identity Center 使用者指派給[許可集](#)。許可集存放在 IAM Identity Center 中，並定義 IAM

Identity Center 使用者對 的存取層級 AWS 帳戶。如果您的管理員為您建立了 IAM Identity Center 使用者，請他們為您新增此存取權。如需詳細資訊，請參閱[將使用者或群組存取權指派給 AWS 帳戶](#)。

- AWS CLI 已安裝 – 若要使用暫時登入資料，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

在您完成為 IAM Identity Center 使用者取得臨時登入資料的步驟之前，請記住下列注意事項：

- IAM Identity Center 建立 IAM 角色 – 當您將 IAM Identity Center 中的使用者指派給許可集時，IAM Identity Center 會從許可集建立對應的 IAM 角色。由許可集建立的 IAM 角色與在 中建立 AWS Identity and Access Management 的 IAM 角色不同，方式如下：
 - IAM Identity Center 擁有並保護由許可集建立的角色。只有 IAM Identity Center 可以修改這些角色。
 - 只有 IAM Identity Center 中的使用者可以擔任與其指派許可集對應的角色。您無法將許可集存取權指派給 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 Identity Center 外部[的主體](#)。

如需有關如何取得您在 IAM 中建立之角色的臨時登入資料的資訊，請參閱AWS Identity and Access Management 《使用者指南》中的[使用臨時安全登入資料搭配 AWS CLI](#)。

- 您可以設定許可集的工作階段持續時間 – 登入 AWS 存取入口網站後，IAM Identity Center 使用者獲指派的許可集會顯示為可用角色。IAM Identity Center 會為此角色建立單獨的工作階段。此工作階段可以是 1 到 12 小時，取決於為許可集設定的工作階段持續時間。預設工作階段持續時間為一小時。如需詳細資訊，請參閱[設定的工作階段持續時間 AWS 帳戶](#)。

取得和重新整理暫時登入資料

您可以自動或手動取得和重新整理 IAM Identity Center 使用者的臨時登入資料。

主題

- [自動登入資料重新整理（建議）](#)
- [手動登入資料重新整理](#)

自動登入資料重新整理（建議）

自動登入資料重新整理使用 Open ID Connect (OIDC) 裝置程式碼授權標準。使用此方法，您可以使用中的 `aws configure sso` 命令直接啟動存取 AWS CLI。您可以使用此命令，自動存取與指派給任何之任何許可集相關聯的任何角色 AWS 帳戶。

若要存取為 IAM Identity Center 使用者建立的角色，請執行 `aws configure sso` 命令，然後從 AWS CLI 瀏覽器視窗授權。只要您有作用中的 AWS 存取入口網站工作階段，AWS CLI 會自動擷取臨時登入資料，並自動重新整理登入資料。

如需詳細資訊，請參閱 AWS Command Line Interface 《使用者指南》中的[使用 設定您的設定檔aws configure sso wizard](#)。

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。如果您建立了 IAM Identity Center 使用者，AWS 請傳送電子郵件邀請，其中包含您的登入 URL。如需詳細資訊，請參閱[登入使用者指南中的登入 AWS 存取入口網站](#)。AWS
2. 在帳戶索引標籤中，找到您要 AWS 帳戶 從中擷取登入資料的。當您選擇帳戶時，與帳戶相關聯的帳戶名稱、帳戶 ID 和電子郵件地址都會出現。

Note

如果您未看到任何 AWS 帳戶列出的項目，則可能尚未指派給該帳戶的許可集。在這種情況下，請聯絡您的管理員，並要求他們為您新增此存取權。如需詳細資訊，請參閱[將使用者或群組存取權指派給 AWS 帳戶](#)。

3. 在帳戶名稱下方，您的 IAM Identity Center 使用者獲指派的許可集會顯示為可用角色。例如，如果您的 IAM Identity Center 使用者指派給帳戶的 PowerUserAccess 許可集，該角色會在 AWS 存取入口網站中顯示為 PowerUserAccess。
4. 根據角色名稱旁的選項，選擇存取金鑰，或選擇命令列或程式設計存取。
5. 在取得登入資料對話方塊中，根據您安裝的作業系統，選擇 macOS 和 Linux、Windows 或 PowerShell AWS CLI。
6. 在 AWS IAM Identity Center 登入資料（建議）下，SSO Region 會顯示您的 SSO Start URL 和。設定已啟用 IAM Identity Center 的設定檔和 `sso-session` 時，需要這些值 AWS CLI。若要完成此組態，請遵循 AWS Command Line Interface 《使用者指南》中的[使用 設定設定檔aws configure sso wizard](#)中的指示。

AWS CLI 視需要繼續使用，AWS 帳戶 直到登入資料過期為止。

手動登入資料重新整理

您可以使用手動登入資料重新整理方法來取得與特定 中特定許可集相關聯之角色的臨時登入資料 AWS 帳戶。若要這樣做，請複製並貼上臨時登入資料所需的命令。使用此方法，您必須手動重新整理暫時登入資料。

您可以執行 AWS CLI 命令，直到暫時登入資料過期為止。

若要取得您手動重新整理的登入資料

1. 使用管理員提供的特定登入 URL 登入 AWS 存取入口網站。如果您建立了 IAM Identity Center 使用者，AWS 請傳送電子郵件邀請，其中包含您的登入 URL。如需詳細資訊，請參閱 [登入使用者指南中的登入 AWS 存取入口網站](#)。AWS
2. 在帳戶索引標籤中，找到您要 AWS 帳戶 從中擷取存取憑證的，然後將其展開以顯示 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

如果您未看到任何AWS 帳戶列出的項目，則可能尚未指派給該帳戶的許可集。在這種情況下，請聯絡您的管理員，並要求他們為您新增此存取權。如需詳細資訊，請參閱[將使用者或群組存取權指派給 AWS 帳戶](#)。

3. 在取得登入資料對話方塊中，選擇 MacOS 和 Linux、Windows 或 PowerShell，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登入資料設定，包括credentials檔案和config檔案中的任何設定。如需詳細資訊，請參閱AWS CLI 《使用者指南》中的[設定的環境變數 AWS CLI](#)。

若要使用此選項，請將命令複製到剪貼簿、將命令貼到您的 AWS CLI 終端機視窗，然後按 Enter 設定所需的環境變數。

- 選項 2：將設定檔新增至您的 AWS 登入資料檔案

選擇此選項，以使用不同的登入資料集執行命令。

若要使用此選項，請將命令複製到剪貼簿，然後將命令貼到您的共用 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 SDKs [和工具參考指南中的共用組態和登入資料檔案](#)。若要使用此登入資料，請在 AWS CLI 命令中指定 `--profile` 選項。這會影響使用相同登入資料檔案的所有環境。

- 選項 3：在您的 AWS 服務用戶端中使用個別值

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 [在 AWS 上建置的工具](#)。

若要使用此選項，請將值複製到剪貼簿、將值貼到您的程式碼中，並將它們指派給 SDK 的適當變數。如需詳細資訊，請參閱特定 SDK API 的文件。

建立 AWS 管理主控台 目的地的捷徑連結

在 AWS 存取入口網站中建立的捷徑連結會將 IAM Identity Center 使用者帶到 中的特定目的地 AWS 管理主控台、具有特定許可集，以及特定 中的特定目的地 AWS 帳戶。

捷徑連結可為您和您的協作者節省時間。透過包括 AWS 存取入口網站的多頁導覽至 AWS 管理主控台（例如，Amazon S3 儲存貯體執行個體頁面）中所需的目的地 URL，您可以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，在此處依優先順序列出：

- （選用）捷徑連結中 AWS 管理主控台 指定的 中的任何目的地 URL。例如，Amazon S3 儲存貯體執行個體頁面。
- （選用）管理員為有問題的許可集設定的轉送狀態 URL。如需設定轉送狀態的詳細資訊，請參閱 [設定轉送狀態以快速存取 AWS 管理主控台](#)。
- AWS 管理主控台 首頁。如果您未指定目的地，則預設目的地為。

Note

只有當您已向 IAM Identity Center 進行身分驗證，並已為 AWS 帳戶和目的地 URL 指派必要的許可集時，才會成功自動導覽至目的地。

AWS 存取入口網站包含建立捷徑按鈕，可協助您建立可共用的捷徑連結。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 複製到剪貼簿以進行共用。

在 AWS 存取入口網站中建立捷徑連結

1. 登入 AWS 存取入口網站時，請選擇帳戶索引標籤，然後選擇建立捷徑按鈕。
2. 在對話方塊中：
 - a. AWS 帳戶 使用帳戶 ID 或帳戶名稱選擇。當您輸入時，下拉式選單會顯示您可以存取的相符帳戶 IDs 和名稱。您只能選擇您有權存取的帳戶。
 - 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許可集。如果您省略選擇角色，系統會提示使用者在使用捷徑連結時，為所選帳戶選取指派給他們的角色。

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許可集。如果使用者沒有為帳戶和目的地 URL 指派的必要許可集，則會拒絕他們存取。

- 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，則會根據先前提到的捷徑連結目的地選項，在使用捷徑連結時自動判斷目的地。
- d. 您的捷徑連結會根據您的輸入，在對話方塊底部產生。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，或與具有相同許可集或其他足夠許可集之相同帳戶的協作者共用書籤。

使用 URL 編碼建構安全 AWS 管理主控台 捷徑連結

URL 的所有參數值，包括帳戶 ID、許可集名稱和目的地 URL，都必須以 URL 編碼。

捷徑連結會以下列路徑延伸 AWS 存取入口網站 URL：

/#/console?

account_id=[*account_ID*]&role_name=[*permission_set_name*]&destination=[*destination*]

傳統 AWS 分割區中的完整 URL 遵循此模式：

IPv4 端點：

https://[*your_subdomain*].awsapps.com/start/#/console?

account_id=[*account_ID*]&role_name=[*permission_set_name*]&destination=[*destination*]

雙堆疊端點

`https://[identity_center_instance_id].portal.[region].app.aws/#/console?account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination]`

以下是範例捷徑連結，123456789012使用 S3FullAccess 許可集將使用者登入 帳戶，並將他們帶到 S3 主控台首頁：

- IPv4 端點： `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- 雙堆疊端點： `https://ssoins-1234567890abcdef.portal.us-east-1.app.aws/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) IPv4 端點： `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`
- (AWS GovCloud (US) Region) 雙堆疊端點： `https://ssoins-1234567890abcdef.portal.us-gov-west-1.app.aws/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

為您的裝置註冊 MFA

對於 Identity Center 目錄中的使用者，請使用 AWS 存取入口網站中的下列程序來註冊新裝置以進行多重驗證 (MFA)。

Important

IAM Identity Center 中的 MFA 目前不支援[外部身分提供者](#)。

開始之前

建議您在開始此程序中的步驟之前，先將適當的 Authenticator 應用程式下載至您的裝置。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

註冊您的裝置以搭配 MFA 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，選取下列其中一個 MFA 裝置類型，然後遵循指示：

- 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 裝置的組態資訊，包括 QR 碼圖形。圖形是秘密金鑰的表示，可在不支援 QR 代碼的裝置上手動輸入。
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. 判斷 MFA 應用程式是否支援 QR 代碼，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，您可以選擇攝影機圖示或選擇類似於掃描碼的選項。然後使用裝置的攝影機掃描程式碼。
 - ii. 選擇顯示私密金鑰，然後在 MFA 應用程式中輸入該私密金鑰。

⚠ Important

當您為 IAM Identity Center 設定 MFA 裝置時，建議您將 QR 碼或私密金鑰的副本儲存在安全的地方。如果您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。如果發生上述任一情況，您可以快速重新設定應用程式以使用相同的 MFA 組態。

3. 在設定驗證器應用程式頁面的驗證器程式碼下，輸入目前出現在實體 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，然後等待太久才提交請求，則 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 搭配使用 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，遵循瀏覽器或平台提供的指示。

 Note

體驗因瀏覽器或平台而異。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。

檢視和結束作用中工作階段

您可以使用 AWS 存取入口網站來檢視作用中工作階段的清單，並視需要結束一或多個工作階段。

使用 AWS 存取入口網站結束作用中的工作階段

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，選擇安全性。
3. 在安全頁面上，作用中工作階段旁的括號中的數字會指出您有多少作用中工作階段。選取您要結束的每個工作階段旁的核取方塊，然後選擇結束工作階段。

 Tip

對於使用者背景工作階段，您可以依使用工作階段之任務的 Amazon Resource Name (ARN) 搜尋工作階段。在工作階段類型清單中，選擇使用者背景工作階段，然後在搜尋方塊中輸入任務 ARN。

您只能結束載入的作用中工作階段。如果您有多個工作階段，請選擇載入更多作用中工作階段以顯示其他工作階段。

4. 選取您要結束的每個工作階段旁的核取方塊，然後選擇結束工作階段。
5. 隨即出現對話方塊，確認您正在結束作用中的工作階段。檢閱資訊，如果您想要繼續，請輸入 `confirm`，然後選擇結束工作階段。
6. 系統會將您返回作用中工作階段的清單。會出現綠色通知訊息，指出選取的工作階段已成功結束。

跨多個 使用 IAM Identity Center AWS 區域

本主題說明如何 AWS IAM Identity Center 跨多個 使用 AWS 區域。了解如何將執行個體複寫至其他區域、管理人力資源存取和工作階段、部署應用程式，以及在服務中斷期間維護帳戶存取。

當您啟用 IAM Identity Center 的組織執行個體時，您可以選擇單一 AWS 區域（主要區域）。AWS 區域 如果符合特定先決條件，您可以將此執行個體複寫至其他。IAM Identity Center 會自動將人力資源身分、許可集、使用者和群組指派、工作階段和其他中繼資料從主要區域複寫到所選的其他區域。

多區域支援的優點

將 IAM Identity Center 複寫至其他 AWS 區域 提供兩個主要優點：

- 改善 AWS 帳戶 存取的彈性 – 即使 IAM Identity Center 執行個體在其主要區域中發生服務中斷，您的人力資源也可以存取其 AWS 帳戶。這適用於在中斷之前佈建許可的存取。
- 為 AWS 受管應用程式選擇部署區域的增強彈性 – 您可以在偏好的區域中部署 AWS 受管應用程式，以滿足應用程式資料駐留需求，並透過與使用者的距離提升效能。部署在其他區域中的應用程式會在本機存取複寫的人力資源身分，以獲得最佳效能和可靠性。

先決條件和考量事項

在複寫 IAM Identity Center 執行個體之前，請確定符合下列要求：

- 執行個體類型 - 您的 IAM Identity Center 執行個體必須是[組織執行個體](#)。[帳戶執行個體](#)中無法使用多區域支援。
- 身分來源 - 您的 IAM Identity Center 執行個體必須連線至外部身分提供者 (IdP)，例如 [Okta](#)。多區域支援不適用於使用 [Active Directory](#) 或 [Identity Center 目錄](#) 做為身分來源的執行個體。
- AWS 區域 - 多區域支援可在您的 [中預設啟用的商業區域中](#) 使用 AWS 帳戶。目前不支援選擇加入區域。
- 靜態加密的 KMS 金鑰類型 - 您的 IAM Identity Center 執行個體必須使用多區域[客戶受管 KMS 金鑰](#)設定。KMS 金鑰必須位於與 IAM Identity Center 相同的 AWS 帳戶中。如需詳細資訊，請參閱[在中實作客戶受管 KMS 金鑰 AWS IAM Identity Center](#)。
- AWS 受管應用程式相容性 - 造訪 中的應用程式資料表[the section called “您可以搭配 IAM Identity Center 使用的應用程式”](#)，以確認下列兩個應用程式需求：

- 組織正在使用的所有 AWS 受管應用程式都必須支援使用客戶受管 KMS 金鑰設定的 IAM Identity Center。
- 您想要在其他區域中部署的 AWS 受管應用程式必須支援這種類型的部署。
- 外部 IdP 相容性 - 若要充分利用多區域支援，外部 IdP 必須支援多個聲明消費者服務 (ACS) URLs。這是 IdPs 支援的 SAML 功能，例如 Okta、Microsoft Entra ID、PingFederate、PingOne 和 JumpCloud。

如果您使用的 IdP 不支援多個 ACS URLs，例如 Google Workspace，我們建議您與 IdP 供應商合作以啟用此功能。如需在沒有多個 ACS URLs 的情況下可用的選項，請參閱 [the section called “使用沒有多個 ACS URLs AWS 受管應用程式”](#) 和 [the section called “AWS 帳戶 在沒有多個 ACS URLs 存取彈性”](#)。

選擇其他區域

在預設啟用的商業區域之間選擇其他區域時，請考慮下列因素：

- 合規要求 – 如果您需要執行 AWS 受管應用程式，因為合規原因而存取僅限特定區域的資料集，請選擇資料集所在的區域。
- 效能最佳化 – 如果資料駐留不是一個因素，請選取最接近您應用程式使用者的 區域，以最佳化其體驗。
- 應用程式支援 – 驗證您選擇的區域是否提供所需的 AWS 應用程式。
- AWS 帳戶 存取彈性 – 若要持續存取 AWS 帳戶，請選擇地理上與 IAM Identity Center 執行個體主要區域相距的區域。

Note

IAM Identity Center 對 的數量有配額 AWS 區域。如需詳細資訊，請參閱[the section called “其他配額”](#)。

將 IAM Identity Center 複寫至其他區域

如果您的環境符合[先決條件](#)，例如使用多區域客戶受管 KMS 金鑰設定 IAM Identity Center，請完成下列步驟，將 IAM Identity Center 執行個體複寫至其他區域。在這些步驟期間和之後，您的主要區域會繼續正常運作。

步驟 1：在其他區域中建立複本金鑰

將 IAM Identity Center 複寫到區域之前，您必須先在該區域中建立客戶受管 KMS 金鑰的複本金鑰，並使用 IAM Identity Center 操作所需的許可來設定複本金鑰。如需建立多區域複本金鑰的說明，請參閱[建立多區域複本金鑰](#)。

KMS 金鑰許可的建議方法是從主要金鑰複製金鑰政策，這會授予在主要區域中為 IAM Identity Center 建立的相同許可。或者，您可以定義區域特定的金鑰政策，雖然此方法會增加跨區域管理許可的複雜性，而且未來更新政策時可能需要額外的協調。

Note

AWS KMS 不會同步多區域 KMS 金鑰跨區域的 KMS 金鑰政策。若要讓 KMS 金鑰政策跨 KMS 金鑰區域保持同步，您需要個別在每個區域中套用變更。

步驟 2：在 IAM Identity Center 中新增區域

在 IAM Identity Center 中新增區域會觸發 IAM Identity Center 資料的自動複寫至該區域。複寫與最終一致性是非同步的。下列索引標籤提供在 AWS 管理主控台 和 中執行此操作的說明 AWS CLI。

Console

新增區域

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在導覽窗格中，選擇設定。
3. 選擇 Management (管理) 標籤，
4. 在 IAM Identity Center 的區域區段中，選擇新增區域。
5. 在AWS 區域 可用於複寫的 區段中，選擇您偏好的 AWS 區域。如果 區域未出現在清單中，則無法複寫，因為 KMS 金鑰尚未複寫。如需詳細資訊，請參閱[the section called “實作客戶受管 KMS 金鑰”](#)。
6. 選擇新增區域。
7. 在 IAM Identity Center 的區域區段中，監控區域狀態。視需要使用重新整理按鈕（圓形箭頭）檢查最新的區域狀態。複寫完成後，請繼續步驟 2。

AWS CLI

新增區域

```
aws sso-admin add-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

檢查目前區域狀態

```
aws sso-admin describe-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

當區域狀態為 ACTIVE 時，您可以繼續進行步驟 2。

初始複寫至其他區域的持續時間取決於 IAM Identity Center 執行個體中的資料量。在大多數情況下，後續增量變更會在幾秒內複寫。

步驟 3：更新外部 IdP 設定

請遵循 中外部 IdP 的教學[身分來源教學課程](#)課程進行下列步驟：

步驟 3.a：將宣告消費者服務 (ACS) URLs 新增至外部 IdP

此步驟會啟用每個額外區域的直接登入，並且需要啟用在這些區域中部署的 AWS 受管應用程式的登入，以及 AWS 帳戶透過這些區域存取。若要了解在何處尋找 ACS URLs，請參閱 [主要和其他 中的 ACS 端點 AWS 區域](#)。

步驟 3.b（選用）：在外部 IdP 入口網站 AWS 存取入口網站 中提供

在外部 IdP 入口網站 AWS 存取入口網站 中，將其他區域中的 設為書籤應用程式。書籤應用程式僅包含所需目的地的連結 (URL)，類似於瀏覽器書籤。您可以在 IAM Identity Center 區域區段中選擇檢視 allURL，AWS 存取入口網站 URLs 以在 主控台中找到 URL。AWS 存取入口網站 URLs 如需詳細資訊，請參閱[the section called “AWS 主要和其他 中的存取入口網站端點 AWS 區域”](#)。

IAM Identity Center 在每個額外的區域中支援 IdP 起始的 SAML SSO，但外部 IdPs 通常僅支援單一 ACS URL。為了持續性，我們建議讓主要區域的 ACS URL 用於 IdP 起始的 SAML SSO，並依賴書籤應用程式和瀏覽器書籤來存取其他區域。

步驟 4：確認防火牆和閘道允許清單

在防火牆或閘道中檢閱您的網域允許清單，並根據[記錄的允許清單](#)進行更新。

步驟 5：提供資訊給您的使用者

為您的使用者提供有關新設定的資訊，包括其他區域中的 AWS 存取入口網站 URL，以及如何使用其他區域。如需相關詳細資訊，請參閱下列各節：

- [the section called “透過其他 區域的人力資源存取”](#)
- [the section called “容錯移轉至其他 區域以進行 AWS 帳戶 存取”](#)
- [the section called “在多個 之間部署和管理應用程式 AWS 區域”](#)

新增第一個區域以外的區域變更

您可以新增和移除其他區域。除了刪除整個 IAM Identity Center 執行個體之外，無法移除主要區域。如需移除區域的詳細資訊，請參閱 [the section called “從 IAM Identity Center 移除區域”](#)。

您無法將其他區域提升為主要區域，或將主要區域降級為其他區域。

複寫哪些資料？

IAM Identity Center 會複寫下列資料：

資料	複寫來源和目標
人力身分（使用者、群組、群組成員資格）	從主要區域到其他區域
許可集及其對使用者和群組的指派	從主要區域到其他區域
組態（例如外部 IdP SAML 設定）	從主要區域到其他區域
使用者和群組的應用程式中繼資料和應用程式指派	從應用程式的連線 IAM Identity Center 區域到其他已啟用的區域
受信任權杖發行者	從主要區域到其他區域

資料	複寫來源和目標
工作階段	從工作階段的原始區域到其他已啟用的區域

Note

IAM Identity Center 不會複寫存放在 AWS 受管應用程式中的資料。此外，它不會變更應用程式部署的區域足跡。例如，如果您在美國東部（維吉尼亞北部）的 IAM Identity Center 執行個體，且您已在相同區域中部署 Amazon Redshift，則將 IAM Identity Center 複寫至美國西部（奧勒岡）不會影響 Amazon Redshift 的部署區域及其存放的資料。

考量：

- 跨已啟用區域的全域資源識別符 - 使用者、群組、許可集和其他資源在已啟用的區域具有相同的識別符。
- 複寫不會影響佈建的 IAM 角色 - 從許可集指派佈建的現有 IAM 角色，會在任何已啟用區域的帳戶登入期間使用。

透過其他 區域的人力資源存取

本節說明當您在多個區域中啟用 IAM Identity Center 時 AWS 帳戶，您的人力資源如何存取 AWS 存取入口網站、和 應用程式。

其他區域中 AWS 存取入口網站 的 會以與主要區域中相同的方式顯示您的人力資源可存取的 AWS 帳戶和應用程式。您的人力資源可以透過 AWS 存取入口網站 直接連結至區域入口網站端點（例如，<https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com>），或透過您在外部 IdP 中設定的 [書籤應用程式](#)，在其他區域中登入。

您可以使用其他區域中的 AWS 存取入口網站 端點，授權 AWS CLI 以 IAM Identity Center 使用者身分存取 APIs。此功能的運作方式與主要區域相同。不過，CLI 授權不會跨已啟用的區域複寫。因此，您必須個別授權每個區域中的 CLI。

跨多個 的使用者工作階段 AWS 區域

IAM Identity Center 會將使用者工作階段從原始區域複寫到其他已啟用的區域。一個區域中的工作階段撤銷和登出也會複寫到其他區域。

IAM Identity Center 管理員撤銷工作階段

IAM Identity Center 管理員可以在其他區域中撤銷使用者工作階段。當跨區域複寫工作階段時，在正常情況下，撤銷單一區域中的工作階段就足夠，並讓 IAM Identity Center 將變更複寫到其他已啟用的區域。如果 IAM Identity Center 的主要區域發生中斷，管理員可以在其他區域中執行此操作。

AWS 存取入口網站 主要和額外 中的 端點 AWS 區域

如果您需要查詢已啟用區域的 AWS 存取入口網站 URLs，請遵循下列步驟：

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在導覽窗格中，選擇設定。
3. 選擇 Management (管理) 標籤，
4. 在 IAM Identity Center 的區域區段中，選擇檢視所有 AWS 存取入口網站 URLs。

下表指定 IAM Identity Center 執行個體之主要和其他區域的 AWS 存取入口網站 端點。

AWS 存取入口網站 endpoint	主要區域	其他區域	URL 模式和範例
僅限傳統 IPv4 ¹	是	否	模式： <code>https://[Identity Store ID].awsapps.com/start</code> 範例： <code>https://d-12345678.awsapps.com/start</code>
僅限自訂別名 IPv4 ¹	是 (選用)	否	模式： <code>https://[custom alias].awsapps.com/start</code> 範例： <code>https://mycompany.awsapps.com/start</code>
僅限替代 IPv4 ²	是	是	模式： <code>https://[Identity Center instance ID].[Region].amazonaws.com</code>

AWS 存取入口網站 endpoint	主要區域	其他區域	URL 模式和範例
			範例：https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com
雙堆疊 ²	是	是	模式：https://[<i>Identity Center instance ID</i>].portal.[<i>Region</i>].app.aws 範例：https://ssoins-111111h2222j33pp.portal.eu-west-1.app.aws

¹ 在其他區域中，不支援自訂別名，且awsapps.com父網域無法使用。

² 替代的僅限 IPv4 和雙堆疊入口網站端點在 URL /start中沒有結尾。

主要和其他 中的聲明消費者服務 (ACS) 端點 AWS 區域

如果您需要查詢 ACS URLs 或將其下載為 SAML 中繼資料的一部分，請遵循下列步驟：

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在導覽窗格中，選擇設定。
3. 選擇身分來源索引標籤。
4. 在動作下拉式功能表中，選擇管理身分驗證。
5. 服務提供者中繼資料區段會顯示每個已啟用區域的 AWS 存取入口網站 和 ACS URL。IPv4-only 和雙堆疊 URLs 會顯示在不同的索引標籤上。如果您的 IdP 支援上傳 SAML 中繼資料檔案，您可以選擇下載中繼資料檔案，以下載具有所有 ACS URLs SAML 中繼資料檔案。如果您的 IdP 不支援上傳中繼資料檔案，或者您偏好個別新增 ACS URLs，您可以從主控台的資料表複製個別 URLs，或選擇檢視 ACS URLs，然後選擇複製所有 URLs。保留已為主要區域設定的 ACS URL，以確保服務供應商從主要區域起始的 SAML 單一登入保持正常運作。

下表指定 IAM Identity Center 執行個體之主要和其他區域的 SAML 聲明消費者服務 (ACS) 端點：

ACS 端點	主要區域	其他區域	URL 模式和範例
僅限 IPv4	是	是	模式：https://[<i>Region</i>].signin.aws/platform/saml/acs/ [<i>Tenant ID</i>] 範例： https://us-west-2.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111
僅限替代 IPv4*	是	否	模式：https://[<i>Region</i>].signin.aws.amazon.com/platform/saml/acs/ [<i>Tenant ID</i>] 範例： https://us-west-2.signin.aws.amazon.com/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111
雙堆疊	是	是	模式：https://[<i>Region</i>].sso.signin.aws/platform/saml/acs/[<i>Tenant ID</i>] 範例： https://us-west-2.sso.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111

* 對於在 2026 年 2 月之前啟用的執行個體，請保留此端點，因為服務供應商起始的主要區域的 SAML 單一登入需要它。IAM Identity Center 不會將此端點用於 2026 年 2 月或之後啟用的執行個體。

使用沒有多個 ACS URLs AWS 受管應用程式

有些外部身分提供者 (IdPs) 在其 IAM Identity Center 應用程式中不支援多個聲明消費者服務 (ACS) URLs。多個 ACS URLs 是直接登入多區域 IAM Identity Center 中特定區域所需的 SAML 功能。

例如，如果您透過應用程式連結啟動 AWS 受管應用程式，系統會透過應用程式的連線 IAM Identity Center 區域觸發登入。不過，如果未在外部 IdP 中設定該區域的 ACS URL，則登入會失敗。

若要解決此問題，請與您的 IdP 廠商合作，以啟用多個 ACS URLs 的支援。同時，您仍然可以在其他區域中使用 AWS 受管應用程式。首先，登入其 ACS URL 在外部 IdP 中設定的區域（預設為主要區域）。在 IAM Identity Center 中擁有作用中工作階段後，您可以從任何已啟用區域的 AWS 存取入口網站或透過應用程式連結啟動應用程式。

容錯移轉至其他 區域以進行 AWS 帳戶 存取

透過 IAM Identity Center AWS 帳戶 存取的主題廣泛涵蓋在 [AWS 帳戶 存取](#)。本節提供在主要區域中發生服務中斷 AWS 區域 時，維護跨多個 AWS 帳戶 存取的其他詳細資訊。

如果您的 IAM Identity Center 執行個體在主要區域遇到中斷（例如，主要區域中的 AWS 存取入口網站無法使用），您的人力資源可以切換到其他區域，以繼續存取 AWS 帳戶和不受影響的應用程式。如需詳細資訊，請參閱[the section called “透過其他 區域的人力資源存取”](#)。

我們建議您在完成 中的設定後，立即將其他區域中的 AWS 存取入口網站 端點和外部 IdP 設定（例如其他區域的書籤應用程式）傳達給員工[the section called “將 IAM Identity Center 複寫至其他區域”](#)。這將使它們準備好在需要時容錯移轉到其他區域。

同樣地，我們建議 AWS CLI 使用者為主要區域擁有的每個[AWS CLI 設定檔](#)建立其他區域的設定檔。然後，如果主要區域中發生服務中斷，他們可以切換到該設定檔。

Note

對 AWS 帳戶的持續存取也取決於外部 IdP 的運作狀態和許可，例如在服務中斷之前佈建和複寫的許可集指派和群組成員資格。我們建議您的組織也設定[AWS 中斷玻璃存取](#)，以在外部 IdP 發生服務中斷時維持對一小群特殊權限使用者的 AWS 存取。[緊急存取](#)是類似的選項，可避免使用 IAM 使用者，但也取決於外部 IdP。

AWS 帳戶 在沒有多個 ACS URLs存取彈性

有些外部身分提供者 IdPs) 在其 IAM Identity Center 應用程式中不支援多個聲明消費者服務 (ACS) URLs。多個 ACS URLs 是直接登入多區域 IAM Identity Center 中特定區域所需的 SAML 功能。

若要讓使用者 AWS 帳戶 透過多個 IAM Identity Center 區域存取，您必須在外部 IdP 中設定個別的區域 ACS URLs。不過，如果外部 IdP 在其 IAM Identity Center 應用程式中僅支援單一 ACS URL，則使用者可以直接登入單一 IAM Identity Center 區域。

若要解決此問題，請與您的 IdP 廠商合作，以啟用多個 ACS URLs 的支援。同時，您可以使用其他區域做為 存取的備份 AWS 帳戶。

如果主要區域發生 IAM Identity Center 服務中斷，您必須使用其他區域的 ACS URL 更新外部 IdP 中的 ACS URL。在此更新之後，您的使用者可以使用外部 IdP 入口網站中現有的 IAM Identity Center 應用程式，或透過您與他們共用的直接連結，存取其他區域中的 AWS 存取入口網站。

我們建議您定期測試此設定，以確保它在需要時有效，並將此容錯移轉程序傳達給您的組織。

Note

在此設定 AWS 帳戶 中使用其他區域存取時，您的使用者可能無法存取連線至主要區域的 AWS 受管應用程式。因此，我們建議這僅做為維護存取權的暫時措施 AWS 帳戶。

跨多個 AWS 區域部署和管理應用程式

透過 IAM Identity Center 存取應用程式的主題廣泛涵蓋在 [應用程式存取權限](#)。本節提供與跨多個應用程式部署和管理相關的其他詳細資訊 AWS 區域。

在多個 之間部署和管理 AWS 受管應用程式 AWS 區域

使用單一區域 IAM Identity Center 執行個體，您可以在與執行個體相同的區域中部署 AWS 受管應用程式。Amazon Q Business 等某些應用程式支援與 IAM Identity Center 的跨區域連線，如果感興趣的應用程式可在 IAM Identity Center 區域外進行部署。不過，跨區域呼叫可能會導致應用程式效能變慢，而且大多數 AWS 受管應用程式不支援這種類型的連線。

多區域 IAM Identity Center 執行個體可讓您在任何已啟用的區域中部署 AWS 受管應用程式，並連線到相同區域中的 IAM Identity Center (「區域本機連線」)。所有整合的 AWS 受管應用程式都支援主要區域中的部署。若要確認哪些 AWS 受管應用程式支援在 IAM Identity Center 的其他區域中部署，請參閱中的應用程式資料表 [the section called “您可以搭配 IAM Identity Center 使用的應用程式”](#)。在任何情況下，AWS 受管應用程式都必須在您要部署它的區域中可用。

透過與 IAM Identity Center 的區域本機連線，AWS 受管應用程式會存取相同區域中的人力資源身分，以獲得最佳效能和可靠性。每當符合 [先決條件](#) 時，我們建議在部署 AWS 受管應用程式時選擇區域本機連線。

若要在 IAM Identity Center 的其他區域中部署 AWS 受管應用程式，請透過應用程式主控台或 API，以您在主要區域中部署的相同方式在該區域中啟動部署。

考量：

- 如果您尚未將 IAM Identity Center 複寫至該區域，建議您先執行此操作，以便應用程式部署可以立即完成。
- AWS 如果您已將 IAM Identity Center 複寫至 區域，在許多情況下，受管應用程式會自動建立區域本機連線。
- 如果 AWS 受管應用程式提供 IAM Identity Center 的跨區域連線，我們建議您選擇區域本機連線，前提是符合[先決條件](#)。
- 如果應用程式不支援在其他區域中進行部署，您可以在主要區域中進行部署，前提是該應用程式可在該區域中使用。

Important

如果您的 IAM Identity Center 執行個體為多區域，則無論應用程式部署區域為何，組織使用的所有 AWS 受管應用程式都必須支援使用客戶受管 KMS 金鑰設定的 IAM Identity Center。在部署應用程式[the section called “您可以搭配 IAM Identity Center 使用的應用程式”](#)之前，以及在 IAM Identity Center 中設定客戶受管 KMS 金鑰之前，請在 中確認這一點。

應用程式管理區域

使用區域本機連線在 IAM Identity Center 的其他區域中部署 AWS 受管應用程式後，您可以管理應用程式及其對相同區域中使用者和群組的指派。IAM Identity Center 會複寫應用程式中繼資料，包括將使用者和群組指派給其他已啟用的區域，讓您的員工可以從任何已啟用的區域啟動應用程式。

如果您的 AWS 受管應用程式使用 IAM Identity Center 的跨區域連線，您可以透過連線區域中的 IAM Identity Center 主控台和 API，管理應用程式詳細資訊，例如名稱和描述，以及使用者和群組的應用程式指派。無論連線類型為何，您都可以透過其部署區域中的主控台來管理應用程式。

信任的身分傳播

您可以在 IAM Identity Center 執行個體的任何已啟用區域中，將受信任的身分傳播與支援它的 AWS 受管應用程式搭配使用。

將身分內容傳播到彼此的所有應用程式都必須位於相同的 區域。

應用程式對其連線 IAM Identity Center 區域的相依性

每個 AWS 受管應用程式都會在部署期間連線到特定 IAM Identity Center 區域。應用程式接著會根據該區域進行使用者登入，即使您的 IAM Identity Center 已在多個區域中啟用。如果您的 IAM Identity Center 在該區域中遇到中斷，使用者可能無法存取連接到該區域的 AWS 受管應用程式。

在多個 之間部署和管理客戶受管應用程式 AWS 區域

IAM Identity Center 支援 SAML 和 OAuth2 [客戶受管應用程式](#)。您可以選擇在 IAM Identity Center 執行個體的任何已啟用區域中建立它們。建立應用程式後，您可以管理應用程式及其對相同區域中使用者和群組的指派。

從 IAM Identity Center 移除區域

若要從 IAM Identity Center 執行個體中移除其他區域，請遵循下列步驟：

步驟 1：更新外部 IdP 組態

您可以選擇從外部 IdP 中移除此區域的 ACS URL，或保留該 URL，以防稍後要再次新增此區域。建議您移除或隱藏您可能在此區域中為 建立 AWS 存取入口網站 的書籤應用程式。

步驟 2：移除區域

Console

新增區域

1. 開啟 [IAM Identity Center 主控台](#)。
2. 在導覽窗格中，選擇設定。
3. 選擇 Management (管理) 標籤，
4. 在 IAM Identity Center 的區域區段中，選擇您要移除的其他區域。
5. 選擇移除。
6. 選擇移除區域來確認移除之前，請注意在此 IAM Identity Center 區域中建立之應用程式可能無法存取的警告。如果您不確定您是否擁有此類應用程式，請在導覽窗格中選擇應用程式，並確認每個 AWS 受管和客戶受管應用程式的從建立欄中的連線區域。

Note

即使您無法存取這些應用程式，對於仍連線到已移除區域的 AWS 受管應用程式部署，仍可能會繼續產生費用。若要避免這種情況，您需要透過應用程式主控台或 API 移除這些 AWS 受管應用程式部署，才能移除 IAM Identity Center 中的區域。如果您已移除 IAM Identity Center 區域，您可以透過新增區域來還原對應用程式的存取。

7. 在 IAM Identity Center 的區域區段中，監控區域狀態。視需要使用重新整理按鈕（圓形箭頭）來查看最新的區域狀態。移除區域後，區域不會再出現在區域清單中。

AWS CLI

移除區域

```
aws sso-admin remove-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

若要檢查目前的區域狀態

```
aws sso-admin describe-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

移除區域時，請繼續步驟 2。

步驟 3：刪除複本金鑰

您可以選擇從此區域移除複本金鑰，以避免產生 KMS 儲存費用。如需詳細資訊，請參閱[刪除 AWS KMS 金鑰](#)。

⚠ Important

請務必僅刪除此特定區域中的複本金鑰。其他 IAM Identity Center 區域會繼續依賴其他啟用區域中的 KMS 金鑰進行正常操作。

其他 AWS 區域中支援的 IAM Identity Center 服務 APIs

API	其他區域中的功能
Identity Center API	支援： - 應用程式管理讀取/寫入操作 - 執行個體讀取操作 不支援： - 應用程式相關以外的任何寫入操作 - 許可集和帳戶指派讀取操作
Identity Store API	讀取操作
OIDC API	支援所有操作
存取入口網站 API	支援所有操作
SCIM API	不支援任何操作

AWS CloudTrail 主要和其他區域中 IAM Identity Center 的事件

在 中 AWS CloudTrail，您可以稽核 IAM Identity Center 使用者和管理員在已啟用 IAM Identity Center AWS 區域 執行個體的所有 中採取的動作。AWS CloudTrail 事件會發出並記錄在執行動作的區域中。如需詳細資訊，請參閱[the section called “日誌記錄和監控”](#)。

主要和其他區域中 IAM Identity Center 使用案例的可用性

功能	區域可用性
具有使用者入口網站的人力目錄	
使用者對 的存取，AWS 存取入口網站 包括入口網站登入和全域工作階段（適用於所有區域的單一登入）	所有啟用的區域

功能	區域可用性
顯示所有指派的帳戶	所有啟用的區域
顯示所有指派的應用程式（無論應用程式建立的位置為何）	所有啟用的區域
在 AWS 主控台或透過 Identity Store APIs 對使用者、群組和成員資格的讀取存取權	所有啟用的區域
撤銷使用者工作階段	所有啟用的區域
從外部身分來源自動同步使用者和群組，例如透過 SCIM API 或 Identity Store API 的外部 IdP	僅限主要區域
使用 SCIM 設定自動身分佈建	僅限主要區域
使用外部 IdP 設定 SAML SSO	僅限主要區域 - 透過主控台在所有啟用的區域中讀取存取權
透過主控台或 Identity Store APIs 建立 Create/update/delete 使用者、群組和群組成員資格的操作。	主要區域：透過 Identity Store API 提供，但在 SCIM API 用於佈建時在 IAM Identity Center 主控台中封鎖（停用/啟用使用者存取和刪除使用者除外，一律可用）。其他區域：無法使用
多帳戶存取	
透過 AWS 存取入口網站 AWS CLI、和捷徑連結存取指派的帳戶	所有啟用的區域
在主控台和 APIs（包括暫時提升存取）	僅限主要區域
存取應用程式 AWS 和服務	
透過應用程式主控台和 APIs 部署 AWS 受管應用程式	所有啟用的區域 – 受應用程式區域可用性和支援在其他區域中部署的限制
透過 Identity Center 主控台和 APIs 建立客戶受管應用程式	所有啟用的區域

功能	區域可用性
在主控台和 APIs 中管理應用程式中繼資料和指派	應用程式連線的 IAM Identity Center 區域
從 AWS 存取入口網站 或直接透過應用程式連結或書籤 啟動應用程式	所有啟用的區域
SSO 到 Amazon EC2 執行個體	所有啟用的區域
信任的身分傳播	
建立可信權杖發行者	僅限主要區域
受 AWS 管應用程式的受信任身分傳播	所有啟用的區域 - 將身分內容傳播到彼此的 應用程式必須位於相同的區域
其他管理功能	
所有其他管理功能，例如區域管理、KMS 金鑰管理、 執行個體管理和工作階段管理（工作階段撤銷除外）	僅限主要區域 - 某些資料可在所有啟用的 區域中存取讀取（不包括許可集指派）

彈性設計和區域行為

IAM Identity Center 服務受到完整管理，並使用高可用性和耐用 AWS 的服務，例如 Amazon S3 和 Amazon EC2。為了確保在可用區域中斷的情況下的可用性，IAM Identity Center 會在多個可用區域之間運作。您可以將 IAM Identity Center 執行個體複寫到其他區域，以便在發生區域中斷時，使用已佈建的許可維持帳戶存取。如需詳細資訊，請參閱[跨多個 使用 IAM Identity Center AWS 區域](#)。

您可以在 AWS Organizations 管理帳戶中啟用 IAM Identity Center。這是 IAM Identity Center 跨所有佈建、取消佈建和更新角色的必要項目 AWS 帳戶。當您啟用 IAM Identity Center 時，它會部署到目前選取的 AWS 區域，稱為「主要區域」。如果您想要部署到特定 AWS 區域，請在啟用 IAM Identity Center 之前變更區域選擇，因為在啟用 IAM Identity Center 之後無法變更主要區域。

IAM Identity Center 僅支援主要區域的大多數管理函數。這包括與外部身分提供者的連線、使用者和群組的同步，以及建立和指派許可集給使用者和群組。相反地，應用程式及其指派的管理必須在建立應用程式的 IAM Identity Center 區域中進行。

Note

即使您的 IAM Identity Center 已複寫至其他區域，仍建議您設定[AWS 碎片存取](#)。這可協助您在外部 IdP 的服務中斷等事件期間，維持一小組特殊權限使用者的 AWS 存取權。[緊急存取](#)是使用外部 IdP 而非 IAM 使用者的身分的另一個選項；不過，它無法防止外部 IdP 中的中斷。

雖然 IAM Identity Center 會決定您啟用服務所在區域的存取權，但 AWS 帳戶 是全域的。這表示使用者登入 IAM Identity Center 後，只要 AWS 帳戶 透過 IAM Identity Center 存取，就可以在任何區域中操作。不過，Amazon SageMaker AI 等大多數 AWS 受管應用程式必須安裝在 IAM Identity Center 執行個體的區域中，讓使用者驗證和指派這些應用程式的存取權。如需搭配 IAM Identity Center 使用應用程式時的區域限制條件資訊，請參閱應用程式和 的文件[the section called “在多個 之間部署和管理 AWS 受管應用程式 AWS 區域”](#)。

您也可以使用 IAM Identity Center 驗證和授權存取可透過公有 URL 連線的 SAML 型客戶受管應用程式，無論應用程式建置所在的平台或雲端為何。

我們不建議使用 [IAM Identity Center 的帳戶執行個體](#)。做為實作彈性的方法，因為它們不支援 AWS 帳戶存取，而且會建立未連線至組織執行個體的第二個隔離控制點。

專為可用性而設計

下表提供 IAM Identity Center 設計為在單一區域中實現的可用性 AWS。這些值不代表服務水準協議或保證，而是提供設計目標的洞見。可用性百分比參考對資料或函數的存取，而不是對耐用性的參考（例如，資料的長期保留）。

服務元件	可用性設計目標
資料平面（包括登入）	99.95%
控制平面	99.90%

設定 的緊急存取 AWS 管理主控台

IAM Identity Center 是以高度可用的 AWS 基礎設施建置而成，並使用可用區域架構來消除單一故障點。如需在 IAM Identity Center 發生罕見事件或 AWS 區域 中斷時多一層保護，建議您設定組態，以便使用來暫時存取 AWS 管理主控台。

AWS 可讓您：

- [將您的第三方 IdP 連接到 IAM Identity Center](#)。
- 使用 [SAML 2.0 型聯合](#) AWS 帳戶 將您的第三方 IdP 連接到個人。

如果您使用 IAM Identity Center，您可以使用這些功能來建立下列各節所述的緊急存取組態。此組態可讓您使用 IAM Identity Center 做為 AWS 帳戶 存取機制。如果 IAM Identity Center 中斷，您的緊急操作使用者可以使用存取其帳戶的相同登入資料，AWS 管理主控台 透過直接聯合登入。當 IAM Identity Center 無法使用，但 IAM 資料平面和外部身分提供者 (IdP) 可用時，此組態即可運作。如果您不想依賴外部 IdP，請考慮設定[AWS 碎片存取](#)

Important

我們建議您在中斷發生之前部署此組態，因為如果您建立所需 IAM 角色的存取權也中斷，則無法建立組態。此外，請定期測試此組態，以確保您的團隊了解 IAM Identity Center 中斷時該怎麼做。

主題

- [緊急存取組態摘要](#)
- [如何設計關鍵操作角色](#)
- [如何規劃您的存取模型](#)
- [如何設計緊急角色、帳戶和群組映射](#)
- [如何建立緊急存取組態](#)
- [緊急準備任務](#)
- [緊急容錯移轉程序](#)
- [返回正常操作](#)
- [在 中一次性設定直接 IAM 聯合應用程式 Okta](#)
- [使用 設定一次直接 IAM 聯合應用程式 ADFS](#)

緊急存取組態摘要

若要設定緊急存取，您必須完成下列任務：

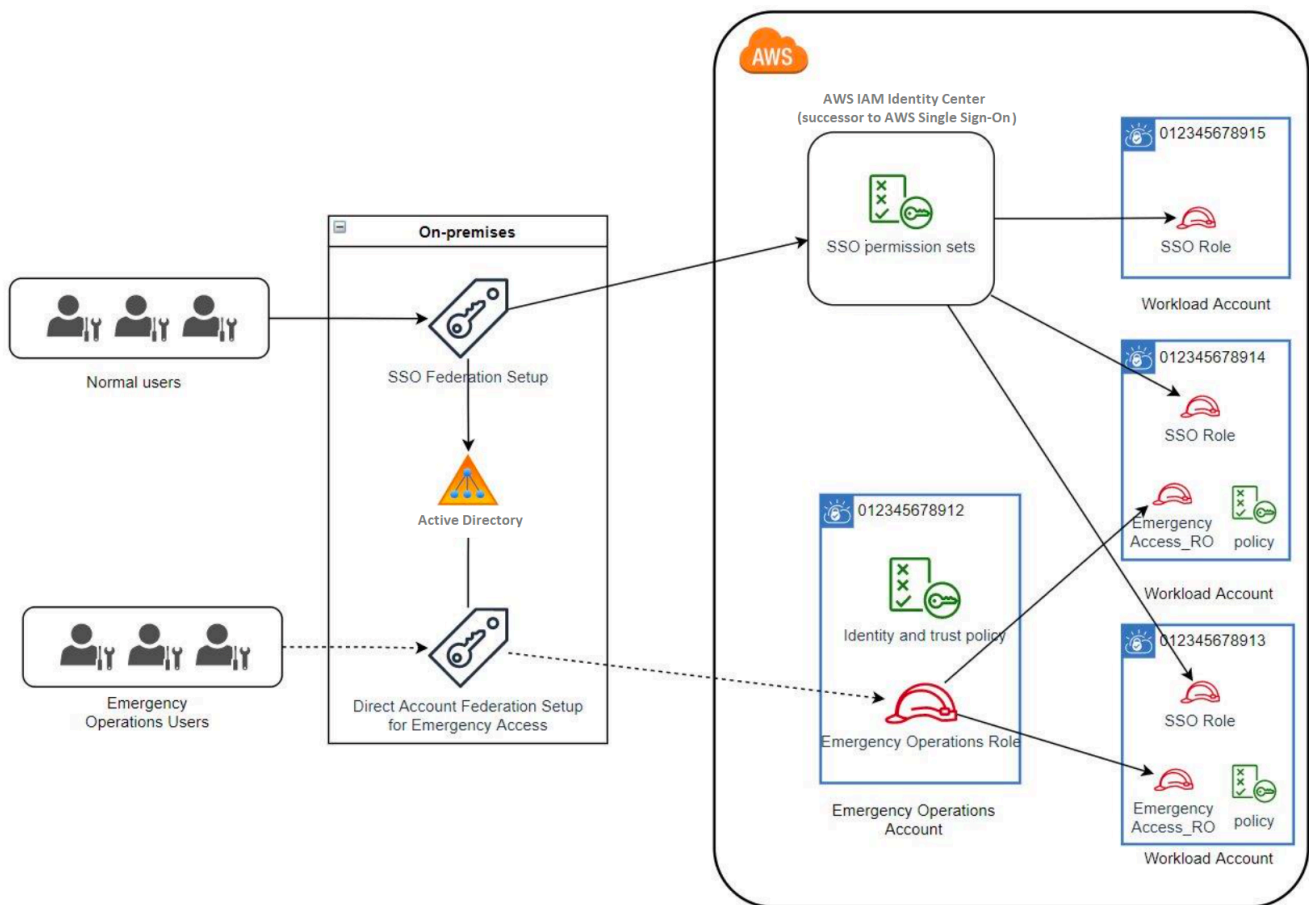
1. [在 中在您的組織中建立緊急操作帳戶 AWS Organizations](#)。此帳戶將成為您的緊急操作帳戶。
2. 使用以 [SAML 2.0 為基礎的聯合](#)，將您的 IdP 連接到緊急操作帳戶。
3. 在緊急操作帳戶中，[為第三方身分提供者聯合建立角色](#)。此外，在每個工作負載帳戶中建立具有所需許可的緊急操作角色。
4. [針對您在緊急操作帳戶中建立的 IAM 角色，委派對工作負載帳戶的存取權](#)。若要授權存取您的緊急操作帳戶，請在 IdP 中建立沒有成員的緊急操作群組。
5. 在 IdP 中建立規則以[啟用 SAML 2.0 聯合存取 AWS 管理主控台](#)，讓 IdP 中的緊急操作群組能夠使用緊急操作角色。

在正常操作期間，沒有人可以存取緊急操作帳戶，因為 IdP 中的緊急操作群組沒有成員。如果發生 IAM Identity Center 中斷，請使用 IdP 將信任的使用者新增至 IdP 中的緊急操作群組。這些使用者可以登入 IdP、導覽至 AWS 管理主控台，並在緊急操作帳戶中擔任緊急操作角色。從那裡，這些使用者可以將[角色切換](#)到工作負載帳戶中需要執行操作工作的緊急存取角色。

如何設計關鍵操作角色

透過此設計，您可以設定透過 IAM 聯合 AWS 帳戶 的單一，讓使用者可以擔任關鍵操作角色。關鍵操作角色具有信任政策，可讓使用者在您的工作負載帳戶中擔任對應的角色。工作負載帳戶中的角色提供使用者執行基本工作所需的許可。

下圖提供設計概觀。



如何規劃您的存取模型

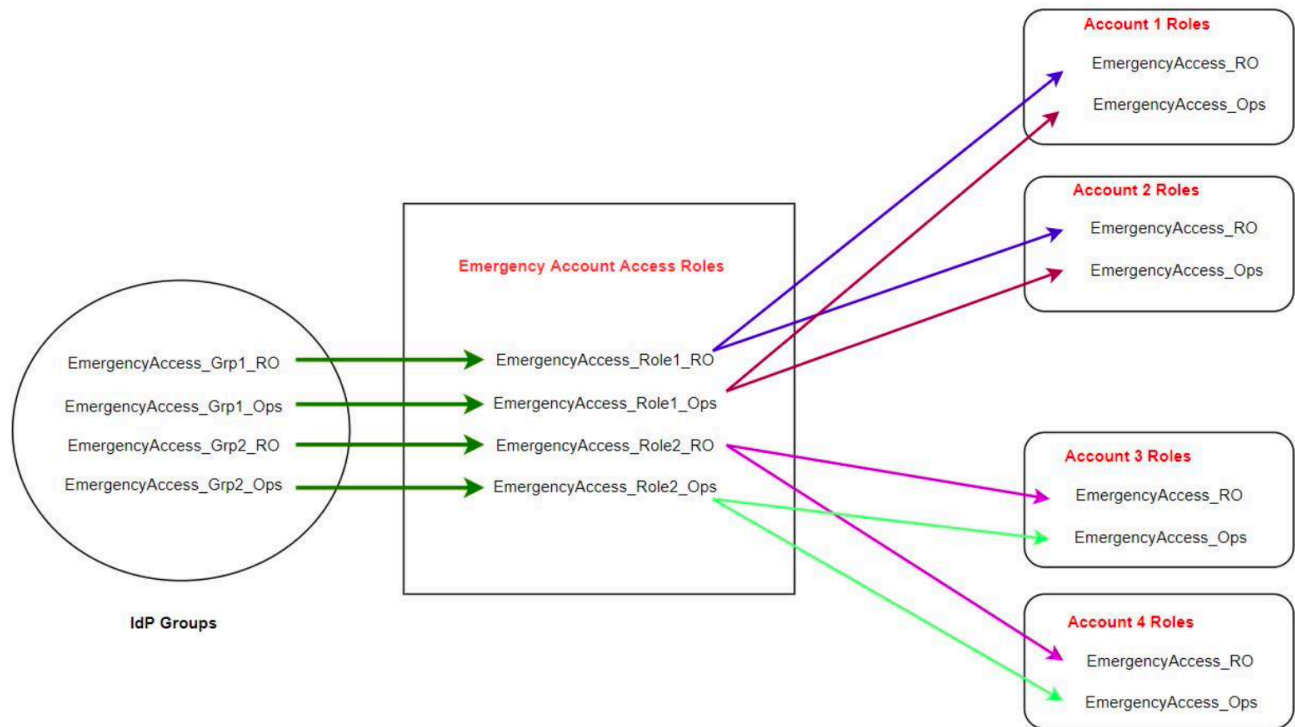
設定緊急存取之前，請建立存取模型運作方式的計劃。請使用下列程序來建立此計劃。

1. 識別在中斷 IAM Identity Center 期間，緊急操作員存取至關重要 AWS 帳戶的。例如，您的生產帳戶可能是必要的，但您的開發和測試帳戶可能不是。
2. 對於該帳戶集合，識別您在帳戶中需要的特定關鍵角色。在這些帳戶中，定義角色可以執行的操作時保持一致。這可簡化您在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) 和操作 (Ops)。如果需要，您可以建立更多角色，並將這些角色映射到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。群組成員是您委派存取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。若要這樣做，請在 IdP 中定義產生宣告的規則，列出群組可存取的角色。這些群組接著可以在緊急存取帳戶中擔任您的唯讀或操作角色。從這些角色中，他們可以在您的工作負載帳戶中擔任對應的角色。

如何設計緊急角色、帳戶和群組映射

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。此圖表也顯示跨帳戶角色信任關係，可讓緊急存取帳戶角色存取工作負載帳戶中的對應角色。我們建議您的緊急計劃設計使用這些映射作為起點。



如何建立緊急存取組態

使用下列映射表來建立您的緊急存取組態。此資料表反映一項計劃，其中包含工作負載帳戶中的兩個角色：唯讀 (RO) 和操作 (Ops)，以及對應的信任政策和許可政策。信任政策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有該角色可在帳戶中執行的許可政策。許可政策可以是 [AWS 受管政策](#) 或 [客戶受管政策](#)。

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 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
帳戶 2	Emergency Access_RO	Emergency Access_Role2_RO	arn : aws : iam : : aws : policy/ReadOnlyAccess
帳戶 2	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	IdP	帳戶中角色資源的 AssumeRole
	Emergency Access_Role1_Ops		
	Emergency Access_Role2_RO		
	Emergency Access_Role2_Ops		

在此映射計劃中，緊急存取帳戶包含兩個唯讀角色和兩個操作角色。這些角色信任您的 IdP 透過在聲明中傳遞角色名稱來驗證和授權所選群組存取角色。工作負載帳戶 1 和帳戶 2 中有對應的唯讀和操作角色。對於工作負載帳戶 1，EmergencyAccess_RO 角色信任位於緊急存取帳戶中 EmergencyAccess_Role1_RO 的角色。資料表指定工作負載帳戶唯讀和操作角色與對應的緊急存取角色之間的類似信任模式。

緊急準備任務

若要準備緊急存取組態，建議您在發生緊急狀況之前執行下列任務。

1. 在 IdP 中設定直接 IAM 聯合應用程式。如果您使用 Okta 或其他外部 IdPs 做為身分來源，請參閱 [在中一次性設定直接 IAM 聯合應用程式 Okta](#)。如果您使用 Active Directory 做為身分來源，請參閱 [使用設定一次直接 IAM 聯合應用程式 ADFS](#)。
2. 在緊急存取帳戶中建立可在事件期間存取的 IdP 連線。
3. 在緊急存取帳戶中建立緊急存取角色，如上表所述。
4. 在每個工作負載帳戶中建立具有信任和許可政策的臨時操作角色。
5. 在 IdP 中建立臨時操作群組。群組名稱將取決於臨時操作角色的名稱。
6. 測試直接 IAM 聯合。
7. 在 IdP 中停用 IdP 聯合應用程式，以防止定期使用。

緊急容錯移轉程序

當 IAM Identity Center 執行個體無法使用，且您判斷您必須提供 AWS 管理主控台的緊急存取權時，建議您執行下列容錯移轉程序。

1. IdP 管理員會在 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請求存取臨時操作群組，例如電子郵件請求、Slack 管道或其他形式的通訊。
3. 您新增至緊急存取群組的使用者會登入 IdP、選取緊急存取帳戶，以及使用者選擇要在緊急存取帳戶中使用的角色。從這些角色中，他們可以在與緊急帳戶角色具有跨帳戶信任的對應工作負載帳戶中擔任角色。

返回正常操作

檢查 [AWS 運作狀態儀表板](#) 以確認 IAM Identity Center 服務的運作狀態何時還原。若要返回正常操作，請執行下列步驟。

1. 在 IAM Identity Center 服務的狀態圖示指出服務狀態良好之後，請登入 IAM Identity Center。
2. 如果您可以成功登入 IAM Identity Center，請通知緊急存取使用者 IAM Identity Center 可供使用。指示這些使用者登出並使用 AWS 存取入口網站重新登入 IAM Identity Center。
3. 在所有緊急存取使用者登出後，請在 IdP 中停用 IdP 聯合應用程式。建議您在工作時間之後執行此任務。
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設施會保留為備份存取計劃，但現在已停用。

在 中一次性設定直接 IAM 聯合應用程式 Okta

1. 以具有管理許可的使用者身分登入Okta您的帳戶。
2. 在Okta管理員主控台的應用程式下，選擇應用程式。
3. 選擇瀏覽應用程式目錄。搜尋並選擇AWS 帳戶聯合。然後選擇新增整合。
4. 遵循如何為帳戶聯合設定 SAML 2.0 中的步驟，AWS 使用 設定直接 IAM 聯合。[AWS](#)為了處理區域故障案例，當您設定登入端點時，建議您為操作的所有區域啟用非區域端點和多個區域端點，以改善聯合彈性。為此緊急存取設定 ACS URL 時，建議您使用與 IAM Identity Center 部署所在區域不同的區域端點。如需區域端點清單，請參閱《[一般參考AWS](#)》中的登入端點。
5. 在登入選項索引標籤上，選取 SAML 2.0，然後輸入群組篩選條件和角色值模式設定。使用者目錄的 群組名稱取決於您設定的篩選條件。

Group Filter	<code>^aws#\S+\#(?[role])[\w\-\+]\#(?[accountid])\d+\$</code>
Role Value Pattern	<code>arn:aws:iam::[accountid]:saml-provider/Okta,arn:aws:iam::[accountid]:role/[role]</code>

在上圖中，role變數適用於緊急存取帳戶中的緊急操作角色。例如，如果您在 中建立EmergencyAccess_Role1_R0角色（如映射表所述）AWS 帳戶123456789012，並且您的群組篩選條件設定如上圖所示，則您的群組名稱應為aws#EmergencyAccess_Role1_R0#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_R0#123456789012）。使用您現有的佈建機制，將您的使用者指派給此群組。
7. 在緊急存取帳戶中，[設定自訂信任政策](#)，提供在中斷期間擔任緊急存取角色所需的許可。以下是連接到EmergencyAccess_Role1_R0角色之自訂信任政策的範例陳述式。如需圖例，請參閱下方圖表中的緊急帳戶[如何設計緊急角色、帳戶和群組映射](#)。將範例 SAML 提供者 ARN 取代為您緊急存取帳戶中建立的正確 ARN。將範例中的區域端點取代為您選擇的區域。

JSON

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

```

    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/[SAML
PROVIDER NAME]"
      },
      "Action": [
        "sts:AssumeRoleWithSAML",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "SAML:aud": [
            "https://signin.aws.amazon.com/saml",
            "https://us-west-2.signin.aws.amazon.com/saml",
            "https://us-west-1.signin.aws.amazon.com/saml",
            "https://us-east-2.signin.aws.amazon.com/saml"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/Okta"
      },
      "Action": "sts:SetSourceIdentity"
    }
  ]
}

```

8. 以下是連接到EmergencyAccess_Role1_R0角色之許可政策的範例陳述式。如需圖例，請參閱下方圖表中的緊急帳戶[如何設計緊急角色、帳戶和群組映射](#)。

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",

```



```

        "Resource": [
            "arn:aws:iam::111122223333:role/EmergencyAccess_R0",
            "arn:aws:iam::444455556666:role/EmergencyAccess_R0"
        ]
    }
}

```

9. 在工作負載帳戶上，設定自訂信任政策。以下是連接到EmergencyAccess_R0角色之信任政策的範例陳述式。在此範例中，帳戶123456789012是緊急存取帳戶。如需圖例，請參閱 [下圖表中的工作負載帳戶如何設計緊急角色、帳戶和群組映射](#)。

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

Note

大多數 IdPs 可讓您將應用程式整合保持停用狀態，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。

使用 設定一次直接 IAM 聯合應用程式 ADFS

本指南說明使用 設定直接 IAM 聯合的一次性設定程序 ADFS，以便在 IAM Identity Center 無法使用 AWS 帳戶 時啟用的緊急存取。

先決條件

如果您打算 ADFS 使用 AWS Managed Microsoft AD 設定，我們建議您先[設定多區域複寫](#)，並在其他區域中繼續進行以下步驟，而不是在主要區域中設定恢復能力。

規劃您的 Active Directory 群組命名慣例

使用特定命名模式建立 AD 群組，以便在群組名稱和 IAM AWS 角色之間自動比對。

群組命名格式：AWS-<AccountNumber>-<RoleName>

如需圖例，請參閱下方圖表中的緊急帳戶[如何設計緊急角色、帳戶和群組映射](#)。將使用者指派給此群組時，會授予他們帳戶中 EmergencyAccess_Role1_R0 角色的存取權 123456789012。如果使用者與多個群組相關聯，他們會看到的可用角色清單 AWS 帳戶，並且可以選擇擔任哪個角色。

AWS 組態

完整的設定包括緊急存取帳戶和工作負載帳戶中的組態。如需整體設定的說明，請參閱[如何設計緊急角色、帳戶和群組映射](#)。

1. [建立 SAML 身分提供者](#)
2. [建立緊急存取角色](#)
3. [設定工作負載帳戶角色](#)

建立 SAML 身分提供者

在緊急存取帳戶中，遵循在 IAM 中建立 SAML 身分提供者中的步驟，[在 IAM 中建立 SAML 身分提供者](#)。從 ADFS 伺服器下載必要的中繼資料：

```
https://<yourADFSserverFQDN>/FederationMetadata/2007-06/  
FederationMetadata.xml
```

建立緊急存取角色

使用 SAML 2.0 Federation 做為信任的實體類型，在[緊急帳戶中建立緊急存取角色](#)。選取您在上一個步驟中建立的 SAML 2.0 提供者。

考量：

- 包含您操作的所有區域 — 選取您擁有作用中工作負載的每個區域，以確保聯合在區域中斷期間保持可用。

- 設定至少一個額外的區域端點，即使您在單一區域中操作 - 例如，如果您僅在 `us-east-1` 中操作 `us-east-1`，請將新增 `us-west-2` 為次要端點。您可以將 IdP 容錯移轉至 `us-west-2` SAML 登入端點，即使沒有 `us-east-1` 的任何工作負載，仍然可以存取您的 `us-east-1` 資源 `us-west-2`。
- 同時啟用非區域端點和區域端點 — 雖然非區域端點 (<https://signin.aws.amazon.com/saml>) 高度可用，但它託管在單一 `us-east-1` 中 AWS 區域，而區域端點 (<https://<region>.signin.aws.amazon.com/saml>) 透過減少對單一全域端點的相依性來改善彈性。

設定信任政策

如需具有多個登入區域端點的範例信任政策，在 [中一次性設定直接 IAM 聯合應用程式 Okta](#)，請參閱。將範例區域端點和 SAML 提供者 ARNs 取代為您。

設定許可政策

如需連接到緊急存取角色，在 [中一次性設定直接 IAM 聯合應用程式 Okta](#) 的許可政策範例，請參閱。

設定工作負載帳戶角色

對於工作負載帳戶角色，請設定自訂信任政策，允許緊急存取帳戶中的緊急存取角色擔任這些角色。如需信任政策，在 [中一次性設定直接 IAM 聯合應用程式 Okta](#) 範例，其中帳戶 `123456789012` 是緊急存取帳戶。

Active Directory 組態

下列步驟說明如何設定 Active Directory 和 ADFS 以進行緊急存取。

1. [建立群組](#)
2. [建立依賴方](#)
3. [建立宣告規則](#)

建立群組

根據先前所述的命名慣例，在 Active Directory 中建立緊急群組（例如 `AWS-123456789012-EmergencyAccess_Role1_R0`）。透過您現有的佈建機制，將使用者指派給這些群組。

建立依賴方

ADFS 聯合需要依賴方組態。依賴方為 AWS Security Token Service (AWS STS)，其會將身分驗證以身分提供者 ADFS 身分外包給。

1. 在 ADFS 管理主控台中，使用動作功能表，然後選取新增依賴方信任。在新增依賴方時，選取宣告感知。
2. 對於聯合中繼資料，輸入來自 IAM 主控台上身分提供者中繼資料資訊的中繼資料 URL。例如：

`https://signin.aws.amazon.com/static/saml/SAMLSPXXXXXX/saml-metadata.xml`
3. 設定依賴方的顯示名稱（例如 AWS 帳戶存取），然後選擇下一步。
4. 選取您要讓存取的人員 AWS。您可以選取特定群組並定義 MFA 等需求。
5. 選擇完成頁面上的關閉以完成新增依賴方信任精靈。現在 AWS 已設定為依賴方。

建立宣告規則

ADFS 使用宣告規則語言，在宣告提供者和依賴方之間發出和轉換宣告。您需要建立四個宣告規則：NameId、RoleSessionName 取得 AD 群組和角色以供 AWS 存取。

在依賴方上按一下滑鼠右鍵，然後選擇編輯宣告發行政策。選擇新增規則以新增規則。

1. NameId.

- a. 選取轉換傳入宣告，然後選擇下一步。
- b. 請使用下列設定：
 - 宣告規則名稱：NameId
 - 傳入宣告類型：Windows Account Name
 - 傳出宣告類型：Name ID
 - 傳出名稱 ID 格式：Persistent Identifier
 - 傳遞所有宣告值：已檢查
- c. 選擇確定。

2. RoleSessionName

- a. 選擇 Add Rule (新增規則)。
- b. 在宣告規則範本清單中，選取傳送 LDAP 屬性做為宣告。
- c. 請使用下列設定：
 - 宣告規則名稱：RoleSessionName

- 屬性存放區：Active Directory
- LDAP 屬性：E-Mail-Addresses
- 傳出宣告類型：<https://aws.amazon.com/SAML/Attributes/RoleSessionName>

d. 選擇確定。

3. 取得 AD 群組

- 選擇 Add Rule (新增規則)。
- 在宣告規則範本清單中，選取使用自訂規則傳送宣告，然後選擇下一步。
- 在宣告規則名稱中輸入 Get AD Groups，然後在自訂規則中輸入以下內容：

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types = ("http://temp/variable"), query =
";tokenGroups;{0}", param = c.Value);
```

此自訂規則使用宣告規則語言中的指令碼，擷取已驗證使用者所屬的所有群組，並將其放入名為的暫時宣告中http://temp/variable。

Note

確保沒有結尾空格，以避免非預期的結果。

4. 角色屬性

- 選擇 Add Rule (新增規則)。
- 在宣告規則範本清單中，選取使用自訂規則傳送宣告，然後選擇下一步。
- 對於宣告規則名稱，輸入 Roles，然後在自訂規則中，輸入以下內容：

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([\d]{12})"]
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
  RegExReplace(c.Value, "AWS-([\d]{12})-", "arn:aws:iam::$1:saml-provider/
<ADFS>,arn:aws:iam::$1:role/"));
```

此自訂規則使用規則表達式，將表單的每個群組成員資格轉換為 AWS 預期的 AWS-<Account Number>-<Role Name> IAM 角色 ARN 和 IAM 聯合提供者 ARN 表單。

 Note

在上述規則語言範例中，ADFS代表在身分提供者設定中提供給 SAML AWS 身分提供者的邏輯名稱。根據您在身分提供者的 IAM 主控台中選擇的邏輯名稱進行變更。

測試組態

透過在 驗證 來測試解決方案是否有效`https://<yourADFSserverFQDN>/adfs/ls/IdpInitiatedSignOn.aspx`。從網站的下拉式清單中選取您建立的依賴方名稱。

在 中更新預設 SAML 聲明端點 ADFS

 Important

在 中設定依賴方信任時ADFS，SAML 聲明端點預設為 `https://signin.aws.amazon.com/`，其不是全域端點且位於 中us-east-1。建議您將預設端點修改為與 IAM Identity Center 設定彈性不同的區域端點。例如，如果您的 IAM Identity Center 部署在 中，us-east-1而且您也在 中操作us-west-2，請將預設 SAML 聲明取用者端點變更為 `https://us-west-2.signin.aws.amazon.com/saml`。

1. 選擇依賴方信任的屬性，然後前往監控索引標籤。清除核取方塊自動更新依賴方。
2. 前往端點索引標籤，選取您偏好的登入端點，然後選擇編輯。
3. 選取核取方塊 將信任的 URL 設定為預設值。選擇確定並套用設定以生效。

 Note

大多數 IdPs可讓您將應用程式整合保持停用狀態，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

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[共同責任模型](#) 將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 Cloud 中執行 AWS 服務的基礎設施。AWS 也為您提供可安全使用的服務。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。若要了解適用的合規計劃 AWS IAM Identity Center，請參閱 [AWS 合規計劃範圍內的服務](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 IAM Identity Center 時套用共同責任模型。下列主題說明如何設定 IAM Identity Center 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 IAM Identity Center 資源。

主題

- [IAM Identity Center 的 Identity and Access Management](#)
- [IAM Identity Center 主控台和 API 授權](#)
- [AWS STS IAM Identity Center 的條件內容索引鍵](#)
- [在 IAM Identity Center 中記錄和監控](#)
- [IAM Identity Center 的合規驗證](#)
- [IAM Identity Center 中的彈性](#)
- [IAM Identity Center 中的基礎設施安全性](#)

IAM Identity Center 的 Identity and Access Management

存取 IAM Identity Center 需要登入資料，AWS 可用來驗證您的請求。這些登入資料必須具有存取 AWS 資源的許可，例如 AWS 受管應用程式。

AWS 存取入口網站的身分驗證是由您已連線至 IAM Identity Center 的目錄所控制。不過，存取 AWS 入口網站內 AWS 帳戶 可供使用者使用的 授權取決於兩個因素：

1. 誰已被指派存取 IAM Identity Center 主控台 AWS 帳戶 中的那些使用者。如需詳細資訊，請參閱[對的單一登入存取 AWS 帳戶](#)。
2. IAM Identity Center 主控台的使用者已獲得何種層級的許可，以允許他們適當存取這些許可 AWS 帳戶。如需詳細資訊，請參閱[建立、管理和刪除許可集](#)。

下列各節說明如何以管理員身分控制對 IAM Identity Center 主控台的存取，或從 IAM Identity Center 主控台委派 day-to-day 任務的管理存取權。

- [身分驗證](#)
- [存取控制](#)

身分驗證

了解如何 AWS 使用 [IAM 身分](#) 存取。

存取控制

您可以擁有有效的登入資料來驗證請求，但除非您具有許可，否則無法建立或存取 IAM Identity Center 資源。例如，您必須擁有建立 IAM Identity Center 連線目錄的許可。

Note

如果您的 IAM Identity Center 執行個體已設定客戶受管 KMS 金鑰，您的 IAM Identity Center 管理員和其他需要存取 KMS 金鑰的執行者將需要額外的許可。請參閱[在中實作客戶受管 KMS 金鑰 AWS IAM Identity Center](#)。

下列各節說明如何管理 IAM Identity Center 的許可。我們建議您先閱讀概觀。

- [管理 IAM Identity Center 資源存取許可的概觀](#)
- [IAM Identity Center 的身分型政策範例](#)
- [IAM Identity Center IAM Identity Center 的資源型政策範例](#)
- [使用 IAM Identity Center 的服務連結角色](#)

管理 IAM Identity Center 資源存取許可的概觀

每個 AWS 資源都由 擁有 AWS 帳戶，而建立或存取資源的許可是由許可政策管理。若要提供存取權，帳戶管理員可以將許可新增至 IAM 身分（即使用者、群組和角色）。有些服務（例如 AWS Lambda）也支援將許可新增至資源。

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 Identity Center 資源和操作](#)
- [了解資源所有權](#)
- [管理 資源的存取](#)
- [指定政策元素：動作、效果、資源和委託人](#)
- [在政策中指定條件](#)

IAM Identity Center 資源和操作

在 IAM Identity Center 中，主要資源是應用程式執行個體、設定檔和許可集。

了解資源所有權

資源擁有者是建立資源 AWS 帳戶 的。也就是說，資源擁有者是驗證建立資源之請求 AWS 帳戶 的委託人實體（帳戶、使用者或 IAM 角色）的。下列範例說明其如何運作：

- 如果 AWS 帳戶根使用者 建立 IAM Identity Center 資源，例如應用程式執行個體或許可集，則您的 AWS 帳戶 是該資源的擁有者。
- 如果您在 AWS 帳戶中建立使用者，並授予該使用者建立 IAM Identity Center 資源的許可，則使用者可以建立 IAM Identity Center 資源。不過，使用者所屬 AWS 的帳戶擁有資源。
- 如果您在 AWS 帳戶中建立具有建立 IAM Identity Center 資源許可的 IAM 角色，則任何可以擔任該角色的人都可以建立 IAM Identity Center 資源。角色所屬 AWS 帳戶的 擁有 IAM Identity Center 資源。

管理 資源的存取

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 Identity Center 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 Identity Center 僅支援以身分為基礎的政策 (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：

- 將許可政策連接至 中的使用者或群組 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，授予該使用者新增 IAM Identity Center 資源的許可，例如新應用程式。
- 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 Identity Center 資源的相關資訊，例如應用程式執行個體或許可集。請注意，Resource 元素中的萬用字元 (*) 表示允許帳戶擁有的所有 IAM Identity Center 資源執行動作。

JSON

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

```
{
  "Effect": "Allow",
  "Action": "sso:List*",
  "Resource": "*"
}
```

如需搭配 IAM Identity Center 使用身分型政策的詳細資訊，請參閱 [IAM Identity Center 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 Identity Center 不支援以資源為基礎的政策。

指定政策元素：動作、效果、資源和委託人

對於每個 IAM Identity Center 資源 (請參閱 [IAM Identity Center 資源和操作](#))，服務會定義一組 API 操作。若要授予這些 API 操作的許可，IAM Identity Center 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，`sso:DescribePermissionsPolicies` 許可允許使用者執行 IAM Identity Center `DescribePermissionsPolicies` 操作的許可。
- 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。如果您不明確授予存取 (允許) 資源，即隱含拒絕存取。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 Identity Center 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 Identity Center 沒有特定的條件索引鍵。不過，您可以視需要使用 AWS 條件索引鍵。如需 AWS 金鑰的完整清單，請參閱《IAM 使用者指南》中的[可用全域條件金鑰](#)。

IAM Identity Center 的身分型政策範例

本主題提供您可以建立的 IAM 政策範例，以授予使用者和角色管理 IAM Identity Center 的許可。

Important

建議您先檢閱簡介主題，這些主題說明可用於管理 IAM Identity Center 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 Identity Center 資源存取許可的概觀](#)。

本主題中的各節涵蓋下列內容：

- [自訂政策範例](#)
- [使用 IAM Identity Center 主控台所需的許可](#)

自訂政策範例

本節提供需要自訂 IAM 政策的常見使用案例範例。這些範例政策是身分型政策，不會指定主體元素。這是因為使用身分型政策時，您不會指定取得許可的委託人。反之，您可以將政策連接至委託人。當您將身分型許可政策連接至 IAM 角色時，角色信任政策中識別的委託人會取得許可。您可以在 IAM 中建立身分型政策，並將其連接到使用者、群組和/或角色。您也可以 IAM Identity Center 中建立許可集時，將這些政策套用至 IAM Identity Center 使用者。

Note

當您為環境建立政策時，請使用這些範例，並確保在生產環境中部署這些政策之前，先測試正面（「授予存取」）和負面（「拒絕存取」）測試案例。如需測試 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 Identity Center](#)
- [範例 2：允許使用者在 IAM Identity Center AWS 帳戶 中管理對 的許可](#)
- [範例 3：允許使用者在 IAM Identity Center 中管理應用程式](#)
- [範例 4：允許使用者管理 Identity Center 目錄中的使用者和群組](#)

範例 1：允許使用者檢視 IAM Identity Center

下列許可政策會將唯讀許可授予使用者，讓他們可以檢視 IAM Identity Center 中設定的所有設定和目錄資訊。

Note

此政策僅供參考。在生產環境中，我們建議您使用 IAM Identity Center 的 ViewOnlyAccess AWS 受管政策。

JSON

```
{
  "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:ListDelegatedAdministrators",
        "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：允許使用者在 IAM Identity Center AWS 帳戶 中管理對 的許可

下列許可政策會授予許可，以允許使用者為您的 建立、管理和部署許可集 AWS 帳戶。

JSON

```

{
  "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

列出的其他許可 "Sid": "IAMListPermissions"、和 "Sid": "AccessToSSOProvisionedRoles" 區段只需要讓使用者在 AWS Organizations 管理帳戶中建立指派。在某些情況下，您可能還需要將 `iam:UpdateSAMLProvider` 新增至這些區段。

範例 3：允許使用者在 IAM Identity Center 中管理應用程式

下列許可政策授予許可，允許使用者在 IAM Identity Center 中檢視和設定應用程式，包括來自 IAM Identity Center 目錄中的預先整合 SaaS 應用程式。

Note

管理應用程式的使用者和群組指派需要下列政策範例中使用的 `sso:AssociateProfile` 操作。它還允許使用者 AWS 帳戶 使用現有的許可集將使用者和群組指派給。如果使用者必須在 IAM Identity Center 中管理 AWS 帳戶 存取權，且需要管理許可集所需的許可，請參閱 [範例 2：允許使用者在 IAM Identity Center AWS 帳戶 中管理對 的許可](#)。

自 2020 年 10 月起，許多這些操作只能透過 AWS 主控台使用。此範例政策包含「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操作相關。

JSON

```
{
  "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 Identity Center 目錄中的使用者和群組

下列許可政策授予許可，允許使用者在 IAM Identity Center 中建立、檢視、修改和刪除使用者和群組。

在某些情況下，對 IAM Identity Center 中的使用者和群組的直接修改會受到限制。例如，當 Active Directory 或啟用自動佈建的外部身分提供者被選取為身分來源時。

JSON

```

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

```

```

        "sso-directory:ListGroupForUser",
        "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 Identity Center 主控台所需的許可

若要讓使用者在沒有錯誤的情況下使用 IAM Identity Center 主控台，則需要額外的許可。如果已建立比最低必要許可更嚴格的 IAM 政策，主控台將無法對具有該政策的使用者如預期般運作。下列範例列出在 IAM Identity Center 主控台中確保無錯誤操作可能需要的一組許可。

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribeAccountAssignmentDeletionStatus",
        "sso:DescribePermissionSet",

```

```

        "sso:DescribePermissionSetProvisioningStatus",
        "sso:DescribeRegisteredRegions",
        "sso:GetApplicationInstance",
        "sso:GetApplicationTemplate",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetMfaDeviceManagementForDirectory",
        "sso:GetPermissionSet",
        "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": "*"
}
]
}

```

IAM Identity Center IAM Identity Center 的資源型政策範例

使用 IAM Identity Center 並使用 [OAuth 2.0 的每個應用程式](#) 都需要資源型政策。應用程式可以是客戶受管或受 AWS 管。必要的資源型政策稱為應用程式政策（或 APIs 中的 [ActorPolicy](#)），定義哪些 [IAM 主體](#) 有權呼叫 IAM 身分驗證方法 API 動作，例如 [CreateTokenWithIAM](#)。IAM 身分驗證方法允許 IAM 主體，例如 IAM 角色或服務 AWS，透過向 IAM Identity Center OIDC 服務提供 IAM 憑證來請求或管理 /token 的存取權杖？aws_iam=t 端點。

應用程式政策會管理發出權杖的操作 (CreateTokenWithIAM)。此政策也會控管僅限 AWS 受管應用程式用於驗證權杖 (IntrospectTokenWithIAM) 和撤銷權杖 () 的僅限許可動作 RevokeTokenWithIAM。對於客戶受管應用程式，您可以透過指定有權呼叫的 IAM 主體來設定此政策 CreateTokenWithIAM。當授權委託人呼叫此 API 動作時，委託人會收到應用程式的存取和重新整理權杖。

如果您使用 IAM Identity Center 主控台來設定受[信任身分傳播](#)的客戶受管應用程式，請參閱[設定客戶受管 OAuth 2.0 應用程式](#)中的步驟 4，以取得如何設定應用程式政策的資訊。如需範例政策，請參閱本主題[範例政策：允許 IAM 角色建立存取和重新整理權杖](#)稍後的。

政策要求

政策必須符合下列要求：

- 政策必須包含設定為 "2012-10-17" 的 Version 元素。
- 政策必須至少包含一個 Statement 元素。
- 每個政策 Statement 必須包含下列元素：Effect、Action、Principal 和 Resource。

政策元素

政策必須包含下列元素：

版本

指定政策文件版本。將版本設定為 2012-10-17 (最新版本)。

陳述式

包含政策 Statements。政策必須至少包含一個 Statement。

每個政策 Statement 都包含下列元素。

Effect

(必要) 決定是允許還是拒絕政策陳述式中的許可。有效值為 Allow 或 Deny。

Principal

(必要) [主體](#)是取得政策陳述式中指定許可的身分。您可以指定 IAM 角色 AWS 或服務主體。

Action

(必要) 要允許或拒絕的 IAM Identity Center OIDC 服務 API 操作。有效的動作包括：

- `sso-oauth:CreateTokenWithIAM`：此動作對應於 [CreateTokenWithIAM](#) API 操作，授予許可，為使用任何 IAM 實體驗證的授權用戶端應用程式建立和傳回存取和重新整理權杖，例如 AWS 服務角色或使用者。這些字符可能包含指定許可的已定義範圍，例如 `read:profile`或 `write:data`。
- `sso-oauth:IntrospectTokenWithIAM` 【僅限許可】：授予許可，以驗證和擷取作用中 OAuth 2.0 存取權杖和重新整理權杖的相關資訊，包括其相關聯的範圍和許可。此許可僅供 AWS 受管應用程式使用，不會記錄在 IAM Identity Center OIDC API 參考中。
- `RevokeTokenWithIAM` 【僅限許可】：授予撤銷 OAuth 2.0 存取權杖和重新整理權杖的許可，使其在正常過期之前失效。此許可僅供 AWS 受管應用程式使用，不會記錄在 IAM Identity Center OIDC API 參考中。

資源

(必要) 在此政策中，`Resource`元素的值為 `"*"`，這表示「此應用程式」。

如需 AWS 政策語法的詳細資訊，請參閱 [《AWS IAM 使用者指南》中的 IAM 政策參考](#)。

範例政策：允許 IAM 角色建立存取和重新整理權杖

下列許可政策會將許可授予工作負載擔任的 `ExampleAppClientRoleIAM` 角色，以建立和傳回存取權和重新整理權杖。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRoleToCreateTokens",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleAppClientRole"
      }
    }
  ]
}
```



```
    },  
    "Action": "sso-oauth:CreateTokenWithIAM",  
    "Resource": "*"    
  }  
]  
}
```

AWS IAM Identity Center 的 受管政策

[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 受管政策。您無法變更 AWS 受管政策中的許可。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 受管政策移除許可，因此政策更新不會破壞您現有的許可。

此外，AWS 支援跨多個 服務之任務函數的受管政策。例如，ReadOnlyAccess AWS 受管政策提供所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時，會為新操作和資源 AWS 新增唯讀許可。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。此頁面將更新此命名空間中動作的任何其他許可。建立自訂 IAM 政策時，請避免在 *之後使用，identitystore-auth因為這適用於目前或未來存在於 命名空間中的所有動作。

AWS 受管政策：AWSSSOMasterAccountAdministrator

此AWSSSOMasterAccountAdministrator政策為委託人提供必要的管理動作。此政策適用於執行 AWS IAM Identity Center 管理員任務角色的主體。隨著時間的推移，所提供的動作清單將會更新，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。當您將AWSSSOMasterAccountAdministrator政策連接到身分時，您會授予管理 AWS IAM Identity Center 許可。使用此政策的委託人可以存取 AWS Organizations 管理帳戶和所有成員帳戶中的 IAM Identity Center。此主體可以完整管理所有 IAM Identity Center 操作，包括建立 IAM Identity Center 執行個體、使用者、許可集和指派的能力。委託人也可以在整個 AWS 組織成員帳戶中執行個體化這些指派，並在 AWS Directory Service 受管目錄和 IAM Identity Center 之間建立連線。隨著新的管理功能發佈，帳戶管理員將自動獲得這些許可。

此政策也包含使用客戶受管金鑰進行加密的 IAM Identity Center 執行個體所需的 AWS Key Management Service 許可。

許可分組

此政策會根據提供的許可集分組到陳述式中。

- `AWSSSOMasterAccountAdministrator` – 允許 IAM Identity Center [將名為的服務角色傳遞](#) `AWSServiceRoleforSSO` 至 IAM Identity Center，以便之後可以擔任該角色並代表他們執行動作。當人員或應用程式嘗試啟用 IAM Identity Center 時，這是必要的。如需詳細資訊，請參閱[設定的存取權 AWS 帳戶](#)。
- `AWSSSOMemberAccountAdministrator` – 允許 IAM Identity Center 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 受管政策：AWSSSOMemberAccountAdministrator](#)。
- `AWSSSOManageDelegatedAdministrator` – 允許 IAM Identity Center 為您的組織註冊和取消註冊委派管理員。
- `AllowKMSKeyUseViaService` 和 `AllowKMSKeyDiscovery` – 允許 IAM Identity Center 執行個體使用的客戶受管金鑰 AWS Key Management Service 操作。

若要檢視此政策的許可，請參閱《AWS 受管政策參考》中的 [AWSSSOMasterAccountAdministrator](#)。

此政策的其他資訊

第一次啟用 IAM Identity Center 時，IAM Identity Center 服務會在 AWS Organizations 管理帳戶（先前的主要帳戶）中建立[服務連結角色](#)，以便 IAM Identity Center 可以管理帳戶中的資源。所需的動作為 `iam:CreateServiceLinkedRole` 和 `iam:PassRole`。

AWS 受管政策：AWSSSOMemberAccountAdministrator

此 `AWSSSOMemberAccountAdministrator` 政策為委託人提供必要的管理動作。此政策適用於執行 IAM Identity Center 管理員任務角色的主體。隨著時間的推移，所提供的動作清單將會更新，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。當您將 `AWSSSOMemberAccountAdministrator` 政策連接到身分時，您會授予管理 AWS IAM Identity Center 許可。使用此政策的委託人可以存取 AWS Organizations 管理帳戶和所有成員帳戶中的 IAM Identity Center。此主體可以完整管理所有 IAM Identity Center 操作，包括建立使用者、許可集和指

派的能力。委託人也可以在整個 AWS 組織成員帳戶中執行個體化這些指派，並在 AWS Directory Service 受管目錄和 IAM Identity Center 之間建立連線。隨著新的管理功能發佈，帳戶管理員會自動獲得這些許可。

此政策也包含使用客戶受管金鑰進行加密的 IAM Identity Center 執行個體所需的 AWS Key Management Service 許可。

若要檢視此政策的許可，請參閱《AWS 受管政策參考》中的 [AWSSSOMemberAccountAdministrator](#)。

此政策的其他資訊

IAM Identity Center 管理員在其 Identity Center 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許可：

- "sso:*"
- "sso-directory:*"

IAM Identity Center 管理員需要下列 Directory Service 動作的有限許可，才能執行每日任務。

- "ds:DescribeTrusts"
- "ds:UnauthorizeApplication"
- "ds:DescribeDirectories"
- "ds:AuthorizeApplication"
- "ds:CreateAlias"

這些許可允許 IAM Identity Center 管理員識別現有目錄和管理應用程式，以便將其設定為與 IAM Identity Center 搭配使用。如需這些動作的詳細資訊，請參閱 [Directory Service API 許可：動作、資源和條件參考](#)。

IAM Identity Center 使用 IAM 政策將許可授予 IAM Identity Center 使用者。IAM Identity Center 管理員會建立許可集，並將政策連接到這些許可集。IAM Identity Center 管理員必須具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之許可集使用的政策。若要設定安全和功能許可，IAM Identity Center 管理員必須具有執行 IAM Access Analyzer 政策驗證的許可。

- "iam:ListPolicies"
- "access-analyzer:ValidatePolicy"

IAM Identity Center 管理員需要對下列 AWS Organizations 動作的有限存取權，才能執行每日任務：

- "organizations:EnableAWSServiceAccess"
- "organizations:ListRoots"
- "organizations:ListAccounts"
- "organizations:ListOrganizationalUnitsForParent"
- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"
- "organizations:ListDelegatedAdministrators"
- "organizations:RegisterDelegatedAdministrator"
- "organizations:DeregisterDelegatedAdministrator"

這些許可可讓 IAM Identity Center 管理員針對基本 IAM Identity Center 管理任務使用組織資源（帳戶），如下所示：

- 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 AWS 的服務存取
- 設定和管理委派管理員

如需搭配 IAM Identity Center 使用委派管理員的詳細資訊，請參閱 [委派的管理](#)。如需如何使用這些許可的詳細資訊 AWS Organizations，請參閱[搭配使用 AWS Organizations 與其他 AWS 服務](#)。

AWS 受管政策：AWSSSODirectoryAdministrator

您可將 AWSSSODirectoryAdministrator 政策連接到 IAM 身分。

此政策會授予 IAM Identity Center 使用者和群組的管理許可。附加此政策的主體可以對 IAM Identity Center 使用者和群組進行任何更新。此政策也包含使用客戶受管金鑰進行加密的 IAM Identity Center 執行個體所需的 AWS Key Management Service 許可。

此政策包含以下許可：

- IAM Identity Center Directory - IAM Identity Center 目錄操作的完整管理存取權。
- Identity Store - 身分存放區操作和身分驗證的完整管理存取權。
- IAM Identity Center - 列出目錄關聯的許可。
- AWS Key Management Service - 解密、描述金鑰，以及為 IAM Identity Center 執行個體使用的客戶受管金鑰產生資料金鑰的許可。

若要檢視此政策的許可，請參閱 AWS 受管政策參考中的 [AWSSSODirectoryAdministrator](#)。

AWS 受管政策：AWSSSOReadOnly

您可將 AWSSSOReadOnly 政策連接到 IAM 身分。

此政策授予唯讀許可，允許使用者檢視 IAM Identity Center 中的資訊。連接此政策的主體無法直接檢視 IAM Identity Center 使用者或群組。附加此政策的主體無法在 IAM Identity Center 中進行任何更新。例如，具有這些許可的主體可以檢視 IAM Identity Center 設定，但無法變更任何設定值。

此政策也包含使用客戶受管金鑰進行加密的 IAM Identity Center 執行個體所需的 AWS Key Management Service 許可。

若要檢視此政策的許可，請參閱《AWS 受管政策參考》中的 [AWSSSOReadOnly](#)。

AWS 受管政策：AWSSSODirectoryReadOnly

您可將 AWSSSODirectoryReadOnly 政策連接到 IAM 身分。

此政策授予唯讀許可，允許使用者檢視 IAM Identity Center 中的使用者和群組。連接此政策的主體無法檢視 IAM Identity Center 指派、許可集、應用程式或設定。附加此政策的主體無法在 IAM Identity Center 中進行任何更新。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。

此政策也包含使用客戶受管金鑰進行加密的 IAM Identity Center 執行個體所需的 AWS Key Management Service 許可。

若要檢視此政策的許可，請參閱《AWS 受管政策參考》中的 [AWSSSODirectoryReadOnly](#)。

AWS 受管政策：AWSIdentitySyncFullAccess

您可將 AWSIdentitySyncFullAccess 政策連接到 IAM 身分。

連接此政策的主體具有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、列出和刪除同步篩選條件，以及開始或停止同步的完整存取許可。

許可詳細資訊

若要檢視此政策的許可，請參閱《AWS 受管政策參考》中的 [AWSIdentitySyncFullAccess](#)。

AWS 受管政策：AWSIdentitySyncReadOnlyAccess

您可將 AWSIdentitySyncReadOnlyAccess 政策連接到 IAM 身分。

此政策授予唯讀許可，允許使用者檢視身分同步設定檔、篩選條件和目標設定的相關資訊。連接此政策的主體無法對同步設定進行任何更新。例如，具有這些許可的主體可以檢視身分同步設定，但無法變更任何設定檔或篩選條件值。

若要檢視此政策的許可，請參閱《AWS 受管政策參考》中的 [AWSIdentitySyncReadOnlyAccess](#)。

AWS 受管政策：AWSSSOServiceRolePolicy

您無法將 AWSSSOServiceRolePolicy 政策連接至 IAM 身分。

此政策連接到服務連結角色，允許 IAM Identity Center 委派和強制執行哪些使用者具有特定 AWS 帳戶中的單一登入存取權 AWS Organizations。當您啟用 IAM 時，會在組織 AWS 帳戶中的所有中建立服務連結角色。IAM Identity Center 也會在每個帳戶中建立相同的服務連結角色，該角色隨後會新增至您的組織。此角色允許 IAM Identity Center 代表您存取每個帳戶的資源。在每個中建立的服務連結角色命名 AWS 帳戶為 AWSServiceRoleForSSO。如需詳細資訊，請參閱[使用 IAM Identity Center 的服務連結角色](#)。

AWS 受管政策：AWSIAMIdentityCenterAllowListForIdentityContext

使用 IAM Identity Center 身分內容擔任角色時，AWS Security Token Service (AWS STS) 會自動將 AWSIAMIdentityCenterAllowListForIdentityContext 政策連接至角色。

此政策提供當您搭配 IAM Identity Center 身分內容擔任的角色使用受信任身分傳播時允許的動作清單。使用此內容呼叫的所有其他動作都會遭到封鎖。身分內容會傳遞為 ProvidedContext。

若要檢視此政策的許可，請參閱 AWS 受管政策參考中的 [AWSIAMIdentityCenterAllowListForIdentityContext](#)。

AWS 受管政策：AWSIdentityCenterExternalManagementPolicy

您可將 AWSIdentityCenterExternalManagementPolicy 政策連接到 IAM 身分。

此政策提供從外部供應商管理 IAM Identity Center 使用者的存取權。

若要檢視此政策的許可，請參閱 AWS 受管政策參考中的 [AWSIdentityCenterExternalManagementPolicy](#)。

AWS 受管政策的 IAM Identity Center 更新

下表說明自此服務開始追蹤這些變更以來，IAM Identity Center AWS 受管政策的更新。如需此頁面變更的自動提醒，請訂閱 IAM Identity Center 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	Date
AWSIdentityCenterExternalManagementPolicy	更新 受管政策，以變更佈建租用用戶的 ARN。	2025 年 12 月 5 日
AWSIdentityCenterExternalManagementPolicy	此政策提供從外部供應商管理 IAM Identity Center 使用者的存取權。	2025 年 11 月 21 日
AWSSSOMasterAccountAdministrator 、 AWSSSOMemberAccountAdministrator 、 AWSSSOReadOnly 、 AWSSSODirectoryAdministrator 、 AWSSSODirectoryReadOnly	已更新 受管政策，以包含使用客戶受管金鑰進行加密的 IAM Identity Center 執行個體所需的 AWS KMS 許可。	2025 年 9 月 17 日
AWSSSOServiceRolePolicy	此政策現在包含呼叫 的許可 <code>identity-sync:DeleteSyncProfile</code> 。	2025 年 2 月 11 日
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包含 <code>qapps:ListQAppSessionData</code> 和 <code>qapps:ExportQAppSessionData</code> 動作，以支援支援這些工作階段之 AWS 受管應用程式的身分增強主控台工作階段。	2024 年 10 月 2 日

變更	描述	Date
AWSSSOMasterAccountAdministrator	IAM Identity Center 新增了新的動作，以授予 DeleteSyncProfile 許可，允許您使用此政策刪除同步設定檔。這是與 DeleteInstance API 相關聯的動作。	2024 年 9 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包含支援支援支援這些工作階段之 AWS 受管應用程式的身分增強主控台工作階段s3:ListCallerAccessGrants 的動作。	2024 年 9 月 4 日
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包含 aoss:APIAccessAll 、 es:ESHttpHead 、 es:ESHttpPost 、 es:ESHttpDelete 、 和 es:ESHttpGet es:ESHttpPatch es:ESHttpPut 動作，以支援支援這些工作階段之 AWS 受管應用程式的身分增強主控台工作階段。	2024 年 7 月 12 日

變更	描述	Date
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包含 <code>qapps:PredictQApp</code> 、 <code>qapps:ImportDocume</code> <code>nt</code> 、 <code>qapps:AssociateLibraryItemR</code> <code>evuew</code> 、 <code>qapps:Dis</code> <code>associateLibraryIt</code> <code>emReview</code> 、 <code>qapps:Get</code> <code>QAppSessi</code> <code>on</code> 、 <code>qapps:Upd</code> <code>ateQAppSessionMeta</code> <code>data</code> 、 <code>qapps:Upd</code> <code>ateQAppSession</code> <code>qapps:GetQAppSessi</code> <code>onMetadata</code> 和 <code>qapps:TagResource</code> 動作，以支援支援這些工作階段之 AWS 受管應用程式的身分增強主控台工作階段。	2024 年 6 月 27 日
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包含 <code>elasticmapreduce:AddJobFlow</code> <code>Steps</code> 、 <code>elasticma</code> <code>preduce:DescribeCl</code> <code>uster</code> 、 <code>elasticma</code> <code>preduce:DescribeSt</code> <code>ep</code> 、 <code>elasticma</code> <code>preduce:CancelStep</code> <code>s</code> 和 <code>elasticma</code> <code>preduce:ListSteps</code> 動作，以支援 Amazon EMR 中的受信任身分傳播。	2024 年 5 月 17 日

變更	描述	Date
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包含 qapps:CreateQApp 、 qapps:PredictProblemStatementFromConversation 、 qapps:PredictQAppFromProblemStatement 、 qapps:CopyQApp 、 qapps:GetQApp qapps:ListQApps 、 qapps:UpdateQApp qapps:DeleteQApp 、 qapps:AssociateQAppWithUser 、 、 qapps:DisassociateQAppFromUser 、 qapps:ImportDocumentToQApp qapps:ImportDocumentToQAppSession 、 qapps:CreateLibraryItem 、 qapps:GetLibraryItem qapps:UpdateLibraryItem 、 、 qapps:CreateLibraryItemReview 、 、 qapps:StartQAppSession 、 、 和 qapps:ListLibraryItems qapps:CreateSubscriptionToken qapps:StopQAppSession 動作，以支援支援這些工	2024 年 4 月 30 日

變更	描述	Date
	作階段之 AWS 受管應用程式的身分增強主控台工作階段。	
AWSSSOMasterAccountAdministrator	此政策現在包含 <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> 和 <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> 動作，以支援支援這些工作階段之 AWS 受管應用程式的身分增強主控台工作階段。	2024 年 4 月 26 日
AWSSSOMemberAccountAdministrator	此政策現在包含 <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> 和 <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> 動作，以支援支援這些工作階段之 AWS 受管應用程式的身分增強主控台工作階段。	2024 年 4 月 26 日
AWSSSORReadOnly	此政策現在包含 <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> 動作，以支援支援這些工作階段之 AWS 受管應用程式的身分增強主控台工作階段。	2024 年 4 月 26 日

變更	描述	Date
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包含支援支援支援這些工作階段之 AWS 受管應用程式的身分增強主控台工作階段qbusiness:PutFeedback 的動作。	2024 年 4 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包含 q:StartConversation 、 q:SendMessage 、 q:ListConversations 、 q:GetConversation 、 q:StartTroubleshootingResolutionExplanation 、 和 q:StartTroubleshootingAnalysis q:GetTroubleshootingResults q:UpdateTroubleshootingCommandResult 動作，以支援支援這些工作階段之 AWS 受管應用程式的身分增強主控台工作階段。	2024 年 4 月 24 日
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包含 sts:SetContext 動作，以支援支援這些工作階段之 AWS 受管應用程式的身分增強主控台工作階段。	2024 年 4 月 19 日

變更	描述	Date
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包含 <code>qbusiness:Chat</code> 、 <code>qbusiness:ChatSync</code> 、 <code>qbusiness:ListMessages</code> 、 <code>qbusiness:ListConversations</code> 和 <code>qbusiness:DeleteConversation</code> 動作，以支援支援這些工作階段之 AWS 受管應用程式的身分增強主控台工作階段。	2024 年 4 月 11 日
AWSIAMIdentityCenterAllowListForIdentityContext	此政策現在包含 <code>s3:GetAccessGrantsInstanceForPrefix</code> 和 <code>s3:GetDataAccess</code> 動作。	2023 年 11 月 26 日
AWSIAMIdentityCenterAllowListForIdentityContext	此政策提供當您搭配 IAM Identity Center 身分內容擔任的角色使用受信任身分傳播時允許的動作清單。	2023 年 11 月 15 日
AWSSSODirectoryReadOnly	此政策現在包含 <code>identitystore-auth</code> 具有新許可的新命名空間，允許使用者列出和取得工作階段。	2023 年 2 月 21 日
AWSSSOServiceRolePolicy	此政策現在允許對管理帳戶採取 UpdateSAMLProvider 動作。	2022 年 10 月 20 日
AWSSSOMasterAccountAdministrator	此政策現在包含 <code>identitystore-auth</code> 具有新許可的新命名空間，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	Date
AWSSSOMemberAccountAdministrator	此政策現在包含identitystore-auth 具有新許可的新命名空間，以允許管理員列出和刪除使用者工作階段。	2022 年 10 月 20 日
AWSSSODirectoryAdministrator	此政策現在包含identitystore-auth 具有新許可的新命名空間，以允許管理員列出和刪除使用者工作階段。	2022 年 10 月 20 日
AWSSSOMasterAccountAdministrator	此政策現在包含可 ListDelegatedAdministrators 呼叫的新許可 AWS Organizations。此政策現在也包含許可的子集AWSSSOManageDelegatedAdministrator，其中包含呼叫 RegisterDelegatedAdministrator 和的許可 DeregisterDelegatedAdministrator 。	2022 年 8 月 16 日
AWSSSOMemberAccountAdministrator	此政策現在包含可 ListDelegatedAdministrators 呼叫的新許可 AWS Organizations。此政策現在也包含許可的子集AWSSSOManageDelegatedAdministrator，其中包含呼叫 RegisterDelegatedAdministrator 和的許可 DeregisterDelegatedAdministrator 。	2022 年 8 月 16 日

變更	描述	Date
AWSSSOReadOnly	此政策現在包含可 ListDelegatedAdministrators 呼叫的新許可 AWS Organizations。	2022 年 8 月 11 日
AWSSSOServiceRolePolicy	此政策現在包含呼叫 DeleteRolePermissionsBoundary 和 的新許可 PutRolePermissionsBoundary 。	2022 年 7 月 14 日
AWSSSOServiceRolePolicy	此政策現在包含允許在 ListAWSServiceAccessForOrganization and ListDelegatedAdministrators 中 呼叫 的新許可 AWS Organizations。	2022 年 5 月 11 日
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	新增允許委託人使用政策檢查進行驗證的 IAM Access Analyzer 許可。	2022 年 4 月 28 日
AWSSSOMasterAccountAdministrator	此政策現在允許所有 IAM Identity Center Identity Store 服務動作。 如需 IAM Identity Center Identity Store 服務中可用動作的相關資訊，請參閱 IAM Identity Center Identity Store API 參考 。	2022 年 3 月 29 日

變更	描述	Date
AWSSSOMemberAccountAdministrator	此政策現在允許所有 IAM Identity Center Identity Store 服務動作。	2022 年 3 月 29 日
AWSSSODirectoryAdministrator	此政策現在允許所有 IAM Identity Center Identity Store 服務動作。	2022 年 3 月 29 日
AWSSSODirectoryReadOnly	此政策現在授予 IAM Identity Center Identity Store 服務讀取動作的存取權。從 IAM Identity Center Identity Store 服務擷取使用者和群組資訊時需要此存取權。	2022 年 3 月 29 日
AWSIdentitySyncFullAccess	此政策允許完整存取 identity-sync 許可。	2022 年 3 月 3 日
AWSIdentitySyncReadOnlyAccess	此政策會授予唯讀許可，允許委託人檢視 Identity-sync 設定。	2022 年 3 月 3 日
AWSSSOReadOnly	此政策授予唯讀許可，允許委託人檢視 IAM Identity Center 組態設定。	2021 年 8 月 4 日
IAM Identity Center 已開始追蹤變更	IAM Identity Center 開始追蹤 AWS 受管政策的變更。	2021 年 8 月 4 日

使用 IAM Identity Center 的服務連結角色

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 Identity Center 的唯一 IAM 角色類型。它由 IAM Identity Center 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有許可。如需詳細資訊，請參閱[了解 IAM Identity Center 中的服務連結角色](#)。

服務連結角色可讓您更輕鬆地設定 IAM Identity Center，因為您不必手動新增必要的許可。IAM Identity Center 定義其服務連結角色的許可，除非另有定義，否則只有 IAM Identity Center 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 Identity Center 的服務連結角色許可

IAM Identity Center 使用名為 AWSServiceRoleForSSO 的服務連結角色，授予 IAM Identity Center 代表您管理 AWS 資源的許可，包括 IAM 角色、政策和 SAML IdP。

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

- IAM Identity Center (服務字首：sso)

AWSSSOServiceRolePolicy 服務連結角色許可政策允許 IAM Identity Center 對路徑 “/aws-reserved/sso.amazonaws.com/” 上的角色完成下列項目，且名稱字首為「AWSReservedSSO_」：

- iam:AttachRolePolicy
- iam:CreateRole
- iam>DeleteRole
- iam>DeleteRolePermissionsBoundary
- iam>DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetRole
- iam:ListRolePolicies
- iam:PutRolePolicy
- iam:PutRolePermissionsBoundary
- iam>ListAttachedRolePolicies

AWSSSOServiceRolePolicy 服務連結角色許可政策允許 IAM Identity Center 在名稱字首為「AWSSSO_」的 SAML 供應商上完成下列項目：

- iam:CreateSAMLProvider

- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam:DeleteSAMLProvider`

AWSSSOServiceRolePolicy 服務連結角色許可政策允許 IAM Identity Center 在所有組織上完成下列操作：

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

AWSSSOServiceRolePolicy 服務連結角色許可政策允許 IAM Identity Center 在所有 IAM 角色上完成下列項目 (*)：

- `iam:listRoles`

AWSSSOServiceRolePolicy 服務連結角色許可政策允許 IAM Identity Center 在「arn : aws : iam : : * : role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO」上完成下列事項：

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

AWSSSOServiceRolePolicy 服務連結角色許可政策允許 IAM Identity Center 在「arn : aws : identity-sync : * : * : profile/*」上完成下列項目：

- `identity-sync:DeleteSyncProfile`

如需 AWSSSOServiceRolePolicy 服務連結角色許可政策更新的詳細資訊，請參閱 [AWS 受管政策的 IAM Identity Center 更新](#)。

JSON

```
{
```

```
"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": [
        "*"
      ]
    },
    {
      "Sid": "AllowDeleteSyncProfile",
      "Effect": "Allow",
      "Action": [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource": [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    }
  ]
}

```

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 Identity Center 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 Identity Center 會在 AWS Organizations 中組織內的所有帳戶中建立服務連結角色。IAM Identity Center 也會在每個帳戶中建立相同的服務連結角色，該角色隨後會新增至您的組織。此角色允許 IAM Identity Center 代表您存取每個帳戶的資源。

備註

- 如果您登入 AWS Organizations 管理帳戶，它會使用您目前登入的角色，而不是服務連結角色。這可防止權限升級。

- 當 IAM Identity Center 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。這可讓 CloudTrail 中的日誌提供誰在管理帳戶中進行所有權限變更的可見性。

Important

如果您在 2017 年 12 月 7 日之前使用 IAM Identity Center 服務，當它開始支援服務連結角色時，IAM Identity Center 會在您的帳戶中建立 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 Identity Center 的服務連結角色

IAM Identity Center 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 Identity Center 的服務連結角色

您不需要手動刪除 AWSServiceRoleForSSO 角色。從 AWS 組織移除 AWS 帳戶時，IAM Identity Center 會自動清除資源，並從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

如果您嘗試刪除資源時，IAM Identity Center 服務正在使用該角色，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。

刪除 AWSServiceRoleForSSO 使用的 IAM Identity Center 資源

- [移除的使用者和群組存取權 AWS 帳戶](#) 適用於所有可存取的使用者和群組 AWS 帳戶。
- [在 IAM Identity Center 中移除許可集](#) 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 來刪除 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 Identity Center 主控台和 API 授權

現有的 IAM Identity Center 主控台 APIs 支援雙重授權，可讓您在有較新的 API 可用時，維持現有 APIs 操作的使用。如果您有在 2023 年 11 月 15 日之前和 2020 年 10 月 15 日之前建立的現有 IAM Identity Center 執行個體，您可以使用下表來判斷哪些 API 操作現在對應到這些日期之後發行的較新 API 操作。

主題

- [2023 年 11 月之後的 API 動作](#)
- [2020 年 10 月之後的 API 動作](#)

2023 年 11 月之後的 API 動作

2023 年 11 月 15 日之前建立的 IAM Identity Center 執行個體會遵守舊的和新的 API 動作，只要任何動作都沒有明確拒絕。2023 年 11 月 15 日之後建立的執行個體會在 IAM Identity Center 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操作名稱	2023 年 11 月 15 日之後使用的 API 動作
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment

2023 年 11 月 15 日之前使用的主控制台操作名稱	2023 年 11 月 15 日之後使用的 API 動作
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

2020 年 10 月 15 日之前建立的 IAM Identity Center 執行個體會遵守舊的 API 動作和新的 API 動作，只要任何動作都沒有明確拒絕。2020 年 10 月 15 日之後建立的執行個體會在 IAM Identity Center 主控台中使用[較新的 API 動作](#)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
DeleteApplicationInstanceForAWSAccount	DeleteApplicationInstance DeleteTrust	DeleteAccountAssignment

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
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
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile CreateProfile UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust CreateTrust UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS IAM Identity Center 的條件內容索引鍵

當委託人向提出請求時 AWS，會將請求資訊 AWS 收集到請求內容中，用於評估和授權請求。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。請求資訊由不同的來源提供，包括提出請求的委託人、資源、提出請求的請求，以及請求本身的中繼資料。服務特定條件金鑰已定義用於個別 AWS 服務。

IAM Identity Center 包含 AWS STS 內容提供者，可讓 AWS 受管應用程式和第三方應用程式為 IAM Identity Center 定義的條件金鑰新增值。這些金鑰包含在 [IAM 角色](#) 中。當應用程式傳遞字符至時，會設定金鑰值 AWS STS。應用程式 AWS STS 會以下列其中一種方式取得傳遞給的字符：

- 使用 IAM Identity Center 進行身分驗證期間。
- 與[受信任權杖發行者交換權杖](#)之後，以進行受信任身分傳播。在此情況下，應用程式會從信任的權杖發行者取得權杖，並將該權杖交換為 IAM Identity Center 的權杖。

這些金鑰通常由與受信任身分傳播整合的應用程式使用。在某些情況下，當索引鍵值存在時，您可以在您建立的 IAM 政策中使用這些索引鍵來允許或拒絕許可。

例如，您可能想要根據的值提供資源的條件式存取UserId。此值指出哪個 IAM Identity Center 使用者正在使用角色。此範例類似於使用 SourceId。不過SourceId，與不同，的值UserId 代表身分存

放區中經過驗證的特定使用者。此值存在於應用程式取得並傳遞至其中的字符中 AWS STS。它不是可包含任意值的一般用途字串。

主題

- [identitystore:UserId](#)
- [identitystore : IdentityStoreArn](#)
- [identitycenter : ApplicationArn](#)
- [identitycenter : CredentialId](#)
- [identitycenter : InstanceArn](#)

identitystore:UserId

此內容索引鍵是 IAM Identity Center 使用者的 `UserId`，其為 IAM Identity Center 所發出內容聲明的主體。內容聲明會傳遞至 AWS STS。您可以使用此金鑰，將代表提出請求 `UserId` 的 IAM Identity Center 使用者的 與您在政策中指定之使用者的識別符進行比較。

- 可用性 – 設定 IAM Identity Center 發出的內容聲明後，當角色在 AWS CLI 或 AWS STS `AssumeRole` API 操作中使用任意 AWS STS `assume-role` 命令時，此金鑰會包含在請求內容中。
- 資料類型 – [字串](#)
- 值類型 - 單一值

identitystore : IdentityStoreArn

此內容索引鍵是連接到發出內容聲明之 IAM Identity Center 執行個體的身分存放區的 ARN。它也是身分存放區，您可以在其中查詢的屬性 `identitystore:UserID`。您可以在政策中使用此金鑰來判斷是否 `identitystore:UserID` 來自預期的身分存放區 ARN。

- 可用性 – 設定 IAM Identity Center 發出的內容聲明後，當角色在 AWS CLI 或 AWS STS `AssumeRole` API 操作中使用任意 AWS STS `assume-role` 命令時，此金鑰會包含在請求內容中。
- 資料類型 – [Arn](#)、[字串](#)
- 值類型 - 單一值

identitycenter : ApplicationArn

此內容索引鍵是 IAM Identity Center 向其發出內容聲明之應用程式的 ARN。您可以在政策中使用此金鑰來判斷 是否identitycenter:ApplicationArn來自預期的應用程式。使用此金鑰有助於防止意外應用程式存取 IAM 角色。

- 可用性 – 此金鑰包含在 API AWS STS AssumeRole操作的請求內容中。請求內容包含 IAM Identity Center 發出的內容聲明。
- 資料類型 – [Arn](#)、[字串](#)
- 值類型 - 單一值

identitycenter : CredentialId

此內容金鑰是身分增強型角色憑證的隨機 ID，僅用於記錄。由於此索引鍵值無法預測，因此建議您不要將其用於政策中的內容聲明。

- 可用性 – 此金鑰包含在 API AWS STS AssumeRole操作的請求內容中。請求內容包含 IAM Identity Center 發出的內容聲明。
- 資料類型 – [字串](#)
- 值類型 - 單一值

identitycenter : InstanceArn

此內容索引鍵是發出 內容聲明之 IAM Identity Center 執行個體的 ARNidentitystore:UserID。您可以使用此金鑰來判斷 identitystore:UserID和 內容聲明是否來自預期的 IAM Identity Center 執行個體 ARN。

- 可用性 – 此金鑰包含在 API AWS STS AssumeRole操作的請求內容中。請求內容包含 IAM Identity Center 發出的內容聲明。
- 資料類型 – [Arn](#)、[String](#)
- 值類型 - 單一值

在 IAM Identity Center 中記錄和監控

最佳實務是監控您的組織，以確保記錄變更。監控可協助您確保調查任何非預期的變更，並復原不需要的變更。IAM Identity Center 目前支援兩種 AWS 服務，可協助您監控組織及其內發生的活動：AWS CloudTrail 以及 Amazon EventBridge。

主題

- [使用 記錄 IAM Identity Center API 呼叫 AWS CloudTrail](#)
- [使用 記錄 IAM Identity Center SCIM API 呼叫 AWS CloudTrail](#)
- [使用 Amazon EventBridge 連接應用程式元件](#)
- [記錄可設定的 AD 同步錯誤](#)

使用 記錄 IAM Identity Center API 呼叫 AWS CloudTrail

AWS IAM Identity Center 已與 服務整合 AWS CloudTrail，此服務提供使用者、角色或 AWS 服務在 IAM Identity Center 中所採取動作的記錄。CloudTrail 會將 IAM Identity Center 的 API 呼叫擷取為事件。擷取的呼叫包括來自 IAM Identity Center 主控台的呼叫，以及對 IAM Identity Center API 操作的程式碼呼叫。如果您建立[線索](#)，您可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 IAM Identity Center 的事件。如果您未設定追蹤，您仍然可以在 CloudTrail 主控台的事件歷史記錄中檢視最新的事件。您可以使用 CloudTrail 所收集的資訊，判斷向 IAM Identity Center 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「[AWS CloudTrail 使用者指南](#)」。

下表摘要說明 IAM Identity Center 的 CloudTrail 事件、其 CloudTrail 事件來源，以及相符 APIs。請參閱 [IAM Identity Center API 參考](#) 以進一步了解 APIs。

Note

還有一組額外的 CloudTrail 事件，稱為 Sign-in，會 AWS 發出以 IAM Identity Center 使用者 AWS 身分登入。這些事件沒有相符 APIs，因此未列在 API 參考中。

CloudTrail 事件	公 APIs	Description	CloudTrail 事件來源
IAM Identity Center	IAM Identity Center	IAM Identity Center APIs 可管理許可集、	sso.amazonservices.com

CloudTrail 事件	公APIs	Description	CloudTrail 事件來源
		應用程式、信任權杖發行者、帳戶和應用程式指派、IAM Identity Center 執行個體和標籤。	
身分存放區	身分存放區	Identity Store APIs可讓您管理員工使用者和群組的生命週期，以及使用者的群組成員資格。此外，它們也支援管理使用者的MFA裝置。	sso-directory.amazonaws.com, identitystore.amazonaws.com
OIDC	OIDC	OIDC APIs支援受信任的身分傳播，並以已驗證的 IAM Identity Center 使用者身分登入 AWS CLI 和 IDE 工具組。	sso.amazonaws.com, sso-oidauth.amazonaws.com
AWS 存取入口網站	AWS 存取入口網站	AWS 存取入口網站 APIs 支援 AWS 存取入口網站的操作，並支援使用者透過取得帳戶登入資料 AWS CLI。	sso.amazonaws.com
SCIM	SCIM	SCIM APIs 支援透過 SCIM 通訊協定佈建使用者、群組和群組成員資格。如需詳細資訊，請參閱 使用記錄 IAM Identity Center SCIM API 呼叫 AWS CloudTrail 。	identitystore-scim.amazonaws.com

CloudTrail 事件	公APIs	Description	CloudTrail 事件來源
AWS 登入	無公有 API	AWS 向 IAM Identity Center 發出使用者身分驗證和聯合流程的登入 CloudTrail 事件。	signin.amazonaws.com

主題

- [IAM Identity Center 的 CloudTrail 使用案例](#)
- [CloudTrail 中的 IAM Identity Center 資訊](#)

IAM Identity Center 的 CloudTrail 使用案例

IAM Identity Center 發出的 CloudTrail 事件對於各種使用案例可能很有價值。組織可以使用這些事件日誌來監控和稽核使用者在其 AWS 環境中的存取和活動。這有助於合規使用案例，因為日誌會擷取存取資源的人員和時間的詳細資訊。您也可以使用 CloudTrail 資料進行事件調查，讓團隊分析使用者動作並追蹤可疑行為。此外，事件歷史記錄可以支援故障診斷工作，提供一段時間內對使用者許可和組態所做的變更的可見性。

下列各節說明通知工作流程的基本使用案例，例如稽核、事件調查和故障診斷。

在 IAM Identity Center 使用者起始的 CloudTrail 事件中識別使用者

IAM Identity Center 會發出兩個 CloudTrail 欄位，讓您識別 CloudTrail 事件後方的 IAM Identity Center 使用者，例如登入 IAM Identity Center AWS CLI 或使用 AWS 存取入口網站，包括管理 MFA 裝置：

- `userId` – IAM Identity Center 執行個體的 Identity Store 中唯一且不變的使用者識別符。
- `identityStoreArn` – 包含使用者的 Identity Store 的 Amazon Resource Name (ARN)。

`userId` 和 `identityStoreArn` 欄位會顯示在巢狀於 `onBehalfOf` 元素內的 [userIdentity](#) 元素中，如下列範例 CloudTrail 事件日誌所示。此事件日誌會在 `userIdentity` 類型為 "IdentityCenterUser" 的事件上顯示這兩個欄位。您也可以在已驗證 IAM Identity Center 使用者的事件上找到這些欄位，其中 `userIdentity` 類型為 "Unknown"。您的工作流程應該接受這兩種類型值。

```
"userIdentity":{
```

```
"type": "IdentityCenterUser",
"accountId": "111122223333",
"onBehalfOf": {
  "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
  "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
},
"credentialId": "90e292de-5eb8-446e-9602-90f7c45044f7"
}
```

Tip

我們建議您使用 `userId` 和 `identityStoreArn` 來識別 IAM Identity Center CloudTrail 事件後方的使用者。`userIdentity` 元素下的 `userName` 和 `principalId` 欄位不再可用。如果您的工作流程，例如稽核或事件回應，取決於是否有權存取 `username`，您有兩個選項：

- 從 IAM Identity Center 目錄擷取使用者名稱，如 中所述[登入 CloudTrail 事件中的使用者名稱](#)。
- 在登入中的 `additionalEventData` 元素下取得 `UserName` IAM Identity Center 發出的。此選項不需要存取 IAM Identity Center 目錄。如需詳細資訊，請參閱[登入 CloudTrail 事件中的使用者名稱](#)。

若要擷取使用者的詳細資訊，包括 `username` 欄位，您可以使用使用者 ID 和 Identity Store ID 做為參數來查詢 Identity Store。您可以透過 [DescribeUser](#) API 請求或透過 CLI 執行此動作。以下是範例 CLI 命令。如果您的 IAM Identity Center 執行個體位於 CLI 預設區域中，您可以省略 `region` 參數。

```
aws identitystore describe-user \
--identity-store-id d-1234567890 \
--user-id 544894e8-80c1-707f-60e3-3ba6510dfac1 \
--region your-region-id
```

若要判斷上一個範例中 CLI 命令的 Identity Store ID 值，您可以從 `identityStoreArn` 值擷取 Identity Store ID。在範例 ARN 中 `arn:aws:identitystore::111122223333:identitystore/d-1234567890`，身分存放區 ID 為 `d-1234567890`。或者，您也可以從 IAM Identity Center 主控台的設定區段中導覽至 Identity Store 索引標籤，以尋找 Identity Store ID。

如果您要自動查詢 IAM Identity Center 目錄中的使用者，建議您預估使用者查詢的頻率，並考慮 [Identity Store API 上的 IAM Identity Center 限流限制](#)。快取擷取的使用者屬性可協助您保持在限流限制內。

關聯相同使用者工作階段中的使用者事件

登入事件中發出的 [AuthWorkflowID](#) 欄位可在 IAM Identity Center 使用者工作階段開始之前，追蹤與登入序列相關聯的所有 CloudTrail 事件。

對於 AWS 存取入口網站內的使用者動作，`credentialId` 值會設定為用於請求動作之 IAM Identity Center 使用者工作階段的 ID。您可以使用此值來識別在 AWS 存取入口網站的相同已驗證 IAM Identity Center 使用者工作階段中啟動的 CloudTrail 事件。

Note

您無法使用 `credentialId` 將登入事件與後續事件建立關聯，例如使用 AWS 存取入口網站。在登入事件中發出的 `credentialId` 欄位值具有內部使用，我們建議您不要依賴它。使用 OIDC 叫用之 [AWS 存取入口網站事件](#) 所發出的 `credentialId` 欄位值等於存取字符的 ID。

在 IAM Identity Center 使用者起始的 CloudTrail 事件中識別使用者背景工作階段詳細資訊

下列 CloudTrail 事件會擷取 OAuth 2.0 權杖交換的程序，其中代表使用者互動式工作階段的現有存取權杖 (`subjectToken`) 會交換為重新整理權杖 (`requestedTokenType`)。重新整理字符允許任何使用者啟動的長期執行任務繼續使用使用者的許可執行，即使在使用者登出之後也是如此。

對於 IAM Identity Center [使用者背景工作階段](#)，CloudTrail 事件會在 `resource` 元素中包含名為 `requestParameters` 元素。`resource` 參數包含在背景執行之任務的 Amazon Resource Name (ARN)。此元素僅存在於 CloudTrail 事件記錄中，不包含在 IAM Identity Center [CreateTokenWithIAM](#) API 或 SDK 回應中。

```
{
  "clientId": "EXAMPLE-CLIENT-ID",
  "grantType": "urn:ietf:params:oauth:grant-type:token-exchange",
  "code": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "redirectUri": "https://example.com/callback",
  "assertion": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectTokenType": "urn:ietf:params:oauth:token-type:access_token",
  "requestedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
```

```
"resource": "arn:aws:sagemaker:us-west-2:123456789012:training-job/my-job"
}
```

在 IAM Identity Center 和外部目錄之間關聯使用者

IAM Identity Center 提供兩個使用者屬性，您可以用來將其目錄中的使用者與外部目錄中的相同使用者（例如 Microsoft Active Directory 和 ）建立關聯 Okta Universal Directory。

- **externalId** – IAM Identity Center 使用者的外部識別符。我們建議您將此識別符映射到外部目錄中的不可變使用者識別符。請注意，IAM Identity Center 不會在 CloudTrail 中發出此值。
- **username** – 使用者通常登入的客戶提供值。值可能會變更（例如，使用 SCIM 更新）。請注意，當身分來源為 時 Directory Service，IAM Identity Center 在 CloudTrail 中發出的使用者名稱會與您輸入要驗證的使用者名稱相符。使用者名稱不需要與 IAM Identity Center 目錄中的使用者名稱完全相符。

如果您可存取 CloudTrail 事件，但無法存取 IAM Identity Center 目錄，則可以使用登入時在 `additionalEventData` 元素下發出的使用者名稱。如需 中使用者名稱的詳細資訊 `additionalEventData`，請參閱 [登入 CloudTrail 事件中的使用者名稱](#)。

當身分來源為 時，IAM Identity Center 會定義這兩個使用者屬性與外部目錄中對應使用者屬性的映射 Directory Service。如需資訊，請參閱 [IAM Identity Center 與外部身分提供者目錄之間的屬性映射](#)。使用 SCIM 佈建使用者的外部 IdPs 有自己的映射。即使您使用 IAM Identity Center 目錄做為身分來源，也可以使用 `externalId` 屬性將安全主體交叉參考至外部目錄。

下一節說明如何根據使用者的 `username` 和 來查詢 IAM Identity Center 使用者 `externalId`。

依使用者名稱和 `externalId` 檢視 IAM Identity Center 使用者

您可以從 IAM Identity Center 目錄擷取已知使用者名稱的使用者屬性，方法是先 `userId` 使用 [GetUserId](#) API 請求請求對應的 ，然後發出 [DescribeUser](#) API 請求，如先前範例所示。下列範例示範如何 `userId` 從 Identity Store 擷取特定使用者名稱的 。如果您的 IAM Identity Center 執行個體位於使用 CLI 的預設區域中，您可以省略 `region` 參數。

```
aws identitystore get-user-id \
  --identity-store d-9876543210 \
  --alternate-identifier '{
    "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
    }
  }
```



```
}  
    }' \  
--region your-region-id
```

同樣地，當您知道時，可以使用相同的機制 `externalId`。使用 `externalId` 值更新先前範例中的屬性路徑，並使用您要搜尋 `externalId` 的特定更新屬性值。

在 Microsoft Active Directory (AD) 和 `externalId` 中檢視使用者的安全識別符 (SID)

在某些情況下，IAM Identity Center 會在 CloudTrail 事件的 `principalId` 欄位中發出使用者的 SID，例如 AWS 存取入口網站和 OIDC APIs 發出的 SID。這些案例正在逐步淘汰。當您需要 AD 的唯一使用者識別符 `objectguid` 時，建議您的工作流程使用 AD 屬性。您可以在 IAM Identity Center 目錄中的 `externalId` 屬性中找到此值。不過，如果您的工作流程需要使用 SID，請從 AD 擷取該值，因為它無法透過 IAM Identity Center APIs 使用。

[關聯相同使用者工作階段中的使用者事件](#) 說明如何使用 `externalId` 和 `username` 欄位，將 IAM Identity Center 使用者與外部目錄中相符的使用者建立關聯。根據預設，IAM Identity Center 會映射 `externalId` 至 AD `objectguid` 中的屬性，而且此映射是固定的。IAM Identity Center 允許管理員靈活地映射到 AD `userprincipalname` 中的 `username` 預設映射。

您可以在 IAM Identity Center 主控台中檢視這些映射。導覽至設定中的身分來源索引標籤，然後在動作功能表中選擇管理同步。在管理同步區段中，選擇檢視屬性映射按鈕。

雖然您可以使用 IAM Identity Center 中提供的任何唯一 AD 使用者識別符來查詢 AD 中的使用者，但我們建議您在查詢 `objectguid` 中使用，因為它是不可變的識別符。下列範例說明如何使用 Powershell 查詢 Microsoft AD，以使用使用者的 `objectguid` 值擷取使用者 `16809ecc-7225-4c20-ad98-30094aefdbca`。此查詢的成功回應包含使用者的 SID。

```
Install-WindowsFeature -Name RSAT-AD-PowerShell  
  
Get-ADUser `   
-Filter {objectGUID -eq [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `   
-Properties *
```

CloudTrail 中的 IAM Identity Center 資訊

當您建立帳戶 AWS 帳戶時，您的上會啟用 CloudTrail。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 服務事件一起記錄在 CloudTrail 事件中。您可以在中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱[使用 CloudTrail 事件歷史記錄檢視事件](#)。

 Note

如需有關使用者識別和追蹤 CloudTrail 事件中使用者動作如何演變的詳細資訊，請參閱 AWS 安全部落格中 [IAM Identity Center 的重要 CloudTrail 事件變更](#)。

若要持續記錄 中的事件 AWS 帳戶，包括 IAM Identity Center 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南中的以下主題：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案](#)

當您的 中啟用 CloudTrail 記錄時 AWS 帳戶，日誌檔案中會追蹤對 IAM Identity Center 動作發出的 API 呼叫。IAM Identity Center 記錄會與日誌檔案中的其他 AWS 服務記錄一起寫入。CloudTrail 會根據期間與檔案大小，決定何時建立與寫入新檔案。

支援 IAM Identity Center APIs CloudTrail 事件

下列各節提供有關與 IAM Identity Center 支援的下列 APIs 相關聯的 CloudTrail 事件的資訊：

- [IAM Identity Center API](#)
- [Identity Store API](#)
- [OIDC API](#)
- [AWS 存取入口網站 API](#)
- [SCIM API](#)

IAM Identity Center API 操作的 CloudTrail 事件

下列清單包含公有 IAM Identity Center 操作隨事件來源發出的 CloudTrail sso.amazonaws.com 事件。如需公有 IAM Identity Center API 操作的詳細資訊，請參閱 [IAM Identity Center API 參考](#)。

您可以在 CloudTrail 中找到主控台依賴的 IAM Identity Center 主控台 API 操作的其他事件。如需這些主控台 APIs 的詳細資訊，請參閱[服務授權參考](#)。

- [AttachCustomerManagedPolicyReferenceToPermissionSet](#)
- [AttachManagedPolicyToPermissionSet](#)
- [CreateAccountAssignment](#)
- [CreateApplication](#)
- [CreateApplicationAssignment](#)
- [CreateInstance](#)
- [CreateInstanceAccessControlAttributeConfiguration](#)
- [CreatePermissionSet](#)
- [CreateTrustedTokenIssuer](#)
- [DeleteAccountAssignment](#)
- [DeleteApplication](#)
- [DeleteApplicationAccessScope](#)
- [DeleteApplicationAssignment](#)
- [DeleteApplicationAuthenticationMethod](#)
- [DeleteApplicationGrant](#)
- [DeleteInlinePolicyFromPermissionSet](#)
-

[DeleteInstance](#)

-

[DeleteInstanceAccessControlAttributeConfiguration](#)

-

[DeletePermissionsBoundaryFromPermissionSet](#)

-

[DeletePermissionSet](#)

-

[DeleteTrustedTokenIssuer](#)

-

[DescribeAccountAssignmentCreationStatus](#)[S](#)

-

[DescribeAccountAssignmentDeletionStatus](#)

-

[DescribeApplication](#)

-

[DescribeApplicationAssignment](#)

-

[DescribeApplicationProvider](#)

-

[DescribeInstance](#)

-

[DescribeInstanceAccessControlAttributeConfiguration](#)

-

[DescribePermissionSet](#)

-

[DescribePermissionSetProvisioningStatus](#)

-

[DescribeTrustedTokenIssuer](#)

-

[DetachCustomerManagedPolicyReferenceFromPermissionSet](#)

•

[DetachManagedPolicyFromPermissionSet](#)

•

[GetApplicationAccessScope](#)

•

[GetApplicationAssignmentConfiguration](#)

•

[GetApplicationAuthenticationMethod](#)

•

[GetApplicationGrant](#)

•

[GetInlinePolicyForPermissionSet](#)

•

[GetPermissionsBoundaryForPermissionSet](#)

•

[ListAccountAssignmentCreationStatus](#)

•

[ListAccountAssignmentDeletionStatus](#)

•

[ListAccountAssignments](#)

•

[ListAccountAssignmentsForPrincipal](#)

•

[ListAccountsForProvisionedPermissionSet](#)

•

[ListApplicationAccessScopes](#)

•

[ListApplicationAssignments](#)

•

[ListApplicationAssignmentsForPrincipal](#)

•

[ListApplicationAssignmentsForPrincipal](#)

- [ListApplicationAuthenticationMethods](#)
- [ListApplicationGrants](#)
- [ListApplicationProviders](#)
- [ListApplications](#)
- [ListCustomerManagedPolicyReferencesInPermissionSet](#)
- [ListInstances](#)
- [ListManagedPoliciesInPermissionSet](#)
- [ListPermissionSetProvisioningStatus](#)
- [ListPermissionSets](#)
- [ListPermissionSetsProvisionedToAccount](#)
- [ListTagsForResource](#)
- [ListTrustedTokenIssuers](#)
- [ProvisionPermissionSet](#)
- [PutApplicationAccessScope](#)
- [PutApplicationAssignmentConfiguration](#)

- [PutApplicationAuthenticationMethod](#)
- [PutApplicationGrant](#)
- [PutInlinePolicyToPermissionSet](#)
- [PutPermissionsBoundaryToPermissionSet](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateApplication](#)
- [UpdateInstance](#)
- [UpdateInstanceAccessControlAttributeConfiguration](#)
- [UpdatePermissionSet](#)
- [UpdateTrustedTokenIssuer](#)

Identity Store API 操作的 CloudTrail 事件

下列清單包含公有 Identity Store 操作隨事件來源發出的 CloudTrail

identitystore.amazonaws.com事件。如需公有 Identity Store API 操作的詳細資訊，請參閱[Identity Store API 參考](#)。

您可能會在 CloudTrail 中找到具有事件來源的 Identity Store 主控台 API 操作的其他sso-directory.amazonaws.com事件。這些 APIs支援 主控台和 AWS 存取入口網站。如果您需要偵測特定操作的發生，例如將成員新增至群組，建議您同時考慮公有和主控台 API 操作。如需這些主控台 APIs的詳細資訊，請參閱[服務授權參考](#)。

- [CreateGroup](#)
- [CreateGroupMembership](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteGroupMembership](#)
- [DeleteUser](#)
- [DescribeGroup](#)
- [DescribeGroupMembership](#)
- [DescribeUser](#)
- [GetGroupId](#)
- [GetGroupMembershipId](#)
- [GetUserId](#)
- [IsMemberInGroups](#)
- [ListGroupMemberships](#)
- [ListGroupMembershipsForMember](#)
- [ListGroups](#)
- [ListUsers](#)
- [UpdateGroup](#)
- [UpdateUser](#)

OIDC API 操作的 CloudTrail 事件

下列清單包含公有 OIDC 操作發出的 CloudTrail 事件。如需公有 OIDC API 操作的詳細資訊，請參閱 [OIDC API 參考](#)。

- [CreateToken](#) (事件來源 `sso.amazonaws.com`)
- [CreateTokenWithIAM](#) (事件來源 `sso-oauth.amazonaws.com`)

AWS 存取入口網站 API 操作的 CloudTrail 事件

下列清單包含 AWS 存取入口網站 API 操作隨事件來源發出的 CloudTrail `sso.amazonaws.com` 事件。標記為在公有 API 中無法使用的 API 操作支援 AWS 存取入口網站的操作。使用 AWS CLI 可能會

導致公有 AWS 存取入口網站 API 操作和公有 API 中無法使用的 CloudTrail 事件同時發出。如需公開 AWS 存取入口網站 API 操作的詳細資訊，請參閱[AWS 存取入口網站 API 參考](#)。

- Authenticate (不適用於公有 API。提供 AWS 存取入口網站的登入。)
- Federate (不適用於公有 API。為應用程式提供聯合。)
- [ListAccountRoles](#)
- [ListAccounts](#)
- ListApplications (不適用於公有 API。提供使用者指派的資源，以在 AWS 存取入口網站中顯示。)
- ListProfilesForApplication (不適用於公有 API。提供應用程式中繼資料以在 AWS 存取入口網站中顯示。)
- [GetRoleCredentials](#)
- [Logout](#)

SCIM API 操作的 CloudTrail 事件

如需公有 SCIM API 操作的相關資訊，請參閱[AWS 存取入口網站 API 參考](#)。

IAM Identity Center CloudTrail 事件中的身分資訊

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：

- 請求是否使用根使用者還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了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。
- 請求是否由 IAM Identity Center 使用者提出。若是如此，CloudTrail 事件中會提供 `userId` 和 `identityStoreArn` 欄位，以識別啟動請求的 IAM Identity Center 使用者。如需詳細資訊，請參閱[在 IAM Identity Center 使用者起始的 CloudTrail 事件中識別使用者](#)。

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

Note

目前，IAM Identity Center 不會發出 CloudTrail 事件，讓使用者使用 [OIDC API](#) 登入 AWS 受管 Web 應用程式（例如 Amazon SageMaker AI Studio）。這些 Web 應用程式是一組更廣泛的子集，[the section called “AWS 受管應用程式”](#)，其中也包含非 Web 應用程式，例如 Amazon Athena SQL 和 Amazon S3 Access Grants。

了解 IAM Identity Center 的 CloudTrail 事件

追蹤是一種組態，能讓事件交付到您指定的 Amazon S3 儲存貯體。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 事件不是公有 API 呼叫的排序堆疊追蹤，因此不會以任何特定順序顯示。請參閱 [CloudTrail 使用者指南](#)，了解 [CloudTrail 記錄的內容](#)。CloudTrail

此範例示範 CloudTrail 日誌項目，擷取與 IAM Identity Center 互動的 IAM 使用者 (samadams) 所執行 DescribePermissionsPolicies 的動作：

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJAIENLMexample",
        "arn": "arn:aws:iam::08966example:user/samadams",
        "accountId": "111122223333",
        "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": "111122223333"
    }
  ]
}
```

```
}
```

此範例示範 CloudTrail 日誌項目，擷取 AWS 存取入口網站內 IAM Identity Center 使用者執行 ListApplications 的動作：

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IdentityCenterUser",
        "accountId": "111122223333",
        "onBehalfOf": {
          "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
          "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "credentialId": "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
      },
      "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": "111122223333"
    }
  ]
}
```

此範例示範 CloudTrail 日誌項目，擷取由使用 IAM Identity Center OIDC 服務進行驗證的 IAM Identity Center 使用者所執行 CreateToken 的動作：

```
{
  "eventVersion": "1.05",
  "userIdentity": {
```

```

    "type": "IdentityCenterUser",
    "accountId": "111122223333",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
  },
  "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": "111122223333",
      "type": "IdentityStoreId",
      "ARN": "d-1234567890"
    }
  ],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

了解 IAM Identity Center 登入事件

AWS CloudTrail 會記錄所有 IAM Identity Center 身分來源的成功和失敗登入事件。IAM Identity Center 和 Active Directory (AD Connector 和 AWS Managed Microsoft AD) 來源身分包括每次提示使用者解決特定登入資料挑戰或因素時所擷取的額外登入事件，以及該特定登入資料驗證請求的狀態。只有在使用者完成所有必要的登入資料挑戰後，才會登入使用者，這將導致記錄 `UserAuthentication` 事件。

下表擷取每個 IAM Identity Center 登入 CloudTrail 事件名稱、其目的和對不同身分來源的適用性。

事件名稱	事件目的	身分來源適用性
<code>CredentialChallenge</code>	用來通知 IAM Identity Center 已請求使用者解決特定登入資料挑戰 <code>CredentialType</code> ，並指定必要的（例如 <code>PASSWORD</code> 或 <code>TOTP</code> ）。	原生 IAM Identity Center 使用者、AD Connector 和 AWS Managed Microsoft AD
<code>CredentialVerification</code>	用來通知使用者已嘗試解決特定 <code>CredentialChallenge</code> 請求，並指定該登入資料是否成功。	原生 IAM Identity Center 使用者、AD Connector 和 AWS Managed Microsoft AD
<code>UserAuthentication</code>	用來通知使用者遭挑戰的所有身分驗證要求都已成功完成，而且使用者已成功登入。使用者若未成功完成所需的登入資料挑戰，將不會記錄任何 <code>UserAuthentication</code> 事件。	所有身分來源

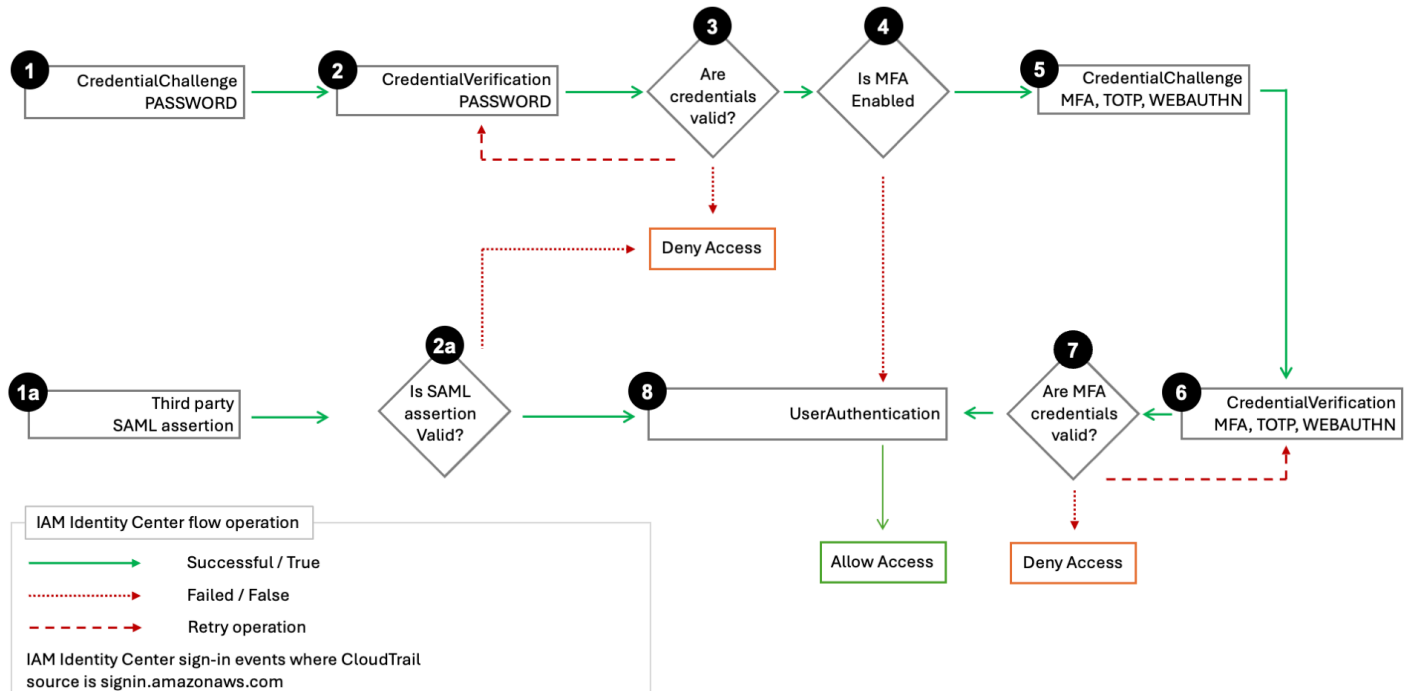
下表擷取特定登入 CloudTrail 事件中包含的其他實用事件資料欄位。

欄位	事件目的	登入事件適用性	範例值
<code>AuthWorkflowID</code>	用來關聯在整個登入序列中發出的所有事件。對於每個使用者	<code>CredentialChallenge</code>	"AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83"

欄位	事件目的	登入事件適用性	範例值
	登入，IAM Identity Center 可能會發出多個事件。	e , CredentialVerification , UserAuthentication	
CredentialType	用來指定受到挑戰的登入資料或因素。UserAuthentication 事件將包含跨使用者登入序列成功驗證的所有CredentialType 值。	CredentialChallenge , CredentialVerification , UserAuthentication	CredentialType" : "PASSWORD" 或 "CredentialType" : "PASSWORD , TOTP" (可能的值包括 : PASSWORD、TOTP、WEBAUTHN、EXTERNAL_IDP、RESYNC_TOTP、EMAIL_OTP)
DeviceEnrollmentRequired	用來指定使用者在登入期間需要註冊 MFA 裝置，且使用者已成功完成該請求。	UserAuthentication	"DeviceEnrollmentRequired" : "true"
LoginTo	用來指定成功登入序列之後的重新導向位置。	UserAuthentication	"LoginTo" : "https://mydirectory.awsapps.com/start/...."

IAM Identity Center 登入流程中的 CloudTrail 事件

下圖說明登入流程和登入發出的 CloudTrail 事件。



圖表顯示密碼登入流程和聯合登入流程。

密碼登入流程由步驟 1–8 組成，示範使用者名稱和密碼登入程序期間的步驟。IAM Identity Center `userIdentity.additionalEventData.CredentialType` 設定為 "PASSWORD"，IAM Identity Center 會經歷登入資料挑戰回應週期，並視需要重試。

步驟數量取決於[登入類型和是否存在多重要素驗證 \(MFA\)](#)。初始程序會產生三或五個 CloudTrail `UserAuthentication` 事件，並結束序列以成功進行身分驗證。當 IAM Identity Center 為 `CredentialChallenge` 一般或啟用 MFA 身分驗證重新發出時，密碼身分驗證嘗試失敗會導致額外的 CloudTrail 事件。

密碼登入流程也涵蓋使用 `CreateUser` API 呼叫新建立的 IAM Identity Center 使用者使用一次性密碼 (OTP) 登入的情況。在此案例中，登入資料類型為「EMAIL_OTP」。

聯合登入流程由步驟 1a、2a 和 8 組成，示範聯合身分驗證程序期間的主要步驟，其中 [SAML 聲明由身分提供者提供](#)、由 IAM Identity Center 驗證，如果成功，則會導致 `UserAuthentication`。IAM Identity Center 不會在步驟 3–7 中叫用內部 MFA 身分驗證序列，因為外部聯合身分提供者負責所有使用者憑證驗證。

登入 CloudTrail 事件中的使用者名稱

IAM Identity Center 會在每次成功登入 IAM Identity Center 使用者時，發出 `additionalEventData` 元素下的 `UserName` 欄位一次。以下清單說明範圍內的兩個登入事件，以及這些事件發生的條件。當使用者登入時，只有其中一個條件是 `true`。

- `CredentialChallenge`
 - 當 `CredentialType` 為「PASSWORD」時 – 適用於使用 Directory Service 或 進行密碼驗證 IAM Identity Center 目錄。
 - 當 `CredentialType` 為「EMAIL_OTP」 – 僅適用於使用 `CreateUser` API 呼叫建立 IAM Identity Center 目錄 的使用者第一次嘗試登入時，使用者會收到一次性密碼，以使用該密碼登入一次。
- `UserAuthentication`
 - 當 `CredentialType` 為「EXTERNAL_IDP」時 – 適用於使用外部 IdP 的身分驗證。

成功驗證 `UserName` 的 值如下所示：

- 當身分來源是外部 IdP 時，該值等於傳入 SAML 聲明中的 `nameID` 值。此值等於 中的 `UserName` 欄位 IAM Identity Center 目錄。
- 當身分來源為 時 IAM Identity Center 目錄，發出的值等於此目錄中 `UserName` 的欄位。
- 當身分來源為 時 Directory Service，發出的值等於使用者在身分驗證期間輸入的使用者名稱。例如，具有使用者名稱 `anyuser@company.com` 的使用者可以使用 `anyuser`、`anyuser@company.com` 或 進行身分驗證 `company.com/anyuser`，而且在每種情況下，輸入的值都會分別在 CloudTrail 中發出。

不正確使用者名稱嘗試的安全遮罩

當記錄的事件是由不正確的使用者名稱輸入所造成的主控台登入失敗時，`UserName` 欄位會包含字串 `HIDDEN_DUE_TO_SECURITY_REASONS`。在這種情況下，CloudTrail 不會記錄內容，因為文字可能包含敏感資訊，如下列範例所述：

- 使用者不小心在使用者名稱欄位中輸入密碼。
- 使用者不小心輸入個人電子郵件帳戶的帳戶名稱、銀行登入識別符或其他一些私有 ID。

Tip

我們建議您使用 `userId` 和 `identityStoreArn` 來識別 IAM Identity Center CloudTrail 事件後方的使用者。如果您需要使用 `userName` 欄位，您可以在每次成功登入發出一次的 `additionalEventData` 元素 `userName` 下使用。

如需如何使用 `UserName` 欄位的其他資訊，請參閱 [關聯相同使用者工作階段中的使用者事件](#)。

IAM Identity Center 登入案例的範例事件

下列範例說明各種 AWS 登入案例期間產生的典型 CloudTrail 事件序列。這些範例可做為參考模式，協助您解譯身分驗證日誌、識別安全問題，以及驗證身分驗證政策是否正常運作。

主題

- [僅使用密碼進行身分驗證時成功登入](#)
- [向外部身分提供者進行身分驗證時成功登入](#)
- [使用密碼和以時間為基礎的一次性密碼 \(TOTP\) 驗證器應用程式進行身分驗證時成功登入](#)
- [使用密碼進行身分驗證並強制進行 MFA 註冊時，登入成功](#)
- [由於密碼身分驗證不正確而無法登入](#)

僅使用密碼進行身分驗證時成功登入

下列事件序列會擷取僅成功登入密碼的範例。

CredentialChallenge (密碼)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    }
  },
```

```

    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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",
    "UserName":"bobsmith@example.com",
    "CredentialType":"PASSWORD"
  },
  "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
  "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
  "readOnly":false,
  "eventType":"AwsServiceEvent",
  "managementEvent":true,
  "eventCategory":"Management",
  "serviceEventDetails":{
    "CredentialChallenge":"Success"
  }
}

```

成功的 CredentialVerification (密碼)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },

```

```

    "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"
    }
  }
}

```

成功的 UserAuthentication (僅限密碼)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBshIc50BAA6ftz73M6LsfLWDlf0xvi02K3wet946lC30f_iWdilx-zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx-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"
    }
  }
}

```

向外部身分提供者進行身分驗證時成功登入

下列事件序列會擷取使用外部身分提供者透過 SAML 通訊協定進行身分驗證時成功登入的範例。

成功的 UserAuthentication (外部身分提供者)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",

```

```

    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"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
Bsh1Ic50BAA6ftz73M6LsfLWD1f0xvi02K3wet9461C30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx
east-1",
  "CredentialType":"EXTERNAL_IDP",
  "UserName":"bobsmith@example.com"
},
"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"
}
}

```

使用密碼和以時間為基礎的一次性密碼 (TOTP) 驗證器應用程式進行身分驗證時成功登入

下列事件序列會擷取範例，其中在登入期間需要多重要素驗證，且使用者已成功使用密碼和 TOTP 驗證器應用程式登入。

CredentialChallenge (密碼)

```
{
```

```

"eventVersion":"1.08",
"userIdentity":{
  "type":"IdentityCenterUser",
  "arn":"",
  "accountId":"111122223333",
  "accessKeyId":"",
  "onBehalfOf": {
    "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"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",
  "UserName":"bobsmith@example.com"
},
"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"
}
}

```

成功的 CredentialVerification (密碼)

```

{
  "eventVersion":"1.08",

```



```

"userIdentity":{
  "type":"IdentityCenterUser",
  "arn": "",
  "accountId":"111122223333",
  "accessKeyId": "",
  "onBehalfOf": {
    "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"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":"IdentityCenterUser",

```

```

    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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"
  }
}

```

CredentialVerification (TOTP) 成功

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",

```

```

    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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"
  }
}

```

成功的 UserAuthentication (密碼 + TOTP)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {

```

```

        "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
        "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"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-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFf00108qc3RPF
Sx-pjBXXG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMLui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nnvCaxPTghHbgHCRIXdfffFtzH0sL1ow419Bobn
\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"
}
}

```

使用密碼進行身分驗證並強制進行 MFA 註冊時，登入成功

以下一系列事件示範成功的密碼身分驗證，其中使用者必須先註冊並成功完成多重要素驗證 (MFA)，才能完成登入程序。

CredentialChallenge (密碼)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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",
    "UserName": "bobsmith@example.com"
  },
  "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"
  }
}
```

成功的 CredentialVerification (密碼)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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"
  }
}
```

成功的 UserAuthentication (需要密碼 + MFA 註冊)

```
{
  "eventVersion": "1.08",
```

```

"userIdentity":{
  "type":"IdentityCenterUser",
  "arn": "",
  "accountId":"111122223333",
  "accessKeyId": "",
  "onBehalfOf": {
    "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"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_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HL1N2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY_EgU3fh0L3QWvWiquYnDPMYPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi50YI9QSc
\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"
}

```

```
}
```

由於密碼身分驗證不正確而無法登入

以下一系列事件示範身分驗證嘗試，其中使用者成功輸入使用者名稱，但密碼驗證步驟失敗，導致登入失敗。

CredentialChallenge (密碼)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": ""
  },
  "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",
    "UserName": "bobsmith@example.com"
  },
  "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"
  }
}
```


CredentialVerification失敗（密碼）

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": ""
  },
  "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"
  }
}
```

使用 記錄 IAM Identity Center SCIM API 呼叫 AWS CloudTrail

[IAM Identity Center SCIM](#) 已與 整合 AWS CloudTrail，此服務可提供使用者、角色或 所採取動作的記錄 AWS 服務。CloudTrail 會將 SCIM 的 API 呼叫擷取為事件。使用 CloudTrail 收集的資訊，您可以判斷所請求動作的相關資訊、動作的日期和時間、請求參數等。若要進一步了解 CloudTrail，請參閱 [AWS CloudTrail 使用者指南](#)。

 Note

當您建立帳戶 AWS 帳戶 時，您的上會啟用 CloudTrail。不過，如果您的權杖是在 2024 年 9 月之前建立的，您可能需要輪換存取權杖，才能查看來自 SCIM 的事件。

如需詳細資訊，請參閱[輪換存取字符](#)。

SCIM 支援將下列操作記錄為 CloudTrail 中的事件：

- [CreateGroup](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteUser](#)
- [GetGroup](#)
- [GetSchema](#)
- [GetUser](#)
- [ListGroups](#)
- [ListResourceTypes](#)
- [ListSchemas](#)
- [ListUsers](#)
- [PatchGroup](#)
- [PatchUser](#)
- [PutUser](#)
- [ServiceProviderConfig](#)

CloudTrail 事件範例

下列範例示範使用 IAM Identity Center 在 SCIM 操作期間產生的典型 CloudTrail 事件日誌。這些範例顯示成功操作和常見錯誤案例的事件結構和內容，協助您了解如何在疑難排解 SCIM 佈建問題時解譯 CloudTrail 日誌。

操作成功 **CreateUser**

此 CloudTrail 事件會顯示透過 SCIM API 成功執行 CreateUser 的操作。事件會同時擷取請求參數（已遮罩敏感資訊）和回應元素，包括新建立的使用者 ID。當身分提供者成功使用 SCIM 通訊協定將新使用者佈建至 IAM Identity Center 時，就會產生此類型的事件。

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "WebIdentityUser",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "schemas" : [
        "urn:ietf:params:scim:schemas:core:2.0:User"
      ],
      "name": {
        "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "active": true,
      "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": {
    "meta" : {
      "created" : "Oct 10, 2024, 1:23:45 PM",
      "lastModified" : "Oct 10, 2024, 1:23:45 PM",
      "resourceType" : "User"
    },
    "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
    "schemas" : [
      "urn:ietf:params:scim:schemas:core:2.0:User"
    ]
  }
}
```

```

    ],
    "name": {
      "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "active": true,
    "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}

```

失敗PatchGroup的操作：缺少必要的路徑屬性

此 CloudTrail 事件會顯示失敗PatchGroup的操作，導致 ValidationException出現錯誤訊息 "Missing path in PATCH request"。發生錯誤是因為PATCH操作需要路徑屬性來指定要修改的群組屬性，但請求中缺少此屬性。

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "Missing path in PATCH request",
  "requestParameters": {

```

```

    "httpBody": {
      "operations": [
        {
          "op": "REMOVE",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ],
      "schemas": [
        "HIDDEN_DUE_TO_SECURITY_REASONS"
      ]
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}

```

失敗CreateGroup的操作：群組名稱已存在

此 CloudTrail 事件顯示操作失敗CreateGroup，導致 ConflictException出現錯誤訊息 "Duplicate GroupDisplayName"。嘗試建立顯示名稱已存在於 IAM Identity Center 的群組時，會發生此錯誤。身分提供者必須使用唯一的群組名稱或更新現有的群組，而不是建立新的群組。

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateGroup",

```

```

"awsRegion": "us-east-1",
"sourceIPAddress": "xxx.xxx.xxx.xxx",
"userAgent": "Go-http-client/2.0",
"errorCode": "ConflictException",
"errorMessage": "Duplicate GroupDisplayName",
"requestParameters": {
  "httpBody": {
    "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "tenantId": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

失敗 **PatchUser** 操作：不支援多個電子郵件地址

此 CloudTrail 事件顯示操作失敗 **PatchUser**，導致 `ValidationException` 出現錯誤訊息 "List attribute emails exceeds allowed limit of 1"。嘗試將多個電子郵件地址指派給使用者時發生此錯誤，因為 IAM Identity Center 每個使用者僅支援一個電子郵件地址。身分提供者必須設定 SCIM 映射，才能為每個使用者傳送單一電子郵件地址。

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",

```

```
"userAgent": "Go-http-client/2.0",
"errorCode": "ValidationException",
"errorMessage": "List attribute emails exceeds allowed limit of 1",
"requestParameters": {
  "httpBody": {
    "operations": [
      {
        "op": "REPLACE",
        "path": "emails",
        "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
      }
    ],
    "schemas": [
      "HIDDEN_DUE_TO_SECURITY_REASONS"
    ]
  },
  "tenantId": "xxxx",
  "id": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}
```

IAM Identity Center 中的常見 SCIM API 驗證錯誤

使用 SCIM API 搭配 IAM Identity Center 時，以下驗證錯誤訊息通常會出現在 CloudTrail 事件中。這些驗證錯誤通常發生在使用者和群組佈建操作期間。

如需解決這些錯誤並正確設定 SCIM 佈建的詳細指導，請參閱此[AWS re:Post 文章](#)。

- 清單屬性電子郵件超過允許的 1 限制
- 列出允許的屬性地址限制為 1

- 偵測到 1 個驗證錯誤：'*name.familyName*' 的值無法滿足限制條件：成員必須滿足規則表達式模式：【`\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r`】 +
- 偵測到 2 個驗證錯誤：'name.familyName' 的值無法滿足限制條件：成員的長度必須大於或等於 1；'name.familyName' 的值無法滿足限制條件：成員必須滿足規則表達式模式：【`\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r`】 +
- 偵測到 2 個驗證錯誤：'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value' 的值無法滿足限制條件：成員的長度必須大於或等於 1；'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value' 的值無法滿足限制條件：成員必須滿足規則表達式模式：【`\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r`】 + "，
- RequestBody 的 JSON 無效
- 無效的篩選條件格式

使用 Amazon EventBridge 連接應用程式元件

您可以將 IAM Identity Center 與 [Amazon EventBridge](#) 整合，以引發啟動管理通知或叫用自動化工作流程的事件，以回應 CloudTrail 事件中記錄的特定 IAM Identity Center 動作。

例如，您可以設定 [EventBridge 規則](#) 來偵測使用者何時刪除應用程式，或 IAM Identity Center 何時建立新群組。根據您的使用案例，您可以將這些事件路由到 Amazon SNS 主題，以通知管理員或使用 AWS Lambda [Step Functions](#) 或其他 [EventBridge 支援的服務](#) 叫用其他自動化。

記錄可設定的 AD 同步錯誤

您可以在可設定的 Active Directory (AD) 同步組態上啟用記錄，以接收包含同步程序期間可能發生之錯誤相關資訊的日誌。透過這些日誌，您可以監控可設定的 AD 同步是否存在問題，並在適用時採取動作。您可以將日誌傳送至 Amazon CloudWatch Logs 日誌群組、Amazon Simple Storage Service (Amazon S3) 儲存貯體，或支援跨帳戶交付的 Amazon Data Firehose，適用於 Amazon S3 儲存貯體和 Firehose。

如需限制、許可和付費日誌的詳細資訊，請參閱 [啟用記錄來源 AWS 服務](#)。

Note

您需要支付記錄費用。如需詳細資訊，請參閱 [Amazon CloudWatch 定價](#) 頁面上的 [已修訂日誌](#)。

啟用可設定的 AD 同步錯誤日誌

1. 登入 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，選擇動作，然後選擇管理日誌。
4. 選擇新增日誌交付和下列其中一個目的地類型。
 - a. 選擇至 Amazon CloudWatch Logs。然後選擇或輸入目的地日誌群組。
 - b. 選擇至 Amazon S3。然後選擇或輸入目的地儲存貯體。
 - c. 選擇至 Firehose。然後選擇或輸入目的地交付串流。
5. 選擇提交。

停用可設定的 AD 同步錯誤日誌

1. 登入 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 在設定頁面上，選擇身分來源索引標籤，選擇動作，然後選擇管理日誌。
4. 針對您要移除的目的地，選擇移除。
5. 選擇提交。

可設定的 AD 同步錯誤日誌欄位

如需可能的錯誤日誌欄位，請參閱下列清單。

`sync_profile_name`

同步設定檔的名稱。

`error_code`

代表已發生之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

同步來源是實體的同步來源。對於 IAM Identity Center，這是由 管理的 Active Directory (AD) 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 Identity Center，這是 Identity Store。同步目標包含受影響的 Identity Store ARN。

source_entity_id

造成錯誤的實體的唯一識別符。對於 IAM Identity Center，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

發生錯誤時的時間戳記。

可設定的 AD 同步錯誤日誌範例

範例 1：AD 目錄過期密碼的錯誤日誌

```
{
  "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：具有非唯一使用者名稱之使用者的錯誤日誌

```
{
```

```
"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 Identity Center 的合規驗證

第三方稽核人員會評估的安全與合規，AWS 服務例如 AWS IAM Identity Center 做為多個 AWS 合規計畫的一部分。

若要了解是否 AWS 服務在特定合規計畫範圍內，請參閱[AWS 服務合規計畫範圍內](#)然後選擇您感興趣的合規計畫。如需一般資訊，請參閱[AWS 合規計畫](#)。

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[在 中下載報告 AWS Artifact](#)。

您使用時的合規責任 AWS 服務取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。如需使用時合規責任的詳細資訊 AWS 服務，請參閱[AWS 安全文件](#)。

支援的合規標準

IAM Identity Center 已針對下列標準進行稽核，並有資格做為您需要取得合規認證之解決方案的一部分使用。



AWS 已擴展其健康保險流通與責任法案 (HIPAA) 合規計劃，將 IAM Identity Center 納入為符合 [HIPAA 資格的服務](#)。

AWS 提供以 [HIPAA 為重心的白皮書](#) 給想要進一步了解他們可以如何使用 AWS 服務 來處理和存放健康資訊的客戶。如需詳細資訊，請參閱 [HIPAA 合規](#)。



資訊安全註冊評估商計劃 (IRAP) 可讓澳洲政府客戶確保實施適當的合規控制，並確定適當的責任模型，以解決澳洲網路安全中心 (ACSC) 制定的澳洲政府資訊安全手冊 (ISM) 的要求。如需詳細資訊，請參閱 [IRAP 資源](#)。



IAM Identity Center 在服務提供者層級 1 具有支付卡產業 (PCI) 資料安全標準 (DSS) 3.2 版的合規證明。

使用 AWS 產品和服務來存放、處理或傳輸持卡人資料的客戶，可以在 IAM Identity Center 中使用下列身分來源來管理自己的 PCI DSS 合規認證：

- Active Directory
- 外部身分提供者

IAM Identity Center 身分來源目前不符合 PCI DSS。

如需 PCI DSS 的詳細資訊，包括如何請求 AWS PCI 合規套件的副本，請參閱 [PCI DSS 第 1 級](#)。



系統和組織控制 (SOC) 報告是獨立的第三方檢查報告，示範 IAM Identity Center 如何實現關鍵合規控制和目標。這些報告可協助您和稽核人員了解 控制如何支援操作和合規。SOC 報告有三種類型：

- AWS SOC 1 報告 - [使用 AWS 成品下載](#)
- AWS SOC 2：安全性、可用性和機密性報告 - [使用 AWS 成品下載](#)
- [AWS SOC 3：安全性、可用性和機密性報告](#)

IAM Identity Center 在 AWS SOC 1、SOC 2 和 SOC 3 報告的範圍內。如需詳細資訊，請參閱 [SOC 合規](#)。

IAM Identity Center 中的彈性

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置。AWS 區域提供多個實體隔離和隔離的可用區域，這些區域以低延遲、高輸送量和高度備援的網路連接。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 AWS 區域和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

若要進一步了解 AWS IAM Identity Center 彈性，請參閱 [彈性設計和區域行為](#)。

IAM Identity Center 中的基礎設施安全性

作為受管服務，AWS IAM Identity Center 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 IAM Identity Center。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。

IAM Identity Center 中的資料保護

AWS [共同責任模型](#)適用於 IAM Identity Center AWS 中的資料保護。如此模型所述，AWS 負責保護執行所有雲端的 AWS 全球基礎設施。您負責維護在此基礎設施上託管內容的控制權。您也必須負責您所使用 AWS 服務的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱[資料隱私權常見問答集](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全部落格上的 [AWS 共同責任模型和 GDPR](#) 部落格文章。

建議您以下列方式保護您的資料：

- 搭配 IAM Identity Center 使用多重驗證 (MFA)。
- 使用 TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《使用者指南》中的[使用 CloudTrail 追蹤](#)。
- 使用 AWS 加密解決方案，以及 服務中的所有 AWS 預設安全控制。

我們強烈建議您絕對不要將機密或敏感資訊，例如客戶的電子郵件地址，放入標籤或任意格式的文字欄位中，例如名稱欄位。這包括當您使用 時 AWS IAM Identity Center，或使用 AWS 主控台、API AWS CLI或其他 服務時 AWS SDKs。您在標籤或用於名稱的任意格式文字欄位中輸入的任何資料都可用於診斷日誌。

傳輸中加密

IAM Identity Center 透過使用 Transport Layer Security (TLS) 1.2 或 TLS 1.3 加密通訊協定自動加密所有網路間資料，保護傳輸中往返服務的資料。使用 Signature 第 [AWS 4 版演算法](#)簽署透過 IAM 驗證並傳送至 IAM Identity Center APIs、Identity Store API 或 OIDC API 的直接 HTTPS 請求，以建立安全連線。

資料隱私權

透過 IAM Identity Center，您可以保留對組織資料的控制。只有在您使用 IAM Identity Center 啟用其他 AWS 服務，以及這些服務需要時，儲存在 IAM Identity Center 中的使用者和群組身分才會與其他 服務共用，例如[AWS 受管應用程式](#)。

如需詳細資訊，請參閱[AWS 資料隱私權常見問答集](#)。

資料保留

IAM Identity Center 會儲存您的資料，例如使用者和群組身分和中繼資料，直到您從服務中刪除它們為止。當您刪除 IAM Identity Center 執行個體時，它包含的資料也會一併刪除。

靜態加密

IAM Identity Center 提供加密，以使用下列金鑰類型保護靜態客戶資料：

- **AWS 擁有的金鑰（預設金鑰類型）** — IAM Identity Center 預設使用這些金鑰自動加密您的資料。您無法檢視、管理、稽核其使用方式，或將 AWS 擁有的金鑰用於其他用途。IAM Identity Center 會完全處理金鑰管理，以確保資料的安全，而無須採取任何動作。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》<https://docs.aws.amazon.com/kms/latest/developerguide/overview.html> 中的 [AWS 擁有的金鑰](#)。
- **客戶受管金鑰** — 在 IAM Identity Center 的組織執行個體中，您可以選擇對稱客戶受管金鑰，用於加密其餘人力資源身分資料，例如使用者和群組屬性。您可以建立、擁有和管理這些加密金鑰。您可以完全控制此層加密，因此能執行以下任務：
 - 建立和維護金鑰政策，以限制只有需要存取的 IAM 主體才能存取金鑰，例如 IAM Identity Center 和相同 AWS Organizations 及其管理員 [AWS 受管應用程式](#)。
 - 建立和維護存取金鑰的 IAM 政策，包括跨帳戶存取
 - 啟用和停用金鑰政策
 - 輪換金鑰密碼編譯資料
 - 稽核需要金鑰存取的資料存取權
 - 新增 標籤
 - 建立金鑰別名
 - 安排金鑰供刪除

若要了解如何在 IAM Identity Center 中實作客戶受管 KMS 金鑰，請參閱 [在中實作客戶受管 KMS 金鑰 AWS IAM Identity Center](#)。如需客戶受管金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的 [客戶受管金鑰](#)。

Note

IAM Identity Center 會使用 AWS 擁有的 KMS 金鑰自動啟用靜態加密，以免費保護客戶資料。不過，使用客戶受管金鑰時會產生 AWS KMS 費用。如需定價的詳細資訊，請參閱 [AWS Key Management Service 定價](#)。

實作客戶受管金鑰的考量：

- 專用金鑰：我們建議為每個 IAM Identity Center 執行個體建立新的專用客戶受管 KMS 金鑰，而不是重複使用現有的金鑰。這種方法提供更明確的職責分離、簡化存取控制管理，並使安全稽核更加直接。擁有專用金鑰也會透過限制金鑰變更對單一 IAM Identity Center 執行個體的影響來降低風險。
- 跨多個使用 IAM Identity Center AWS 區域：如果您計劃將 IAM Identity Center 執行個體複寫至其他執行個體 AWS 區域，則需要使用客戶受管 KMS 金鑰進行靜態加密。多區域 IAM Identity Center 不支援預設 AWS 擁有的 KMS 金鑰類型。如需詳細資訊，請參閱[跨多個使用 IAM Identity Center AWS 區域](#)。

Note

IAM Identity Center 使用[信封加密](#)來加密您的人力資源身分資料。您的 KMS 金鑰扮演包裝金鑰的角色，可加密實際用來加密資料的資料金鑰。

如需 AWS KMS 的詳細資訊，請參閱[什麼是 AWS Key Management Service ?](#)

IAM Identity Center 加密內容

[加密內容](#)是一組選用的非私密金鑰值對，其中包含有關資料的其他內容資訊。AWS KMS 會使用加密內容作為額外的已驗證資料，以支援已驗證的加密。當您在加密資料的請求中包含加密內容時，會將加密內容 AWS KMS 繫結至加密的資料。若要解密資料，您必須在請求中包含相同的加密內容。如需加密內容的詳細資訊，請參閱[AWS KMS 開發人員指南](#)。

IAM Identity Center 使用來自下列項目的加密內容金鑰：aws:sso:instance-arn、aws:identitystore:identitystore-arn 和 tenant-key-id。例如，下列加密內容可能會出現在 IAM Identity Center AWS KMS API 調用的 API 操作中。<https://docs.aws.amazon.com/singlesignon/latest/APIReference/welcome.html>

```
"encryptionContext": {  
  "tenant-key-id": "ssoins-1234567890abcdef",  
  "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"  
}
```

以下加密內容可能會出現在 Identity Store AWS KMS API 調用的 API 操作中。<https://docs.aws.amazon.com/singlesignon/latest/IdentityStoreAPIReference/welcome.html>


```
"encryptionContext": {
  "tenant-key-id": "12345678-1234-1234-1234-123456789012",
  "aws:identitystore:identitystore-arn":
    "arn:aws:identitystore::123456789012:identitystore/d-1234567890"
}
```

使用加密內容控制對客戶受管金鑰的存取

您也可以在金鑰政策和 IAM 政策中，使用加密內容來控制對對稱客戶受管金鑰的存取。中的某些金鑰政策範本[進階 KMS 金鑰政策陳述式](#)包含此類條件，以確保金鑰僅用於特定的 IAM Identity Center 執行個體。

監控 IAM Identity Center 的加密金鑰

當您搭配 IAM Identity Center 執行個體使用客戶受管 KMS 金鑰時，您可以使用 [AWS CloudTrail](#) 或 [Amazon CloudWatch Logs](#) 來追蹤 IAM Identity Center 傳送的請求 AWS KMS。IAM Identity Center 呼叫的 KMS API 操作會列在中 [步驟 2：準備 KMS 金鑰政策陳述式](#)。這些 API 操作的 CloudTrail 事件包含加密內容，可讓您監控 IAM Identity Center 執行個體呼叫的 AWS KMS API 操作，以存取客戶受管金鑰加密的資料。

AWS KMS API 操作的 CloudTrail 事件中的範例加密內容：

```
{
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "encryptionContext": {
      "aws:sso:instance-arn": "arn:aws:sso::instance/ssoins-xxxxxxxxxxxxxxxx",
      "tenant-key-id": "ssoins-xxxxxxxxxxxxxxxx"
    }
  }
}
```

AWS 受管應用程式的儲存、加密和刪除 IAM Identity Center 身分屬性

您部署的一些 AWS 受管應用程式 AWS IAM Identity Center，例如 AWS Systems Manager 和 Amazon CodeCatalyst，會將來自 IAM Identity Center 的特定使用者和群組屬性存放在自己的資料存放區中。在 IAM Identity Center 中使用客戶受管 KMS 金鑰進行靜態加密，不會延伸至存放在 AWS 受管應用程式中的 IAM Identity Center 使用者和群組屬性。AWS 受管應用程式對其存放的資料支援不同

的加密方法。最後，當您在 IAM Identity Center 中刪除使用者和群組屬性時，這些 AWS 受管應用程式可能會繼續將此資訊儲存在 IAM Identity Center 的刪除之後。請參閱 AWS 受管應用程式的使用者指南，了解存放在應用程式中資料的加密和安全性。

在中實作客戶受管 KMS 金鑰 AWS IAM Identity Center

客戶受管金鑰是您建立、擁有和管理的 AWS Key Management Service 金鑰。若要在 IAM Identity Center 中實作用於靜態加密的客戶受管 KMS AWS 金鑰，請遵循下列步驟：

Important

某些 AWS 受管應用程式無法搭配以客戶受管 KMS 金鑰設定的 AWS IAM Identity Center 使用。請參閱 [AWS 可與 IAM Identity Center 搭配使用的 受管應用程式](#)。

1. [步驟 1：識別組織的使用案例](#) - 若要定義使用 KMS 金鑰的正確許可，您需要識別整個組織的相關使用案例。KMS 金鑰許可由 KMS 金鑰政策陳述式和身分型政策組成，這些政策共同運作，以允許適當的 IAM 主體針對其特定使用案例使用 KMS 金鑰。
2. [步驟 2：準備 KMS 金鑰政策陳述式](#) - 根據步驟 1 中識別的使用案例選擇相關的 KMS 金鑰政策陳述式範本，並填寫所需的識別符和 IAM 主體名稱。從基準 KMS 金鑰政策陳述式開始，如果您的安全政策需要，請依照進階 KMS 金鑰政策陳述式所述來精簡它們。
3. [步驟 3：建立客戶受管 KMS 金鑰](#) - 在符合 IAM Identity Center 要求的 KMS 中建立 AWS KMS 金鑰，並將步驟 2 中準備的 KMS 金鑰政策陳述式新增至 KMS 金鑰政策。
4. [步驟 4：設定 KMS 金鑰跨帳戶使用的 IAM 政策](#) - 根據步驟 1 中識別的使用案例選擇相關的 IAM 政策陳述式範本，並填入金鑰 ARN 以準備使用。然後，允許每個特定使用案例的 IAM 主體跨帳戶使用 KMS 金鑰，方法是將備妥的 IAM 政策陳述式新增至主體的 IAM 政策。
5. [步驟 5：在 IAM Identity Center 中設定 KMS 金鑰](#) - 啟用 IAM Identity Center 執行個體中的客戶受管 KMS 金鑰，以將其用於靜態加密。

步驟 1：識別組織的使用案例

在建立和設定客戶受管 KMS 金鑰之前，請先識別您的使用案例，並準備必要的 KMS 金鑰許可。如需 [AWS KMS 金鑰政策的詳細資訊](#)，請參閱 [KMS 開發人員指南](#)。

呼叫 IAM Identity Center 服務 APIs IAM 主體需要許可。例如，委派管理員有權透過許可集政策使用這些 APIs。使用客戶受管金鑰設定 IAM Identity Center 時，IAM 主體也必須具有透過 IAM Identity

Center 服務 API 使用 KMS APIs 許可。您可以在兩個位置定義這些 KMS API 許可：KMS 金鑰政策和與 IAM 主體相關聯的 IAM 政策。

KMS 金鑰許可包含：

1. 您在 中建立 KMS 金鑰期間在 KMS 金鑰上指定的 KMS 金鑰政策陳述式 [步驟 3：建立客戶受管 KMS 金鑰](#)。
2. 在建立 KMS 金鑰 [步驟 4：設定 KMS 金鑰跨帳戶使用的 IAM 政策](#) 後，您在 中指定的 IAM 主體的 IAM 政策陳述式。

下表指定需要許可才能使用 KMS 金鑰的相關使用案例和 IAM 主體。

使用案例	需要許可才能使用 KMS 金鑰的 IAM 主體	必要/選用
使用 AWS IAM Identity Center	• IAM Identity Center AWS 的管理員 • IAM Identity Center 服務和相關聯的 Identity Store 服務	必要
搭配 IAM Identity Center 使用 AWS 受管應用程式	• AWS 受管應用程式的管理員 • AWS 受管應用程式 • AWS 受管應用程式擔任以呼叫 IAM Identity Center 服務 APIs 的服務 角色	選用
在已啟用的 AWS IAM Identity Center 執行個體 AWS Control Tower 上使用	• AWS Control Tower 管理員	選用
使用 IAM Identity Center 的 SSO 至 Amazon EC2 AWS 執行個體	• 獲授權執行 SSO 至 Amazon EC2 執行個體的 IAM 主體	選用
使用 IAM 主體呼叫 IAM Identity Center 服務 APIs 的任何其他使用案例，例如客戶受管應用程式、許可集、佈建工作流程或 AWS Lambda 函數	• 這些工作流程用來呼叫 IAM Identity Center 服務 APIs IAM 主體	選用

Note

資料表中列出的多個 IAM 主體需要 AWS KMS API 許可。不過，為了保護您的 IAM Identity Center 中的使用者和群組資料，只有 IAM Identity Center 和 Identity Store 服務會直接呼叫 AWS KMS API。

步驟 2：準備 KMS 金鑰政策陳述式

從開始，[基準 KMS 金鑰政策](#)並為您的組織自訂它。如果您需要根據您的安全需求更具體的政策，您可以使用中的範例修改政策陳述式[進階 KMS 金鑰政策陳述式](#)。如需此決策的指引，請參閱[選擇基準與進階 KMS 金鑰政策陳述式的考量事項](#)。

1. 將基準政策複製到編輯器，並在 KMS 金鑰政策陳述式中插入所需的識別符和 IAM 主體名稱。如需尋找參考識別符值的說明，請參閱[尋找所需識別符的位置](#)。
2. 如果您的安全需求需要它，請使用中的範例來精簡政策陳述式[進階 KMS 金鑰政策陳述式](#)。

Important

修改 IAM Identity Center 已使用之金鑰的 KMS 金鑰政策時請小心。雖然 IAM Identity Center 會在您最初設定 KMS 金鑰時驗證加密和解密許可，但無法驗證後續的政策變更。不小心移除必要的許可可能會中斷 IAM Identity Center 的正常操作。如需疑難排解 IAM Identity Center 中客戶受管金鑰相關常見錯誤的指引，請參閱[對中的客戶受管金鑰進行故障診斷 AWS IAM Identity Center](#)。

Note

IAM Identity Center 及其相關聯的 Identity Store 需要服務層級許可，才能使用您的客戶受管 KMS 金鑰。此需求延伸至使用服務憑證呼叫 IAM Identity Center 服務 APIs AWS 受管應用程式。對於使用[轉送存取工作階段](#)呼叫 IAM Identity Center 服務 APIs 的其他使用案例，只有啟動 IAM 主體（例如管理員）需要 KMS 金鑰許可。值得注意的是，使用 AWS 存取入口網站和 AWS 受管應用程式的最終使用者不需要直接 KMS 金鑰許可，因為它們是透過個別的服務授予。

步驟 3：建立客戶受管 KMS 金鑰

您可以使用 AWS 管理主控台或 KMS APIs 在 AWS 中建立客戶受管金鑰。建立金鑰時，請將您在步驟 2 中準備的 KMS 金鑰政策陳述式新增至 KMS 金鑰政策。如需詳細說明，包括預設 KMS 金鑰政策的指引，請參閱 [AWS Key Management Service 開發人員指南](#)。

金鑰必須符合下列要求：

- KMS 金鑰必須與 IAM Identity Center 執行個體位於相同的 AWS 區域
- 您可以選擇多區域或單一區域金鑰。不過，如果您打算在多個 AWS 區域中使用 IAM Identity Center，則必須建立多區域 KMS 金鑰。您無法將單一區域 KMS 金鑰轉換為多區域 KMS 金鑰，因此建議您從多區域 KMS 金鑰開始，除非您有使用單一區域 KMS 金鑰的特定需求。
- KMS 金鑰必須是針對「加密和解密」用量設定的對稱金鑰
- KMS 金鑰必須與 IAM Identity Center 的組織執行個體位於相同的 AWS Organizations 管理帳戶中

Note

如果您打算將此 KMS 金鑰複製到要複製 IAM Identity Center 的區域，建議您先完成本節中的設定，然後遵循 [the section called “將 IAM Identity Center 複製至其他區域”](#) 中的指引。

步驟 4：設定 KMS 金鑰跨帳戶使用的 IAM 政策

任何使用其他 AWS 帳戶 IAM Identity Center 服務 APIs 的 IAM 主體，例如 IAM Identity Center 委派管理員，也需要允許透過這些 APIs 使用 KMS 金鑰的 IAM 政策陳述式。

對於步驟 1 中識別的每個使用案例：

1. 在基準 KMS 金鑰和 IAM 政策陳述式中尋找相關的 IAM 政策陳述式範本。
2. 將範本複製到編輯器並填入金鑰 ARN，現在可在步驟 3 中建立 KMS 金鑰後使用。如需尋找金鑰 ARN 值的說明，請參閱 [尋找所需識別符的位置](#)。
3. 在 AWS 管理主控台，找到與使用案例相關聯的 IAM 主體的 IAM 政策。此政策的位置會根據使用案例和授予存取權的方式而有所不同。
 - 對於直接在 IAM 中授予的存取，您可以在 IAM 主控台中找到 IAM 主體，例如 IAM 角色。
 - 對於透過 IAM Identity Center 授予的存取，您可以在 IAM Identity Center 主控台中找到相關的許可集。
4. 將使用案例特定的 IAM 政策陳述式新增至 IAM 角色，並儲存變更。

 Note

此處所述的 IAM 政策是以身分為基礎的政策。雖然這類政策可以連接到 IAM 使用者、群組和角色，但我們建議您盡可能使用 IAM 角色。如需 IAM 角色與 IAM 使用者的詳細資訊，請參閱 IAM 使用者指南。

某些 AWS 受管應用程式中的其他組態

有些 AWS 受管應用程式會要求您設定服務角色，以允許應用程式使用 IAM Identity Center 服務 APIs。如果您的組織搭配 IAM Identity Center 使用 AWS 受管應用程式，請為每個部署的應用程式完成以下步驟：

1. 請參閱應用程式的使用者指南，確認是否已更新許可，以包含搭配 IAM Identity Center 使用應用程式的 KMS 金鑰相關許可。
2. 若是如此，請依照應用程式使用者指南的指示更新許可，以避免中斷應用程式的操作。

 Note

如果您不確定 AWS 受管應用程式是否使用這些許可，建議您檢查所有部署受 AWS 管應用程式的使用者指南。您只需要為每個需要組態的應用程式執行一次此組態。

步驟 5：在 IAM Identity Center 中設定 KMS 金鑰

 Important

繼續此步驟之前：

- 確認您的 AWS 受管應用程式與客戶受管 KMS 金鑰相容。如需相容應用程式的清單，請參閱[AWS 可與 IAM Identity Center 搭配使用的受管應用程式](#)。如果您有不相容的應用程式，請勿繼續。
- 設定使用 KMS 金鑰的必要許可。如果沒有適當的許可，此步驟可能會失敗或中斷 IAM Identity Center 管理、受 AWS 管應用程式的使用，以及其他需要 KMS 金鑰許可的使用案例。如需詳細資訊，請參閱[步驟 1：識別組織的使用案例](#)。
- 確保使用 IAM 角色呼叫 IAM Identity Center 服務 APIs 的 AWS 受管應用程式和客戶受管應用程式的許可，也允許透過 IAM Identity Center 服務 APIs 使用 KMS 金鑰。有些 AWS 受管

應用程式會要求您設定許可，例如 服務角色，以使用這些 APIs。請參閱每個已部署 AWS 受管應用程式的使用者指南，以確認是否需要新增特定的 KMS 金鑰許可。

在啟用 IAM Identity Center 的新組織執行個體時指定 KMS 金鑰

啟用 IAM Identity Center 的新組織執行個體時，您可以在設定期間指定客戶受管 KMS 金鑰。這可確保執行個體從一開始就使用您的金鑰進行靜態加密。開始之前，請參閱 [客戶受管 KMS 金鑰和進階 KMS 金鑰政策的考量](#)。

1. 在啟用 IAM Identity Center 頁面上，展開靜態加密區段。
2. 選擇 Manage Encryption (管理加密)。
3. 選擇客戶受管金鑰。
4. 對於 KMS 金鑰，請執行下列其中一項操作：
 - a. 從 KMS 金鑰中選擇選取，然後從下拉式清單中選取您建立的金鑰。
 - b. 選擇輸入 KMS 金鑰 ARN，然後輸入金鑰的完整 ARN。
5. 選擇儲存。
6. 選擇啟用以完成設定。

如需詳細資訊，請參閱[啟用 IAM Identity Center](#)。

變更 IAM Identity Center 現有組織執行個體的金鑰組態

您可以隨時將客戶受管 KMS 金鑰變更為另一個金鑰，或切換至擁有的 AWS 金鑰。

Console

若要變更 KMS 金鑰組態

1. 開啟位於 <https://console.aws.amazon.com/singlesignon/> 的 IAM Identity Center 主控台。
2. 在導覽窗格中，選擇設定。
3. 前往其他設定分頁。
4. 選擇管理加密。
5. 選擇下列其中一項：

- a. 客戶受管金鑰 - 從下拉式清單中選取不同的客戶受管金鑰，或輸入新的金鑰 ARN。
 - b. AWS 擁有的金鑰 - 切換到預設加密選項。
6. 選擇儲存。

AWS CLI

若要變更 IAM Identity Center 的現有組織執行個體，以使用 KMS 客戶受管金鑰

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration \  
    KeyType=CUSTOMER_MANAGED_KEY,KmsKeyArn=arn:aws:kms:us-  
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

若要將 IAM Identity Center 的現有組織執行個體變更為使用 AWS 擁有的金鑰

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration KeyType=AWS_OWNED_KMS_KEY
```

客戶受管金鑰考量

- 更新 IAM Identity Center 操作的 KMS 金鑰設定不會影響 IAM Identity Center 中的作用中使用者工作階段。在此過程中，您可以繼續使用 AWS 存取入口網站、IAM Identity Center 主控台和 IAM Identity Center APIs。
- 切換到新的 KMS 金鑰時，IAM Identity Center 會驗證是否可以成功地使用該金鑰進行加密和解密。如果您在設定金鑰政策或 IAM 政策時發生錯誤，主控台會顯示解釋性錯誤訊息，而先前的 KMS 金鑰將保持使用中。
- 預設的年度 KMS 金鑰輪換會自動發生。如需[金鑰輪換](#)、[監控 AWS KMS 金鑰](#)和[控制金鑰刪除存取](#)等主題的資訊，請參閱 [AWS KMS 開發人員指南](#)。

Important

如果 IAM Identity Center 執行個體使用的客戶受管 KMS 金鑰因 KMS 金鑰政策不正確而遭到刪除、停用或無法存取，您的人力資源使用者和 IAM Identity Center 管理員將無法使用 IAM

Identity Center。視情況而定，存取的遺失可以是暫時性（可以更正金鑰政策）或永久（無法還原已刪除的金鑰）。我們建議您[限制對關鍵操作的存取](#)，例如刪除或停用 KMS 金鑰。此外，我們建議您的組織設定[AWS 中斷玻璃存取程序](#)，以確保您的特權使用者在 AWS 無法存取 IAM Identity Center 時可以存取。

尋找所需識別符的位置

設定客戶受管 KMS 金鑰的許可時，您需要特定的 AWS 資源識別符才能完成金鑰政策和 IAM 政策陳述式範本。在 KMS 金鑰政策陳述式中插入所需的識別符（例如組織 ID）和 IAM 主體名稱。

以下是在 AWS 管理主控台中尋找這些識別符的指南。

IAM Identity Center Amazon Resource Name (ARN) 和 Identity Store ARN

IAM Identity Center 執行個體是一種 AWS 資源，具有自己的唯一 ARN，例如 `arn:aws:sso::instance/ssoinstances-1234567890abcdef`。ARN 遵循服務授權參考的 IAM Identity Center 資源類型區段中記錄的模式。

每個 IAM Identity Center 執行個體都有關聯的 Identity Store，可存放使用者和群組身分。Identity Store 具有稱為 Identity Store ID 的唯一識別符（例如，`d-123456789a`）。ARN 遵循[服務授權參考](#)的 Identity Store 資源類型區段中記錄的模式。

您可以在 IAM Identity Center 的設定頁面上找到 ARN 和 Identity Store ID 值。身分存放區 ID 位於身分來源索引標籤中。

AWS Organizations ID

如果您想要在金鑰政策中指定組織 ID（例如 `o-exampleorg1`），您可以在 IAM Identity Center 和 Organizations 主控台的設定頁面中找到其值。ARN 遵循服務授權參考中 Organizations 資源類型區段中記錄的模式。

KMS 金鑰 ARN

您可以在 AWS KMS 主控台中找到 KMS 金鑰的 ARN。選擇左側的客戶受管金鑰，按一下您要查詢其 ARN 的金鑰，您會在一般組態區段中看到該金鑰。ARN 遵循服務授權參考 AWS KMS 的資源類型區段中記錄的模式。

如需中金鑰政策 AWS KMS 與故障診斷 AWS KMS 許可的詳細資訊，請參閱 AWS Key Management Service 開發人員指南。如需 IAM 政策及其 JSON 表示法的詳細資訊，請參閱 IAM 使用者指南。

基準 KMS 金鑰政策

下列 KMS 金鑰政策涵蓋最常見的部署案例：具有委派管理員和 AWS 受管應用程式的 IAM Identity Center 執行個體 AWS Control Tower，包括 SSO 到 Amazon EC2 執行個體和自訂工作流程。建立 IAM Identity Center 的客戶受管 KMS 金鑰時，請使用此政策做為起點。如果您需要更精細的存取控制，例如將金鑰限制在特定 IAM Identity Center 執行個體或應用程式，請參閱 [進階 KMS 金鑰政策陳述式](#)。請注意，如果使用多區域金鑰，則應在所有複本中使用相同的政策，以協助確保一致的授權。

若要使用此政策，請將下列預留位置值取代為您自己的值：

- **111122223333** — IAM Identity Center 執行個體的帳戶 AWS ID (AWS Organizations 管理帳戶)。
- **444455556666** — 委派管理 AWS 帳戶的帳戶 ID。如果您不使用委派的管理，請移除此委託人。

由於 AWS IAM Identity Center 要求 KMS 金鑰與服務位於相同的 AWS 帳戶中，因此下列陳述式會使用 `${aws:ResourceOrgID}` 和 `${aws:ResourceAccount}` 變數，而非常值。如果您想要的話，您可以將這些變數取代為 AWS 組織 ID 和 AWS 帳戶 ID。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIdentityCenterAdminAccounts",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowIdentityCenterAndIdentityStoreToDescribeKey",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "identitystore.amazonaws.com",
          "sso.amazonaws.com"
        ]
      }
    }
  ]
}
```

```

    },
    "Action": "kms:DescribeKey",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "${aws:ResourceAccount}"
      }
    }
  },
  {
    "Sid": "AllowIdentityCenterAndIdentityStoreToUseKey",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "identitystore.amazonaws.com",
        "sso.amazonaws.com"
      ]
    },
    "Action": [
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "${aws:ResourceAccount}"
      },
      "ForAnyValue:StringEquals": {
        "kms:EncryptionContextKeys": [
          "aws:sso:instance-arn",
          "aws:identitystore:identitystore-arn"
        ]
      }
    }
  },
  {
    "Sid": "AllowOrgPrincipalsViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {

```

```

    "StringEquals": {
      "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
    },
    "StringLike": {
      "kms:ViaService": [
        "sso.*.amazonaws.com",
        "identitystore.*.amazonaws.com"
      ]
    },
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": [
        "aws:sso:instance-arn",
        "aws:identitystore:identitystore-arn"
      ]
    }
  },
  {
    "Sid": "AllowManagedApps",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "${aws:ResourceOrgID}"
      },
      "StringLike": {
        "kms:ViaService": [
          "identitystore.*.amazonaws.com",
          "sso.*.amazonaws.com"
        ]
      },
      "ForAnyValue:StringEquals": {
        "kms:EncryptionContextKeys": [
          "aws:sso:instance-arn",
          "aws:identitystore:identitystore-arn"
        ]
      }
    }
  }
}

```

```
]
}
```

此政策包含五個陳述式。下表說明每個陳述式的功能。

陳述式	用途
<code>AllowIdentityCenterAdminAccounts</code>	將完整的 KMS 金鑰許可授予 IAM Identity Center 管理帳戶和委派的管理帳戶。這包括金鑰管理動作，例如修改金鑰政策和排程金鑰刪除。如果這些帳戶中的管理員在其身分型政策中具有必要的許可，則可以管理和使用金鑰。
<code>AllowIdentityCenterAndIdentityStoreToDescribeKey</code>	允許 IAM Identity Center 和 Identity Store 服務主體擷取金鑰中繼資料。這對於在不執行加密或解密的情況下驗證金鑰的服務操作是必要的。 <code>aws:SourceAccount</code> 條件有助於確保只有 IAM Identity Center 執行個體可以使用 KMS 金鑰。
<code>AllowIdentityCenterAndIdentityStoreToUseKey</code>	允許 IAM Identity Center 和 Identity Store 服務主體使用金鑰進行加密操作，例如加密、解密和重新加密資料。 <code>aws:SourceAccount</code> 條件有助於確保只有 IAM Identity Center 執行個體可以使用 KMS 金鑰。
<code>AllowOrgPrincipalsViaIdentityCenterAndIdentityStore</code>	允許 AWS 組織中的 IAM 主體透過 IAM Identity Center 和 Identity Store 服務解密資料。這涵蓋使用轉送存取工作階段 (FAS) 與 IAM Identity Center 整合 AWS 服務互動的應用程式管理員。
<code>AllowManagedApps</code>	允許 AWS 受管應用程式透過 IAM Identity Center 和 Identity Store 解密受 KMS 金鑰保護的資料。

在 中使用下列 IAM 政策陳述式 [步驟 4：設定 KMS 金鑰跨帳戶使用的 IAM 政策](#)，以允許委派管理員透過 IAM Identity Center 服務 APIs 使用 KMS 金鑰。將範例金鑰 ARN 取代為您實際的 KMS 金鑰 ARN。範例中的萬用字元區域可容納多區域 KMS 金鑰的所有複本。

對於 IAM Identity Center 管理以外的跨帳戶使用案例，例如 SSO 到 Amazon EC2 執行個體或 AWS 受管應用程式的管理，範圍 `AllowCrossAccountKMSKeyUse` 僅限於 `kms:Decrypt` 並移除 `AllowListKMSKeyAliases` 陳述式。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountKMSKeyUse",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:*:111122223333:key/mrk-1234abcd-12ab-34cd-56ef-1234567890ab"
      ]
    },
    {
      "Sid": "AllowListKMSKeyAliases",
      "Effect": "Allow",
      "Action": "kms:ListAliases",
      "Resource": "*"
    }
  ]
}
```

進階 KMS 金鑰政策陳述式

使用進階 KMS 金鑰政策陳述式，為您的客戶受管 KMS 金鑰實作更精細的存取控制。透過新增加密內容條件和服務特定限制[基準 KMS 金鑰政策](#)，這些政策以 為基礎。決定是否使用進階 KMS 金鑰政策陳述式之前，請務必檢閱相關考量事項。

使用加密內容來限制存取

您可以將加密內容條件新增至 中的 AllowOrgPrincipalsViaIdentityCenterAndIdentityStore 和 AllowManagedApps 陳述式，將 KMS 金鑰用量限制為特定 IAM Identity Center 執行個體 [基準 KMS 金鑰政策](#)。使用特定 Identity Center 執行個體 ARN 和 Identity Store ARN 新增下列條件。您也可以將相同的加密內容條件新增至設定為跨帳戶使用 KMS 金鑰的 IAM 政策。

Identity Center

```
"StringEquals": {
  "kms:EncryptionContext:aws:sso:instance-arn":
  "arn:aws:sso:::instance/ssoins-1234567890abcdef"
}
```

身分存放區

```
"StringEquals": {
  "kms:EncryptionContext:aws:identitystore:identitystore-arn":
  "arn:aws:identitystore:::111122223333:identitystore/d-1234567890"
}
```

如果您需要尋找這些識別符的說明，請參閱 [尋找所需識別符的位置](#)。

Note

您只能將客戶受管 KMS 金鑰與 IAM Identity Center 的組織執行個體搭配使用。客戶受管金鑰必須位於 AWS 組織的管理帳戶中，這有助於確保金鑰與單一 IAM Identity Center 執行個體搭配使用。不過，加密內容機制提供單一執行個體使用的獨立技術保護措施。您也可以適用於 Identity Center 和 Identity Store 服務主體的 KMS 金鑰政策陳述式中使用 `aws:SourceArn` 條件金鑰。

實作加密內容條件的考量

在實作加密內容條件之前，請檢閱下列要求：

- **DescribeKey 動作。**加密內容無法套用至「`kms:DescribeKey`」動作，IAM Identity Center 管理員可以使用。設定 KMS 金鑰政策時，請排除此特定動作的加密內容，以確保 IAM Identity Center 執行個體能正常運作。
- **新的執行個體設定。**如果您要使用客戶受管 KMS 金鑰啟用新的 IAM Identity Center 執行個體，請參閱 [客戶受管 KMS 金鑰和進階 KMS 金鑰政策的考量](#)。
- **身分來源變更。**將您的身分來源變更為 Active Directory 或從 Active Directory 變更時，加密內容需要特別注意。請參閱 [變更身分來源的考量事項](#)。

政策範本

根據您的安全需求，從這些進階政策範本中進行選擇。平衡精細存取控制及其帶來的管理開銷。

此處涵蓋的主題：

- [特定 IAM Identity Center 執行個體的唯讀使用的 KMS 政策陳述式](#)。本節示範使用加密內容進行 IAM Identity Center 的唯讀存取。
- [精簡 KMS 金鑰政策陳述式以使用 AWS 受管應用程式](#)。本節示範如何使用加密內容和應用程式資訊來精簡 AWS 受管應用程式的 KMS 金鑰政策，例如應用程式服務主體、應用程式 ARN 和 AWS 帳戶 ID。

特定 IAM Identity Center 執行個體的唯讀使用的 KMS 政策陳述式

此政策允許[安全稽核人員](#)和其他只需要讀取 IAM Identity Center 存取權的人員使用 KMS 金鑰。

若要使用此政策：

1. 將範例唯讀管理員 IAM 主體取代為您的實際管理員 IAM 主體
2. 將範例 IAM Identity Center 執行個體 ARN 取代為您的實際執行個體 ARN
3. 將範例 Identity Store ARN 取代為您實際的 Identity Store ARN
4. 如果使用[委派的管理](#)，請參閱 [步驟 4：設定 KMS 金鑰跨帳戶使用的 IAM 政策](#)

如果您需要協助尋找這些識別符的值，請參閱 [尋找所需識別符的位置](#)。

使用值更新範本後，請視需要返回 [步驟 2：準備 KMS 金鑰政策陳述式](#)以準備其他 KMS 金鑰政策陳述式。

kms:Decrypt 動作本身不會限制對唯讀操作的存取。IAM 政策必須在 IAM Identity Center 服務 APIs 上強制執行唯讀存取。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToIdentityCenterAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
```



```

        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn":
"arn:aws:sso:::instance/ssoins-1234567890abcdef"
    },
    {
        "Sid": "AllowReadOnlyAccessToIdentityStoreAPI",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
        },
        "Action": "kms:Decrypt",
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "identitystore.*.amazonaws.com",
                "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
            }
        }
    }
]
}

```

精簡 KMS 金鑰政策陳述式以使用 AWS 受管應用程式

這些政策範本可讓您更精細地控制哪些 AWS 受管應用程式可以使用您的 KMS 金鑰。

Note

某些 AWS 受管應用程式無法搭配以客戶受管 KMS 金鑰設定的 IAM Identity Center 使用。請參閱[AWS 可與 IAM Identity Center 搭配使用的受管應用程式](#)。

基準 KMS 金鑰政策 允許來自相同 AWS 組織中任何帳戶的 AWS 受管應用程式使用 KMS 金鑰。使用這些精簡政策來限制存取：

- 應用程式服務主體
- 應用程式執行個體 ARNs
- AWS 帳戶 IDs

- 特定 IAM Identity Center 執行個體的加密內容

 Note

服務主體是 AWS 服務的唯一識別符，通常格式為 `servicename.amazonaws.com`（例如 Amazon EMR 的 `elasticmapreduce.amazonaws.com`）。

依帳戶限制

此 KMS 金鑰政策陳述式範本允許特定 AWS 帳戶中的 AWS 受管應用程式使用特定 IAM Identity Center 執行個體來使用 KMS 金鑰。

若要使用此政策：

1. 將範例服務主體取代為您實際的應用程式服務主體
2. 將範例帳戶 IDs 取代為部署受 AWS 管應用程式的實際帳戶 IDs
3. 將範例 Identity Store ARN 取代為您實際的 Identity Store ARN
4. 將範例 IAM Identity Center 執行個體 ARN 取代為您的實際執行個體 ARN

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "111122223333",
            "444455556666"
          ]
        },
        "StringLike": {
```

```

        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
    },
    "Bool": {
        "aws:PrincipalIsAWSService": "true"
    }
},
{
    "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
        "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": [
                "111122223333",
                "444455556666"
            ]
        },
        "StringLike": {
            "kms:ViaService": "identitystore.*.amazonaws.com",
            "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore:::111122223333:identitystore/d-1234567890"
        },
        "Bool": {
            "aws:PrincipalIsAWSService": "true"
        }
    }
}
]
}

```

依應用程式執行個體限制

此 KMS 金鑰政策陳述式範本允許特定 AWS 受管應用程式執行個體使用特定 IAM Identity Center 執行個體來使用 KMS 金鑰。

若要用此政策：

1. 將範例服務主體取代為您實際的應用程式服務主體
2. 將範例應用程式 ARN 取代為您實際的應用程式執行個體 ARN
3. 將範例 Identity Store ARN 取代為您實際的 Identity Store ARN
4. 將範例 IAM Identity Center 執行個體 ARN 取代為您的實際執行個體 ARN

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-application"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/ssoinstances-1234567890abcdef"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    },
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```

        "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
    },
    "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "Bool": {
        "aws:PrincipalIsAWSService": "true"
    }
}
]
}

```

客戶受管 KMS 金鑰和進階 KMS 金鑰政策的考量

使用 IAM Identity Center 實作客戶受管 KMS 金鑰時，請考慮這些會影響加密組態設定、安全性和持續維護的因素。

選擇基準與進階 KMS 金鑰政策陳述式的考量事項

決定是否使用 讓 KMS 金鑰許可更具體時[進階 KMS 金鑰政策陳述式](#)，請考慮管理開銷以及您組織的安全需求。更具體的政策陳述式可更精細地控制誰可以使用金鑰以及用於什麼目的；不過，隨著 IAM Identity Center 組態的演進，它們需要持續維護。例如，如果您將 KMS 金鑰的使用限制為特定 AWS 受管應用程式部署，則每當組織想要部署或取消部署應用程式時，都需要更新金鑰政策。限制性較低的政策可減少管理負擔，但可能會授予比安全需求所需的更廣泛許可。

使用客戶受管 KMS 金鑰啟用新 IAM Identity Center 執行個體的考量

如果您使用 中所述的加密內容[進階 KMS 金鑰政策陳述式](#)，將 KMS 金鑰的使用限制在特定 IAM Identity Center 執行個體，則適用此處的考量。

使用客戶受管 KMS 金鑰啟用新的 IAM Identity Center 執行個體時，IAM Identity Center 和 Identity Store ARNs 會在設定完成後才能使用。您有下列選項：

- 暫時使用一般 ARN 模式，然後在執行個體啟用後以完整 ARNs 取代。請記得視需要在 StringEquals 和 StringLike 運算子之間切換。
 - 對於 IAM Identity Center SPN："arn : \${Partition} : sso : : instance/*"。
 - 對於 Identity Store SPN："arn : \${Partition} : identitystore : : \${Account} : identitystore/*"。

- 在 ARN 中暫時使用「purpose : KEY_CONFIGURATION」。這僅適用於執行個體啟用，且必須以實際 ARN 取代，IAM Identity Center 執行個體才能正常運作。此方法的優點是，在執行個體啟用後，您不會忘記取代此選項。
- 對於 IAM Identity Center SPN，請使用："arn : \${Partition} : sso : : instance/purpose : KEY_CONFIGURATION"
- 對於 Identity Store SPN，請使用："arn : \${Partition} : identitystore : : \${Account} : identitystore/purpose : KEY_CONFIGURATION"

 Important

請勿將此組態套用至已在現有 IAM Identity Center 執行個體中使用的 KMS 金鑰，因為這可能會中斷其正常操作。

- 從 KMS 金鑰政策省略加密內容條件，直到啟用執行個體為止。

標記 AWS IAM Identity Center 資源

標籤是您新增至 AWS 資源的自訂屬性標籤，可讓您更輕鬆地識別、組織和搜尋資源。每個 標籤都有兩個部分：

- 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定為空字串，但無法將標籤的值設定為 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組織 AWS 資源。許多 AWS 服務支援標記，因此您可以將相同的標籤指派給來自不同服務的資源，以指出資源相關。例如，您可以將相同的標籤指派給 IAM Identity Center 執行個體中的特定許可集。如需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，以協助控制誰可以檢視資源並與之互動。若要進一步了解如何使用標籤來控制存取，請參閱《IAM 使用者指南》中的[使用標籤控制對 AWS 資源的存取](#)。例如，您可以允許使用者更新 IAM Identity Center 許可集，但前提是 IAM Identity Center 許可集具有值為該使用者名稱的owner標籤。

您只能將標籤套用至許可集。您無法將標籤套用至 IAM Identity Center 建立的對應角色 AWS 帳戶。您可以使用 IAM Identity Center 主控台 AWS CLI 或 IAM Identity Center APIs 來新增、編輯或刪除許可集的標籤。

下列各節提供有關 IAM Identity Center 標籤的詳細資訊。

主題

- [標籤限制](#)
- [使用 IAM Identity Center 主控台管理標籤](#)
- [AWS CLI 範例](#)
- [使用 IAM Identity Center API 管理標籤](#)

標籤限制

下列基本限制適用於 IAM Identity Center 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。
- 標籤索引鍵和值的有效字元為：
a-z、A-Z、0-9、空格和下列字元：_ . : / = + - 和 @
- 索引鍵和值會區分大小寫。
- 不要使用 aws: 做為金鑰的字首；它保留供 AWS 使用

使用 IAM Identity Center 主控台管理標籤

您可以使用 IAM Identity Center 主控台來新增、編輯和移除與執行個體或許可集相關聯的標籤。

管理 IAM Identity Center 主控台的許可集標籤

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇許可集。
3. 選擇具有您要管理之標籤的許可集名稱。
4. 在許可索引標籤的標籤下，執行下列其中一項操作，然後繼續下一個步驟：
 - a. 如果已為此許可集指派標籤，請選擇編輯標籤。
 - b. 如果未將標籤指派給此許可集，請選擇新增標籤。
5. 對於每個新標籤，在索引鍵和值（選用）欄中輸入值。完成時，請選擇 Save changes (儲存變更)。

若要移除標籤，請在您要移除的標籤旁的移除欄中選擇 X。

管理 IAM Identity Center 執行個體的標籤

1. 開啟 [IAM Identity Center 主控台](#)。
2. 選擇設定。
3. 選擇 Tags (標籤) 索引標籤。
4. 對於每個標籤，在金鑰和值（選用）欄位中輸入值。完成後，請選擇新增標籤按鈕。

若要移除標籤，請選擇您要移除之標籤旁的移除按鈕。

AWS CLI 範例

AWS CLI 提供的命令可讓您用來管理指派給許可集的標籤。

指派標籤

使用下列命令將標籤指派給您的許可集。

Example **tag-resource** 許可集的命令

在一組命令[tag-resource](#)中使用，將標籤指派給許可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** – 執行操作的 IAM Identity Center 執行個體的 Amazon Resource Name (ARN)。
- **resource-arn** – 資源的 ARN，其中包含要列出的標籤。
- **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您已指派給許可集的標籤。

Example **list-tags-for-resource** 許可集的命令

在sso一組命令[list-tags-for-resource](#)中使用 檢視指派給許可集的標籤：

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

移除標籤

使用下列命令從許可集中移除標籤。

Example **untag-resource** 許可集的命令

在sso一組命令[untag-resource](#)中使用 從許可集中移除標籤：

```
$ 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。

建立許可集時套用標籤

使用以下命令，在您建立許可集時指派標籤。

Example 搭配標籤的 `create-permission-set` 命令

當您使用 [create-permission-set](#) 命令建立許可集時，您可以使用 `--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 Identity Center API 管理標籤

使用下列 API 動作來指派、檢視和移除 IAM Identity Center 許可集或執行個體的標籤。

- [TagResource](#)
- [ListTagsForResource](#)
- [UntagResource](#)
- [CreatePermissionSet](#)
- [CreateInstance](#)

將 AWS CLI 與 IAM Identity Center 整合

AWS 命令列界面 (CLI) 第 2 版與 IAM Identity Center 整合可簡化登入程序。開發人員可以使用他們通常用來登入 IAM Identity Center AWS CLI 的相同 Active Directory 或 IAM Identity Center 登入資料直接登入，並存取其指派的帳戶和角色。例如，在管理員設定 IAM Identity Center 使用 Active Directory 進行身分驗證之後，開發人員可以使用其 Active Directory 登入資料 AWS CLI 直接登入。

AWS CLI 與 IAM Identity Center 整合可提供下列優點：

- 企業可以使用 將 IAM Identity Center 連線至其 Active Directory，讓開發人員使用 IAM Identity Center 或 Active Directory 的憑證登入 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他們已指派存取權的帳戶和角色之間切換。
- 開發人員可以在其 CLI 組態中自動產生並儲存具名角色描述檔，並在 CLI 中參考這些描述檔，以在所需的帳戶和角色中執行命令。
- CLI 會自動管理短期登入資料，讓開發人員可以安全地在 CLI 中啟動和保留，而不會中斷，並執行長時間執行的指令碼。

如何將 AWS CLI 與 IAM Identity Center 整合

若要使用 CLI AWS 與 IAM Identity Center 整合，請下載、安裝和設定第 2 AWS Command Line Interface 版。如需如何下載 並將其 AWS CLI 與 IAM Identity Center 整合的詳細步驟，請參閱AWS Command Line Interface 《使用者指南》中的[設定 AWS CLI 以使用 IAM Identity Center](#)。

AWS 管理主控台 私有存取的考量事項

如果您的組織使用 AWS 管理主控台 私有存取功能，您應該考慮您的使用者將如何登入 IAM Identity Center。

VPC 端點政策會將登入限制在 管理主控台，以防止您的使用者登入 AWS 帳戶 他們無權存取。如需詳細資訊，請參閱AWS 管理主控台 《入門指南》中的[AWS 管理主控台 私有存取](#)。

VPC 端點區塊登入 IAM Identity Center

請務必注意，使用 VPC 端點會封鎖 IAM Identity Center 的登入。當使用者已透過 VPC 端點登入管理主控台時，就會發生這種情況。為了確保您的使用者可以繼續登入 IAM Identity Center，他們必須使用公有端點 AWS 登入，而不是 VPC 端點。

IAM Identity Center 中的配額和限制

下表說明 IAM Identity Center 中的配額。配額增加請求必須來自管理或委派的管理員帳戶。若要增加配額，請參閱[請求增加配額](#)。

Note

如果您有超過 50,000 個使用者、10,000 個群組或 500 個許可集，建議使用 AWS CLI 和 APIs 來管理 IAM Identity Center。如需 CLI 的詳細資訊，請參閱 [將 AWS CLI 與 IAM Identity Center 整合](#)。如需 APIs 的詳細資訊，請參閱 [歡迎使用 IAM Identity Center API 參考](#)。

應用程式配額

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 聲明限制	50,000 個字元	否
上傳至 IAM Identity Center 之 IdP 憑證的檔案大小限制	2500 (UTF-8) 個字元	否
每個應用程式的存取範圍	25	否

AWS 帳戶 配額

資源	預設配額	可以提高
IAM Identity Center 中允許的許可集數量	3500	是
每個 允許的佈建許可集數目 AWS 帳戶	500	是

資源	預設配額	可以提高
每個許可集的內嵌政策數量	1	否
每個許可集的 AWS 受管和客戶受管政策數量	25 ¹	否
每個許可集的內嵌政策大小上限	32,768 個位元組。 每個許可集內嵌政策中的非空格字元大小上限為 10,240 個位元組。	否
中一次可更新的 IAM AWS 帳戶角色（許可集）數量	1	否

¹AWS 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 AWS 帳戶 您要部署許可集的每個 請求增加連接到 Service Quotas 主控台中 IAM 角色的 IAM 配額受管政策。

Note

[AWS 帳戶 使用許可集管理](#) 在中佈建 AWS 帳戶 為 IAM 角色，或在 中使用現有的 IAM 角色 AWS 帳戶，因此遵循 IAM 配額。如需與 IAM 角色相關聯的配額詳細資訊，請參閱 [IAM 和 STS 配額](#)。

Active Directory 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 Identity Center 身分存放區配額

資源	預設配額	可以提高
IAM Identity Center 支援的使用者數量	200000	是
IAM Identity Center 支援的群組數量	100000	是
可用來評估使用者許可的唯一群組數量	1000	否

IAM Identity Center 調節限制

資源	預設配額
IAM Identity Center APIs	IAM Identity Center APIs 的集體限流限制為每秒 20 筆交易 (TPS)。對於讀取 APIs，您可以開啟支援案例來請求提高限制。 CreateAccountAssignment 寫入 API 有 15 個未完成的非同步呼叫的限制。此限制無法提高。
Identity Store APIs	Identity Store APIs 的調節限制為每個 API 每秒 20 筆交易 (TPS)。此限制適用於每個 Identity Store 執行個體。您可以開啟支援案例來請求提高限制。
SCIM APIs	SCIM APIs 的寫入 API 每個 API 限流限制為每秒 25 筆交易 (TPS)APIs 則為 40 TPS APIs。這些限制適用於每個 Identity Store 執行個體。您可以開啟支援案例來請求提高限制。 CreateGroup 或 PatchGroup 呼叫中的每個個別成員資格操作都會計入每個 Identity Store 個別成員資格操作調節限制的交易。

如果您的 IAM Identity Center 執行個體在多個 中啟用 AWS 區域，調節限制同樣適用於每個啟用的區域。例如，每個啟用區域中的 Identity Store APIs 會有 20 TPS 限流限制。如需其他區域可使用哪些 API 操作的詳細資訊，請參閱對應的[資料表](#)。

OIDC 服務請求配額

資源	預設值 (每秒請求數)	可以提高
從遠端地址請求註冊公有 OAuth 用戶端的速率 適用於： RegisterClient	20	是
向向 OIDC 服務註冊的公有用戶端請求速率 適用於： CreateToken 、 StartDeviceAuthorization	80	是
向使用相同 IAM Identity Center 執行個體註冊的所有公有用戶端請求速率 適用於： CreateToken	250	是
使用字符交換和重新整理字符授予向 IAM Identity Center 執行個體註冊的 IAM Identity Center 應用程式請求率。 適用於： CreateTokenWithIAM	80	是
來自使用 JWT Bearer 授予的相同 IAM Identity Center 執行個體註冊之所有 IAM Identity Center 應用程式的字符產生率 適用於： CreateTokenWithIAM	10	聯絡 AWS 支援

如果您的 IAM Identity Center 執行個體在多個 中啟用 AWS 區域，上述請求率同樣適用於每個啟用的區域。例如，如果您允許從遠端地址註冊公有 OAuth 用戶端的請求率為每秒 20 個請求，則每個啟用的區域都可以使用此輸送量。如需其他區域可使用哪些 API 操作的詳細資訊，請參閱對應的[資料表](#)。

其他配額

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 Identity Center 執行個體總數	1	否
受信任字符發行者總數	10	否
可指派給每個 AWS 帳戶或應用程式之許可集的群組總數	100	否
單一 IAM Identity Center 執行個體 AWS 區域 啟用的總數	3	是

* 例如，您可以設定 2750 個帳戶和 250 個應用程式，總共產生 3000 個帳戶和應用程式。

** API [ProvisionPermissionSet](#) 操作可以使用 選項佈建許可集 ALL_PROVISIONED_ACCOUNTS，最多 3500 個 AWS 帳戶。如果您需要將許可設定為 3500 以上 AWS 帳戶，您可以使用 ProvisionPermissionSet API 操作搭配 AWS_ACCOUNT 選項，該選項會在單一 中佈建許可集 AWS 帳戶。您最多可以對 進行三次並行呼叫 ProvisionPermissionSet。

對 IAM Identity Center 問題進行故障診斷

以下可協助您疑難排解在設定或使用 IAM Identity Center 主控台時可能遇到的一些常見問題。

建立 IAM Identity Center 帳戶執行個體的問題

建立 IAM Identity Center 的帳戶執行個體時，可能會有幾項限制。如果您無法透過 IAM Identity Center 主控台或受支援 AWS 受管應用程式的設定體驗建立帳戶執行個體，請驗證下列使用案例：

- 檢查您嘗試在 AWS 帳戶 其中建立帳戶執行個體的 AWS 區域 中的其他 。每個執行個體僅限一個 IAM Identity Center 執行個體 AWS 帳戶。若要啟用應用程式，請使用 IAM Identity Center AWS 區域 執行個體切換到 ，或切換到沒有 IAM Identity Center 執行個體的帳戶。
- 如果您的組織在 2023 年 9 月 14 日之前啟用 IAM Identity Center，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，從管理帳戶中的 IAM Identity Center 主控台啟用帳戶執行個體建立。
- 您的管理員可能已建立服務控制政策，以限制建立 IAM Identity Center 的帳戶執行個體。與您的管理員合作，將您的帳戶新增至允許清單。

當您嘗試檢視已預先設定為與 IAM Identity Center 搭配使用的雲端應用程式清單時，會收到錯誤

當您的政策允許 `sso:ListApplications` 但不允許其他 IAM Identity Center APIs 時，會發生以下錯誤。更新您的政策以解決此錯誤。

`ListApplications` 許可會授權多個 APIs：

- `ListApplications` API。
- 與 IAM Identity Center 主控台中使用的 API 類似的內部 `ListApplicationProviders` API。

為了協助解決重複問題，內部 API 現在也會授權使用 `ListApplicationProviders` 動作。若要允許公有 `ListApplications` 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": "sso:ListApplicationProviders",
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": "sso:ListApplications",
  "Resource": "<instanceArn>" // (or "*" for all instances)
}
]
```

若要允許內部 API 但拒絕 ListApplications，政策只需要允許 ListApplicationProviders。如果未明確允許，則會拒絕 ListApplications API。

```
"Statement": [
{
  "Effect": "Allow",
  "Action": "sso:ListApplicationProviders",
  "Resource": "*"
}
]
```

當您的政策更新時，請聯絡 支援 以移除此主動措施。

IAM Identity Center 建立的 SAML 聲明內容相關問題

從存取 AWS 入口網站存取 AWS 帳戶 和 SAML 應用程式時，IAM Identity Center 為 IAM Identity Center 建立和傳送的 SAML 聲明提供以 Web 為基礎的偵錯體驗，包括這些聲明中的屬性。若要查看 IAM Identity Center 產生的 SAML 聲明的詳細資訊，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，請按住 Shift 鍵，選擇應用程式圖磚，然後釋放 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日後參考，請選擇複製 XML，然後將內容貼到其他位置。
4. 選擇傳送至 <application> 以繼續。此選項會將聲明傳送給服務提供者。

 Note

有些瀏覽器組態和作業系統可能不支援此程序。此程序已在 Windows 10 上使用 Firefox、Chrome 和 Edge 瀏覽器進行測試。

特定使用者無法從外部 SCIM 供應商同步到 IAM Identity Center

如果您的身分提供者 (IdP) 設定為使用 SCIM 同步將使用者佈建至 IAM Identity Center，您可能會在使用者佈建程序期間遇到同步失敗。這可能表示 IdP 中的使用者組態與 IAM Identity Center 要求不相容。發生這種情況時，IAM Identity Center SCIM APIs 會傳回錯誤訊息，提供問題的根本原因洞察。您可以在 IdP 的日誌或 UI 中找到這些錯誤訊息。或者，您可以在[AWS CloudTrail 日誌](#)中找到有關佈建失敗的詳細資訊。

如需 IAM Identity Center SCIM 實作的詳細資訊，包括必要、選用和不支援的使用者物件參數和操作的規格，請參閱 [SCIM 開發人員指南中的 IAM Identity Center SCIM 實作](#)開發人員指南

以下是此錯誤的一些常見原因：

1. IdP 中的使用者物件缺少第一個（名字）名稱、最後一個（家庭）名稱和/或顯示名稱。

錯誤訊息：「偵測到 2 個驗證錯誤：'*name.givenName*' 的值無法滿足限制條件：成員必須滿足規則表達式模式：【`\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r`】 + ；'*name.givenName*' 的值無法滿足限制條件：成員的長度必須大於或等於 1"

- 解決方案：新增使用者物件的第一個（名字）、最後一個（家庭）和顯示名稱。此外，請確定 IdP 中使用者物件的 SCIM 佈建映射已設定為傳送所有這些屬性的非空值。

2. 正在為使用者傳送多個單一屬性的值（也稱為「多值屬性」）。例如，使用者可能同時擁有 IdP 中指定的工作和住家電話號碼，或多個電子郵件或實體地址，而您的 IdP 設定為嘗試同步該屬性的多個或所有值。

錯誤訊息：「列出屬性####超過允許的 1 限制」

- 解決方案選項：
 - i. 更新 IdP 中使用者物件的 SCIM 佈建映射，以僅傳送指定屬性的單一值。例如，設定僅傳送每個使用者工作電話號碼的映射。
 - ii. 如果可以安全地從 IdP 的使用者物件中移除其他屬性，您可以移除其他值，為該使用者設定該屬性的一或零值。

- iii. 如果 中的任何動作不需要 屬性 AWS，請從 IdP 中使用者物件的 SCIM 佈建映射中移除該屬性的映射。
3. 您的 IdP 正在嘗試根據多個屬性來比對目標 (IAM Identity Center，在此案例中為) 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，因此您只需將 指定username為用於比對的屬性。
- 解決方案：確保 IdP 中的 SCIM 組態僅使用單一屬性與 IAM Identity Center 中的使用者進行比對。例如，將 IdP userPrincipalName中的 username或 映射至 SCIM 中的 userName 屬性，以佈建至 IAM Identity Center 將是正確且足以進行大多數實作。

使用外部身分提供者佈建使用者或群組時發生重複的使用者或群組錯誤

如果您在外部身分提供者 (IdP) 中佈建使用者或群組時遇到 IAM Identity Center 同步問題，可能是因為您的外部 IdP 使用者或群組沒有唯一的屬性值。您可能會在外部 IdP 中收到下列錯誤訊息：

拒絕建立新的重複資源

在下列案例中，您可能會遇到此問題：

- 案例 1
 - 您正在外部 IdP 中使用自訂的非唯一屬性，以取得在 IAM Identity Center 中必須是唯一的屬性。現有的 IAM Identity Center 使用者或群組無法同步到您的 IdP。
- 案例 2
 - 您嘗試建立具有重複屬性的使用者，這些屬性在 IAM Identity Center 中必須是唯一的。
 - 例如，您建立或擁有具有下列屬性的現有 IAM Identity Center 使用者：
 - 使用者名稱：Jane Doe
 - 主要電子郵件地址：jane_doe@example.com
 - 然後，您嘗試在外部 IdP 中建立具有下列屬性的另一個使用者：
 - 使用者名稱：Richard Doe
 - 主要電子郵件地址：jane_doe@example.com
 - 外部 IdP 會嘗試同步並在 IAM Identity Center 中建立使用者。不過，這些動作會失敗，因為兩個使用者的主要電子郵件地址都有重複值，且必須是唯一的。

使用者名稱、主要電子郵件地址和 externalID 必須是唯一的，您的外部 IdP 使用者才能成功同步到 IAM Identity Center。同樣地，群組名稱必須是唯一的，外部 IdP 群組才能成功同步到 IAM Identity Center。

解決方案是檢閱您的身分來源的屬性，並確保它們是唯一的。

當使用者的使用者名為 UPN 格式時，使用者無法登入

使用者可能無法根據登入頁面上用來輸入使用者名稱的格式登入 AWS 存取入口網站。在大部分情況下，使用者可以使用其純使用者名稱、下層登入名稱 (DOMAIN\UserName) 或其 UPN 登入名稱 () 來登入使用者入口網站 `UserName@Corp.Example.com`。IAM Identity Center 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開啟時，就會發生這種情況。在此案例中，使用者必須使用其下層登入名稱 (DOMAIN\UserName) 登入。如需詳細資訊，請參閱[MFA for Identity Center 目錄使用者](#)。如需用於登入 Active Directory 之使用者名稱格式的一般資訊，請參閱 Microsoft 文件網站上的[使用者名稱格式](#)。

我在修改 IAM 角色時收到「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 Identity Center 服務在帳戶中建立的角色，它們來自將許可集指派給帳戶。嘗試從 IAM 主控台修改這些角色將導致下列錯誤：

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' - this role is only modifiable by AWS'
```

這些角色只能從位於管理帳戶中的 IAM Identity Center 管理員主控台修改 AWS Organizations。修改後，您可以將變更向下推送至 AWS 其指派的帳戶。

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時？登入 AWS 存取入口網站時的選項，其新密碼必須遵循預設密碼政策，如中所述在[IAM Identity Center 中管理身分時的密碼需求](#)。

如果使用者輸入遵循政策的密碼，然後收到錯誤 `We couldn't update your password`，請檢查是否 AWS CloudTrail 記錄失敗。這可以透過使用下列篩選條件在 CloudTrail 的事件歷史記錄主控台中搜尋來完成：

```
"UpdatePassword"
```

如果訊息陳述以下內容，則您可能需要聯絡 支援：

```
"errorCode": "InternalFailure",  
  "errorMessage": "An unknown error occurred"
```

此問題的另一個可能原因是在套用到使用者名稱值的命名慣例中。命名慣例必須遵循特定模式，例如 'surname.givenName'。不過，某些使用者名稱可能很長，或包含特殊字元，這可能會導致 API 呼叫中捨棄字元，進而導致錯誤。您可能想要以相同的方式嘗試測試使用者重設密碼，以驗證是否為這種情況。

如果問題仍然存在，請聯絡 [AWS 支援中心](#)。

許可集中會參考我的使用者，但無法存取指派的帳戶或應用程式

如果您使用 System for Cross-domain Identity Management (SCIM) 搭配外部身分提供者進行自動佈建，可能會發生此問題。具體而言，當刪除使用者或使用者所屬的群組，然後在身分提供者中使用相同的使用者名稱（適用於使用者）或名稱（適用於群組）重新建立時，會為 IAM Identity Center 中的新使用者或群組建立新的唯一內部識別符。不過，IAM Identity Center 在其許可資料庫中仍有舊識別符的參考，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 參考的基礎使用者或群組 ID 不再存在。

若要還原在此情況下的 AWS 帳戶存取權，您可以從最初指派的 AWS 帳戶（多個）移除舊使用者或群組的存取權，然後將存取權重新指派給使用者或群組。這會更新具有新使用者或群組正確識別符的許可集。同樣地，若要還原應用程式存取，您可以從該應用程式指派的使用者清單中移除使用者或群組的存取，然後再次新增使用者或群組。

您也可以從 CloudTrail 日誌中搜尋參照有問題之使用者或群組名稱的 SCIM 同步事件，以查看是否已 AWS CloudTrail 記錄失敗。

我無法從應用程式目錄正確設定我的應用程式

如果您從 IAM Identity Center 中的應用程式目錄新增應用程式，請注意每個服務供應商都提供自己的詳細文件。您可以從 IAM Identity Center 主控台中應用程式的組態索引標籤存取此資訊。

如果問題與設定服務供應商應用程式和 IAM Identity Center 之間的信任有關，請務必檢查說明手冊中的故障診斷步驟。

錯誤「使用者嘗試使用外部身分提供者登入時發生非預期錯誤」

此錯誤可能有多種原因，但其中一個常見原因是 SAML 請求中傳送的使用者資訊與 IAM Identity Center 中使用者的資訊不相符。

為了讓 IAM Identity Center 使用者在使用外部 IdP 做為身分來源時成功登入，下列項目必須是 true：

- SAML nameID 格式（在您的身分提供者設定）必須為「電子郵件」
- nameID 值必須是正確 (RFC2822) 格式的字串 (user@domain.com)
- nameID 值必須與 IAM Identity Center 中現有使用者的使用者名稱完全相符 (IAM Identity Center 中的電子郵件地址是否相符並不重要 – 傳入比對是根據使用者名稱)
- SAML 2.0 聯合的 IAM Identity Center 實作在身分提供者和 IAM Identity Center 之間的 SAML 回應中僅支援 1 個聲明。它不支援加密的 SAML 聲明。
- 如果在 IAM Identity Center 帳戶中啟用 [存取控制的屬性](#)，則適用下列陳述式：
 - SAML 請求中映射的屬性數目必須為 50 個或更少。
 - SAML 請求不得包含多值屬性。
 - SAML 請求不得包含具有相同名稱的多個屬性。
 - 屬性不得包含結構化 XML 做為值。
 - 名稱格式必須是 SAML 指定的格式，而非一般格式。

Note

IAM Identity Center 不會透過 SAML 聯合為新使用者或群組「即時」建立使用者或群組。這表示使用者必須在 IAM Identity Center 中手動或透過自動佈建預先建立，才能登入 IAM Identity Center。

當身分提供者中設定的宣告消費者服務 (ACS) 端點不符合 IAM Identity Center 執行個體提供的 ACS URL 時，也會發生此錯誤。確定這兩個值完全相符。

此外，您可以前往 AWS CloudTrail 並篩選事件名稱 ExternalIdPDirectoryLogin，進一步疑難排解外部身分提供者登入失敗。

錯誤 '存取控制的屬性無法啟用'

如果啟用 ABAC 的使用者沒有啟用 所需的 `iam:UpdateAssumeRolePolicy` 許可，可能會發生此錯誤 [存取控制的屬性](#)。

當我嘗試為 MFA 註冊裝置時，會收到「瀏覽器不受支援」訊息

Google Chrome、Mozilla Firefox、Microsoft Edge 和 Apple Safari Web 瀏覽器，以及 Windows 10 和 Android 平台目前支援 WebAuthn。WebAuthn 支援的某些元件可能有所不同，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支援的瀏覽器或平台上註冊 WebAuthn 裝置，他們會看到某些顯示為灰色且不支援的選項，或者會收到不支援所有支援方法的錯誤。在這些情況下，請參閱 [FIDO2 : Web Authentication \(WebAuthn\)](#)，以取得瀏覽器/平台支援的詳細資訊。如需 IAM Identity Center 中 WebAuthn 的詳細資訊，請參閱 [FIDO2 驗證器](#)。

Active Directory「網域使用者」群組未正確同步至 IAM Identity Center

Active Directory 網域使用者群組是 AD 使用者物件的預設「主要群組」。IAM Identity Center 無法讀取 Active Directory 主要群組及其成員資格。將存取權指派給 IAM Identity Center 資源或應用程式時，請使用網域使用者群組（或指派為主要群組的其他群組）以外的群組，讓群組成員資格正確反映在 IAM Identity Center 身分存放區中。

無效的 MFA 登入資料錯誤

當使用者嘗試使用外部身分提供者的帳戶（例如，Okta 或 Microsoft Entra ID）登入 IAM Identity Center，再使用 SCIM 通訊協定將帳戶完全佈建至 IAM Identity Center 時，可能會發生此錯誤。將使用者帳戶佈建至 IAM Identity Center 之後，應該解決此問題。確認帳戶已佈建至 IAM Identity Center。如果沒有，請檢查外部身分提供者中的佈建日誌。

當我嘗試使用驗證器應用程式註冊或登入時，收到「發生非預期的錯誤」訊息

時間型一次性密碼 (TOTP) 系統，例如 IAM Identity Center 與程式碼型驗證器應用程式搭配使用的系統，依賴用戶端和伺服器之間的時間同步。請確定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的來源，例如 NIST (<https://www.time.gov/>) 或其他本機/區域對等項目。

我收到 '這不是您，這是嘗試登入 IAM Identity Center 時的錯誤

此錯誤表示您的 IAM Identity Center 執行個體或外部身分提供者 (IdP) IAM Identity Center 正在使用 做為其身分來源時發生設定問題。我們建議您驗證下列項目：

- 驗證您用來登入之裝置上的日期和時間設定。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 Identity Center 的 IdP 憑證與 IdP 提供的憑證相同。您可以導覽至設定，從 IAM Identity Center 主控台檢查憑證。在身分來源索引標籤中，選擇動作，然後選擇管理身分驗證。如果 IdP 和 IAM Identity Center 憑證不相符，請將新憑證匯入 IAM Identity Center。
- 請確定身分提供者中繼資料檔案中的 NameID 格式如下：
 - urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
- 如果您使用 AD Connector 從 AWS Directory Service 做為身分提供者，請確認服務帳戶的登入資料正確且尚未過期。如需詳細資訊，請參閱 [在中更新您的 AD Connector 服務帳戶登入 AWS Directory Service](#) 資料。

我的使用者未收到來自 IAM Identity Center 的電子郵件

IAM Identity Center 服務傳送的所有電子郵件都將來自地址 `no-reply@signin.aws` 或 `no-reply@login.awsapps.com`。必須設定您的郵件系統，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。

錯誤：您無法delete/modify/remove/指派對管理帳戶中佈建之許可集的存取權

此訊息表示 [委派的管理](#) 已啟用此功能，且您先前嘗試的操作只能由具有管理帳戶許可的人員成功執行 AWS Organizations。若要解決此問題，請以具有這些許可的使用者身分登入，然後嘗試再次執行任務，或將此任務指派給具有正確許可的人員。如需詳細資訊，請參閱 [註冊成員帳戶](#)。

錯誤：找不到工作階段字符或工作階段字符無效

當 Web 瀏覽器 AWS 工具組或等用戶端嘗試使用在伺服器端撤銷或失效的工作階段時 AWS CLI，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，包括出現提示時再次登入。這有時可能會要求您取消待處理的請求，例如來自 IDE AWS 工具組內的待處理連線嘗試。

來自信任網域的群組成員不會同步到 IAM Identity Center

如果安全群組成功同步至 IAM Identity Center，但其來自受信任內部部署網域的成員未出現在 IAM Identity Center 中，這可能是由於群組位於 中 AWS Managed Microsoft AD，並包含代表來自受信任網域使用者的外部安全委託人 (FSPs)。

請嘗試下列步驟以診斷故障：

- 直接從信任的網域同步群組：與其從包含跨網域成員 AWS Managed Microsoft AD 的 同步群組，請直接從信任的內部部署網域建立和同步群組。這種方法有效，因為 IAM Identity Center 可以存取來源網域中的實際使用者物件。
- 驗證服務帳戶許可：確保 IAM Identity Center 服務帳戶具有信任網域中使用者物件的必要許可：ReadProperties 和 ListContents 許可。

對 中的客戶受管金鑰進行故障診斷 AWS IAM Identity Center

本主題說明使用 時可能遇到的常見客戶受管金鑰相關錯誤 AWS IAM Identity Center，並提供解決問題的疑難排解步驟。

拒絕存取：KMS 解密許可問題

錯誤：「使用者 xxxxxxxx 未獲授權執行：與此加密文字相關聯的資源上的 kms:Decrypt，因為沒有身分型政策允許 kms:Decrypt 動作」

使用者或 IAM 主體在其 IAM 政策或 KMS 金鑰政策中缺少必要的kms:Decrypt許可。

使用 進行故障診斷 AWS CloudTrail：

1. 尋找 CloudTrail 中的kms.amazonaws.com事件
2. 搜尋事件名稱 Decrypt
3. 檢閱 errorCode和 errorMessage 欄位
4. 檢查 userIdentity以確認哪些委託人嘗試 操作

若要解決此問題，請在其 IAM 政策和 KMS 金鑰政策中授予使用者或 IAM 主體kms:Decrypt存取許可。如需詳細資訊，請參閱[在中實作客戶受管 KMS 金鑰 AWS IAM Identity Center](#)。

AWS 在 IAM Identity Center 中啟用客戶受管 KMS 金鑰的受管應用程式登入失敗

如果 Identity Center 使用者無法登入 AWS 受管應用程式，且您的 IAM Identity Center 執行個體已啟用客戶受管 KMS 金鑰，請確認 KMS 金鑰政策授予 AWS 受管應用程式使用客戶受管 KMS 金鑰的許可。如需詳細資訊，請參閱[基準 KMS 金鑰政策](#)。

AWS 受管應用程式安裝和/或使用使用者指派失敗，並在 IAM Identity Center 中啟用客戶受管 KMS 金鑰

錯誤：「使用者 xxxxxxxx 未獲授權執行：與此加密文字相關聯的資源上的 kms:Decrypt，因為沒有身分型政策允許 kms:Decrypt 動作」

使用者或 IAM 主體在其 IAM 政策或 KMS 金鑰政策中缺少必要的 kms:Decrypt 許可。

使用 CloudTrail 進行故障診斷：

1. 搜尋事件名稱 Decrypt
2. 檢閱 errorCode 和 errorMessage 欄位
3. 檢查 userIdentity 以確認哪些委託人嘗試操作

若要解決此問題，請在其 IAM 政策和 KMS 金鑰政策中授予使用者或 IAM 主體 kms:Decrypt 存取許可。如需詳細資訊，請參閱[在中實作客戶受管 KMS 金鑰 AWS IAM Identity Center](#)。

KMS 許可問題：使用設定客戶受管金鑰 AWS IAM Identity Center

使用者或 IAM 主體在啟用客戶受管金鑰時，缺少一或多個必要的 KMS kms:Encrypt 許可 (kms:Decrypt、kms:GenerateDataKey、kms:DescribeKey)。

使用 CloudTrail 進行故障診斷：

1. 搜尋 Decrypt、GenerateDataKey、Encrypt 或 DescribeKey 事件
2. 檢閱 errorCode 和 errorMessage 欄位
3. 檢查 userIdentity 以確認哪些委託人嘗試操作

若要解決此問題，請將所有必要的 KMS 許可授予其身分型政策或 KMS 金鑰政策中的使用者或 IAM 主體。如需詳細資訊，請參閱[在中實作客戶受管 KMS 金鑰 AWS IAM Identity Center](#)。

AWS 在 IAM Identity Center 中啟用客戶受管 KMS 金鑰的存取入口網站登入失敗

錯誤：「ERROR 代碼：0001 - IdentityCenter 服務存取遭到封鎖。如需後續步驟，請聯絡您的 IdentityCenter 管理員。」

如果使用者無法登入 AWS 存取入口網站，且您的 IAM Identity Center 執行個體已啟用客戶受管 KMS 金鑰，請確認 KMS 金鑰政策授予 Identity Center 和 Identity Store 必要的許可。如需詳細資訊，請參閱[基準 KMS 金鑰政策](#)。

對 中的多區域設定進行故障診斷 AWS IAM Identity Center

本主題說明使用時可能遇到的常見多區域設定相關錯誤 AWS IAM Identity Center，並提供解決問題的疑難排解步驟。

我想要複寫 IAM Identity Center 執行個體的區域無法在 IAM Identity Center 主控台中使用

您必須先在要複寫 IAM Identity Center 執行個體的區域中，為客戶受管 KMS 金鑰建立複本金鑰。建立複本金鑰後，您會在可供複寫的區域清單中看到區域。如需詳細資訊，請參閱[the section called “步驟 1：建立複本金鑰”](#)。

AWS 其他區域中的受管應用程式登入失敗

如果在 IAM Identity Center 中新增區域後，沒有 IAM Identity Center 使用者可以在其他區域中登入 AWS 受管應用程式，請確認您已在外部身分提供者中設定了其他區域的聲明消費者服務 (ACS) URL，如中所述[the section called “步驟 3：更新外部 IdP 設定”](#)。此外，確認您的使用者已連線至區域。

文件歷史記錄

下表說明 AWS IAM Identity Center 文件的重要新增項目。我們也會經常更新文件，以處理您傳送給我們的意見回饋。

- 最新主要文件更新時間：2025 年 10 月 21 日

變更	描述	日期
簡化的基準 KMS 金鑰政策	將基準 KMS 金鑰政策陳述式合併為單一簡化政策，可簡化客戶受管 KMS 金鑰的組態，以進行靜態加密。	2026 年 4 月 30 日
多區域支援	新增多區域支援，包括複寫至其他區域、AWS 帳戶存取和使用其他區域中的 AWS 受管應用程式。	2026 年 2 月 2 日
更新 AWS 受管政策	已更新 AWSIdentityCenterExternalManagementPolicy AWS 受管政策，以變更佈建租用戶的 ARN。	2025 年 12 月 5 日
新的 AWS 受管政策主題	新增 AWSIdentityCenterExternalManagementPolicy AWS 受管政策的詳細資訊。	2025 年 11 月 21 日
自動佈建稽核和調校指引	新增使用 Identity Store APIs 和 AWS CLI 命令稽核和協調 SCIM 自動佈建的使用者、群組和群組成員資格的指引。	2025 年 10 月 17 日
OIDC 服務請求配額	新增 OIDC 服務請求配額，包括 OAuth 用戶端註冊、權杖建	2025 年 10 月 13 日

立和其他 OIDC 操作的速率限制。

[AWS 受管政策的更新](#)

IAM Identity Center 已更新受管政策 AWSSSOMasterAccountAdministrator、AWSSSODirectoryAdministrator、AWSSSOMemberAccountAdministrator、AWSSSODirectoryReadOnly 和 AWSSSODirectoryReadOnly，以包含使用客戶受管金鑰進行加密的 IAM Identity Center 執行個體所需的 AWS KMS 許可。

2025 年 9 月 17 日

[靜態加密的客戶受管金鑰](#)

新增對客戶受管 KMS 金鑰的支援，以加密靜態人力資源身分資料。

2025 年 9 月 17 日

[允許權杖建立的資源型政策範例](#)

新增以資源為基礎的政策範例，允許建立授權用戶端應用程式的權杖。

2025 年 9 月 16 日

[支援使用者背景工作階段](#)

新增使用者背景工作階段的內容。

2025 年 8 月 11 日

[身分增強主控台工作階段](#)

已更新身分增強主控台工作階段的術語（先前稱為身分感知工作階段）。

2025 年 5 月 12 日

[開始重組](#)

重新組織入門內容，以提升清晰度和使用者體驗。

2025 年 5 月 6 日

棄用 IAM Identity Center AD Sync	您無法再使用 IAM Identity Center AD Sync 佈建 Active Directory 使用者。反之，您可以使用 IAM Identity Center 可設定的 AD Sync。	2025 年 4 月 17 日
已更新已驗證工作階段的內容	刪除使用者工作階段時，更新為 IAM Identity Center 工作階段持續時間。	2025 年 4 月 2 日
AWS 受管政策的更新	已更新 AWSSSOServiceRolePolicy AWS 受管政策的許可。	2025 年 2 月 11 日
IAM Identity Center 啟用工作流程已改善	更新啟用 IAM Identity Center 組織執行個體和帳戶執行個體的工作流程。	2025 年 2 月 11 日
IAM Identity Center 啟用的更新	更新啟用 IAM Identity Center 組織執行個體和帳戶執行個體的內容和程序。	2024 年 10 月 10 日
AWS 受管政策的更新	已更新 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的許可。	2024 年 10 月 2 日
AWS 受管政策的更新	已更新 AWSSSOMasterAccountAdministrator AWS 受管政策的許可。	2024 年 9 月 26 日
AWS 受管政策的更新	已更新 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的許可。	2024 年 9 月 4 日

「什麼是 IAM Identity Center？」的更新 主題	更新描述 IAM Identity Center 優點和功能的內容。	2024 年 8 月 19 日
AWS 受管政策的更新	已更新 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的許可。	2024 年 7 月 12 日
AWS 受管政策的更新	已更新 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的許可。	2024 年 6 月 27 日
AWS 受管政策的更新	已更新 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的許可。	2024 年 5 月 17 日
AWS 受管政策的更新	已更新 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的許可。	2024 年 4 月 30 日
AWS 受管政策的更新	已更新 AWSSSOMasterAccountAdministrator AWS 受管政策的許可。	2024 年 4 月 26 日
AWS 受管政策的更新	已更新 AWSSSOMemberAccountAdministrator AWS 受管政策的許可。	2024 年 4 月 26 日
AWS 受管政策的更新	已更新 AWSSS0ReadOnly AWS 受管政策的許可。	2024 年 4 月 26 日

AWS 受管政策的更新	已更新 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的許可。	2024 年 4 月 26 日
AWS 受管政策的更新	已更新 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的許可。	2024 年 4 月 24 日
AWS 受管政策的更新	已更新 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的許可。	2024 年 4 月 19 日
AWS 受管政策的更新	已更新 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的許可。	2024 年 4 月 11 日
AWS 受管政策的更新	已更新 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的許可。	2023 年 11 月 26 日
新的 AWS 受管政策主題	新增 AWSIAMIdentityCenterAllowListForIdentityContext AWS 受管政策的詳細資訊。	2023 年 11 月 15 日
IAM Identity Center 入門的增強型指引	新增了開始使用 IAM Identity Center 和建立管理使用者的新內容	2022 年 9 月 23 日
已更新 Identity Center API 參考中的使用者和群組	此更新包含 Identity Center APIs 參考指南中新建立、更新和刪除 API 的參考。	2022 年 8 月 31 日

AWS 單一登入 (AWS SSO) 已重新命名為 AWS IAM Identity Center	AWS 介紹 AWS IAM Identity Center。IAM Identity Center 擴展 AWS Identity and Access Management (IAM) 的功能，協助您集中管理 帳戶，並為您的人力資源使用者存取應用程式。IAM Identity Center 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
在許可集中支援許可界限和客戶受管政策	新增使用 AWS 受管和客戶受管 AWS Identity and Access Management (IAM) 政策搭配許可集的內容。	2022 年 7 月 14 日
支援手動啟用 AWS 的區域	新增在手動啟用的區域中使用 IAM Identity Center 的內容。	2022 年 6 月 15 日
AWS 受管政策的更新	已更新 AWSSSOServiceRolePolicy AWS 受管政策的許可。	2022 年 5 月 11 日
支援委派的管理	新增委派管理功能的內容。	2022 年 5 月 11 日
AWS 受管政策的更新	已更新 AWSSSOMasterAccountAdministrator、AWSSSOMemberAccountAdministrator 和 AWSSSOREadOnly AWS 受管政策的許可。	2022 年 4 月 28 日
支援可設定的 AD 同步	新增可設定 AD 同步功能的內容。	2022 年 4 月 14 日
新的 AWS 受管政策主題	新增 AWSSSOMasterAccountAdministrator AWS 受管政策的詳細資訊。	2021 年 8 月 4 日

配額的更新	配額資料表的調整。	2020 年 12 月 21 日
新範例政策	已將新的客戶受管政策範例和更新新增至必要的許可區段。	2020 年 12 月 21 日
支援屬性型存取控制 (ABAC)	新增 ABAC 功能的內容。	2020 年 11 月 24 日
支援 MFA 強制註冊	更新以要求使用者在登入時註冊 MFA 裝置。	2020 年 11 月 23 日
支援 WebAuthn	新增新WebAuthn功能的內容。	2020 年 11 月 20 日
支援 Ping 身分	新增內容，以將與 Ping Identity產品整合為支援的外部身分提供者。	2020 年 10 月 26 日
支援 OneLogin	新增與整合的內容，OneLogin 做為支援的外部身分提供者。	2020 年 7 月 31 日
支援Okta	新增與整合的內容，Okta做為支援的外部身分提供者。	2020 年 5 月 28 日
支援外部身分提供者	將參考從目錄變更為身分來源，新增內容以支援外部身分提供者。	2019 年 11 月 26 日
新的 MFA 設定	移除兩步驟驗證主題，並在其位置新增新的 MFA 主題。	2019 年 10 月 24 日
新增兩步驟驗證的新設定	新增如何為使用者啟用兩步驟驗證的內容。	2019 年 1 月 16 日
支援 AWS 帳戶上的工作階段持續時間	新增如何設定 AWS 帳戶工作階段持續時間的內容。	2018 年 10 月 30 日
使用 Identity Center 目錄的新選項	新增了用於選擇 Identity Center 目錄或連接到 Active Directory 中現有目錄的內容。	2018 年 10 月 17 日

支援應用程式上的轉送狀態和工作階段持續時間	新增有關應用程式轉送狀態和工作階段持續時間的內容。	2018 年 10 月 10 日
新應用程式的其他支援	已將 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvalnSync, 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, 和 UserEcho 新增至應用程式目錄。	2018 年 8 月 3 日
支援管理帳戶的多帳戶存取	新增有關如何將多帳戶存取權委派給管理帳戶中使用者的內容。	2018 年 7 月 9 日
支援新應用程式	已將 DocuSign, Keeper Security, 和 SugarCRM 新增至應用程式目錄。	2018 年 3 月 16 日
取得 CLI 存取的臨時登入資料	新增如何取得臨時登入資料以執行 AWS CLI 命令的相關資訊。	2018 年 2 月 22 日
新的指南	這是 IAM Identity Center 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。