aws

管理指南

AWS Directory Service

版本 1.0

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

AWS Directory Service: 管理指南

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

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

Table of Contents

什麼是 AWS Directory Service？ 1
AWS Directory Service 選項 1
該選擇哪種 4
使用 Amazon EC2 5
AWS Managed Microsoft AD 6
該選擇哪種 6
主題 7
AWS Managed Microsoft AD （混合版本） 7
混合目錄先決條件 8
建立混合目錄 15
檢視和編輯混合目錄 16
刪除混合目錄 18
目錄評估 19
故障診斷 22
開始使用 45
AWS Managed Microsoft AD 先決條件 45
AWS IAM Identity Center 先決條件 46
多重要素驗證先決條件 46
建立 AWS Managed Microsoft AD 47
使用 AWS Managed Microsoft AD 建立的內容 49
管理員帳戶和群組許可 58
關鍵概念和最佳實務 60
重要概念 61
最佳實務 64
使用案例 72
使用案例 1：使用Active Directory登入資料登入 AWS 應用程式和服務 72
使用案例 2：管理 Amazon EC2 執行個體 77
使用案例 3：為您的 Active Directory感知工作負載提供目錄服務 77
使用案例 4： AWS IAM Identity Center 至 Office 365 和其他雲端應用程式 77
使用案例 5：將您的內部部署擴展Active Directory到 AWS 雲端 78
使用案例 6：共用您的目錄，以順暢地將 Amazon EC2 執行個體加入跨 AWS 帳戶的網域 78
維護您的目錄 78
檢視目錄資訊 79
使用快照還原目錄 80

部署額外的網域控制器 85
升級您的 AWS Managed Microsoft AD 88
新增備用 UPN 尾碼 90
重新命名目錄的網站名稱 90
刪除您的 AWS Managed Microsoft AD 91
保護您的目錄 93
了解密碼政策 93
啟用多重因素認證 99
啟用安全 LDAP 或 LDAPS 102
管理您的目錄合規性 113
增強網路安全 114
編輯目錄安全設定 125
設定適用於 AD 的 AWS Private CA Connector 132
監控您的目錄 135
了解您的目錄狀態 136
使用 Amazon SNS 啟用目錄狀態通知 137
了解您的目錄日誌 140
啟用 Amazon CloudWatch 日誌轉送 141
使用 CloudWatch 監控您的目錄 145
停用 Amazon CloudWatch 日誌轉送 148
使用 Microsoft 事件檢視器監控 DNS 伺服器 149
存取 AWS 應用程式和服務 149
應用程式相容性 150
啟用存取 AWS 應用程式和服務 152
啟用對 的存取 AWS Management Console 155
建立存取 URL 157
啟用單一登入 158
授予 資源的 AWS 存取權 165
建立新的角色 166
編輯現有角色的信任關係 167
將使用者或群組指派給現有角色 168
檢視指派給角色的使用者和群組 169
從角色移除使用者或群組 170
使用 AWS 受管政策 171
設定多區域複寫 172
運作方式 173

優勢 174
全域與區域功能 175
主要區域與其他區域 175
新增複寫的區域 176
刪除複寫的區域 178
共享您的目錄 179
重要概念 179
考量事項 180
教學課程：共用您的 AWS Managed Microsoft AD 目錄 181
取消共用您的目錄 190
將 Active Directory 使用者遷移至 AWS Managed Microsoft AD 190
連接現有的 Active Directory 基礎設施 191
建立信任關係 191
新增 IP 路由 196
教學：在 AWS Managed Microsoft AD 和自我管理的 Active Directory 域之間建立信任關係 . 197
教學課程：在 AWS Managed Microsoft AD 網域之間建立信任關係 206
擴展您的目錄結構描述 210
何時擴展 AWS Managed Microsoft AD 結構描述 211
教學課程：擴展 AWS Managed Microsoft AD 結構描述 211
將執行個體加入目錄的方法 217
啟動目錄管理執行個體 217
加入 Windows 執行個體 220
加入 Linux 執行個體 227
加入 Mac 執行個體 273
委派目錄聯結權限 275
建立或變更 DHCP 選項集 276
使用者和群組管理 278
AWS Management Console 278
AWS CLI 279
AWS Tools for PowerShell 279
內部部署或 Amazon EC2 執行個體 280
使用主控台、CLI 或 管理使用者和群組 PowerShell 280
使用 Amazon EC2 執行個體管理使用者和群組 318
目錄服務資料 326
複寫和一致性 327
AWS Directory Service Data 屬性 327

群組類型和群組範圍 332
連接到 Microsoft Entra Connect Sync 333
先決條件 333
建立Active Directory網域使用者 333
下載 Entra Connect Sync 334
執行PowerShell指令碼 334
安裝 Entra Connect Sync 336
AWS Managed Microsoft AD 測試實驗室教學課程 337
教學課程：設定您的基礎 AWS Managed Microsoft AD 測試實驗室 337
教學課程：從 AWS Managed Microsoft AD 建立對 EC2 上自我管理 AD 安裝的信任 352
配額 360
故障診斷 361
AWS Managed Microsoft AD 的問題 362
Netlogon 和安全頻道通訊的問題 362
嘗試重設使用者密碼時，您會收到「回應狀態：400 錯誤請求」錯誤 362
密碼復原 362
其他資源 363
Amazon EC2 Linux 執行個體網域聯結錯誤 363
低可用儲存空間 366
結構描述延伸錯誤 369
信任建立狀態原因 371
AD Connector 375
開始使用 376
AD Connector 事前準備 376
建立 AD Connector 390
使用 AD Connector 建立的內容 391
最佳實務 392
設定：事前準備 392
編寫程式設計自己的應用程式 394
使用您的目錄 394
維護您的目錄 395
檢視目錄資訊 395
更新 AD Connector 的 DNS 地址 395
刪除 AD Connector 396
保護您的目錄 397
啟用多重因素認證 398

啟用用戶端 LDAPS ... 400
啟用 mTLS 身分驗證 ... 405
更新您的 AD Connector 服務帳戶憑證 ... 413
設定適用於 AD 的 AWS Private CA Connector ... 414
監控您的目錄 ... 416
了解您的目錄狀態 ... 416
使用 Amazon SNS 啟用目錄狀態通知 ... 417
存取 AWS 應用程式和服務 ... 419
應用程式相容性 ... 419
啟用從 AD Connector 存取 AWS 應用程式和服務 ... 420
將 Amazon EC2 執行個體加入 的方法 Active Directory ... 422
配額 ... 422
故障診斷 ... 423
建立問題 ... 423
連線問題 ... 425
身分驗證問題 ... 426
維護問題 ... 432
我無法刪除我的 AD Connector ... 433
調查 AD Connector 發行者的一般工具 ... 433
Simple AD ... 435
開始使用 ... 436
Simple AD 先決條件 ... 436
建立您的 Simple AD ... 438
使用 Simple AD 建立的內容 ... 441
最佳實務 ... 442
設定：事前準備 ... 442
設定：建立您的目錄 ... 443
編寫程式設計自己的應用程式 ... 444
維護您的目錄 ... 445
檢視目錄資訊 ... 445
設定 DNS 伺服器 ... 445
使用快照還原您的目錄 ... 446
刪除您的 Simple AD ... 448
保護您的目錄 ... 449
重設 krbtgt 帳戶密碼 ... 450
監控您的目錄 ... 451

了解您的目錄狀態 452
使用 Amazon Simple Notification Service 啟用目錄狀態通知 453
存取 AWS 應用程式和服務 455
應用程式相容性 455
啟用對應用程式和服務的 AWS 存取 456
啟用對 的存取 AWS Management Console 457
建立存取 URL 459
啟用單一登入 460
將執行個體加入目錄的方法 467
加入 Windows 執行個體 468
加入 Linux 執行個體 473
委派目錄聯結權限 495
建立 DHCP 選項集 496
使用者和群組管理 497
安裝 AD 管理工具 498
建立使用者 500
刪除使用者 501
重設使用者密碼 501
建立群組 503
將使用者新增至群組 503
配額 504
故障診斷 505
密碼復原 505
將使用者新增至 Simple AD 時，我收到「KDC 無法滿足請求的選項」錯誤 505
我無法更新已加入我的網域之執行個體的 DNS 名稱或 IP 地址 (DNS 動態更新) 506
我無法使用 SQL Server 帳戶登入 SQL Server 506
我的 Simple AD 卡在「請求」狀態 506
我在建立 Simple AD 時收到「可用區域限制」錯誤 506
我的一些使用者無法使用我的 Simple AD 進行身分驗證 506
其他資源 363
對目錄狀態訊息進行故障診斷 507
安全 510
身分與存取管理 511
身分驗證 511
存取控制 511
管理存取概觀 512

AWS 受管政策 516
使用以身分為基礎的政策 (IAM 政策) 519
AWS Directory Service API 許可參考 528
Directory Service Data 條件索引鍵 530
使用 AWS 的應用程式和服務授權 AWS Directory Service 536
在 Active Directory 上授權 AWS 應用程式 536
AWS 具有 Directory Service Data 的應用程式授權 537
使用服務連結角色 539
的服務連結角色許可 AWS Directory Service 539
為 建立服務連結角色 AWS Directory Service 540
編輯 的服務連結角色 AWS Directory Service 541
刪除 的服務連結角色 AWS Directory Service 541
AWS Directory Service 服務連結角色支援的區域 541
日誌記錄和監控 543
AWS Directory Service 日誌 543
AWS Directory Service 資料日誌 546
法規遵循驗證 555
恢復能力 556
基礎架構安全 556
預防跨服務混淆代理人 557
AWS PrivateLink 560
考量事項 560
可用性 561
建立界面 Amazon VPC 端點 561
建立端點政策 561
服務水準協議 564
區域可用性 565
AWS 區域 支援 Directory Service Data 572
瀏覽器相容性 575
什麼是 TLS？ 575
IAM Identity Center 支援哪些 TLS 版本 575
在瀏覽器中啟用受支援 TLS 版本的方法 575
文件歷史紀錄 576
..... dlxxx

什麼是 AWS Directory Service？

AWS Directory Service 提供多種搭配其他服務使用 MicrosoftActive Directory(AD) 的方式 AWS 。目錄存放有關使用者、群組和裝置的資訊，以及管理員使用這些目錄來管理對資訊和資源的存取。 為想要在雲端中使用現有 Microsoft AD 或輕量型目錄存取協定 (LDAP) 感知應用程式的客戶 AWS Directory Service 提供多種目錄選擇。它也同樣為需要使用目錄管理使用者、群組、裝置和存取的開發人員，提供這些選項。

AWS Directory Service 選項

AWS Directory Service 包含數種目錄類型可供選擇。如需詳細資訊，請選擇以下標籤的其中一個：

AWS Directory Service for Microsoft Active Directory

也稱為 AWS Managed Microsoft AD， AWS Directory Service for Microsoft Active Directory 是由 雲端 AWS 中管理的實際 MicrosoftWindows ServerActive Directory(AD) AWS 提供支援。它可讓您將廣泛的Active Directory感知應用程式遷移至 AWS Cloud。 AWS 受管 Microsoft AD 可與 Microsoft SharePoint、 Microsoft SQL Server Always On 可用性群組和許多 .NET 應用程式搭配使用。它還支援 AWS 的受管應用程式和服務，包括 Amazon WorkSpaces、Amazon WorkDocs、Amazon QuickSight、Amazon Chime、Amazon Connect 和 Amazon Relational Database Service for Microsoft SQL Server (Amazon RDS for SQL Server、Amazon RDS for Oracle和 Amazon RDS for PostgreSQL)。

AWS 當您啟用目錄的合規時，Managed Microsoft AD 已獲准用於 AWS 雲端中受美國健康保險流通與責任法案 (HIPAA) 或支付卡產業資料安全標準 (PCI DSS) 合規規範的應用程式。 https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_compliance.html

所有相容的應用程式都會使用您存放在 AWS Managed Microsoft AD 中的使用者登入資料，或者您可以使用信任來連線到現有的 AD 基礎設施，並使用執行Active Directory中內部部署或 EC2 Windows 上的登入資料。如果您將 EC2 執行個體加入 AWS Managed Microsoft AD，您的使用者可以使用與存取內部部署網路中的工作負載時相同的 Windows 單一登入 (SSO) 體驗來存取 AWS 雲端中的 Windows 工作負載。

AWS Managed Microsoft AD 也支援使用 Active Directory憑證的聯合使用案例。單獨， AWS 受管 Microsoft AD 可讓您登入 AWS Management Console。透過 AWS IAM Identity Center，您也可以取得短期登入資料以搭配 AWS SDK 和 CLI 使用，並使用預先設定的 SAML 整合來登入許多雲端應用程式。透過新增 Microsoft Entra Connect (先前稱為 Azure Active Directory Connect) 和選用

Active Directory的聯合服務 (AD FS)，您可以使用儲存在 AWS Managed Microsoft AD 中的登入資料登入 Microsoft Office 365 和其他雲端應用程式。

此服務包括一些重要功能，可讓您擴展您的結構描述、管理密碼政策，以及透過 Secure Socket Layer (SSL)/Transport Layer Security (TLS) 啟用安全 LDAP 通訊。您也可以為 AWS Managed Microsoft AD 啟用多重要素驗證 (MFA)，以便在使用者從網際網路存取 AWS 應用程式時提供額外的安全層。由於 Active Directory 是 LDAP 目錄，因此您也可以使用 AWS Managed Microsoft AD for Linux Secure Shell (SSH) 身分驗證和其他啟用 LDAP 的應用程式。

AWS 在 服務中提供監控、每日快照和復原，您可以將使用者和群組新增至 AWS Managed Microsoft AD，並使用在加入 AWS Managed Microsoft AD 網域的Windows電腦上執行的熟悉 Active Directory工具來管理群組政策。您也可透過以下方式擴展目錄：部署額外的網域控制站，並在大量的網域控制站之間分佈請求以協助提升應用程式效能。

AWS Managed Microsoft AD 提供兩種版本：Standard 和 Enterprise。

- 標準版本：AWS Managed Microsoft AD (標準版) 經過最佳化，適合擁有多達 5,000 名員工的中小型企業做為主要目錄使用。其提供您足夠的儲存容量，可支援最多 30,000* 個目錄物件，例如使用者、群組和電腦。
- 企業版本：AWS Managed Microsoft AD (企業版) 可支援擁有多達 500,000* 個目錄物件的企業組織。

* 上限為約略值。您的目錄可支援更多或更少個目錄物件，這取決於您物件的大小和您應用程式的行為和效能需求。

使用情況

AWS 如果您需要支援 AWS 應用程式或Windows工作負載的實際Active Directory功能，包括適用於 的 Amazon Relational Database Service，則 Managed Microsoft AD 是您的最佳選擇 Microsoft SQL Server。如果您想要在支援 Office 365 的 AWS 雲端Active Directory中獨立運作，或需要 LDAP 目錄來支援 Linux 應用程式，也是最佳選擇。如需詳細資訊，請參閱AWS Managed Microsoft AD。

AD Connector

AD Connector 是一種代理服務，可讓您輕鬆將Windows Server執行個體的 Amazon WorkSpaces、Amazon QuickSight 和 Amazon EC2 等相容 AWS 應用程式連線至您現有的內部部署 Microsoft Active Directory。使用 AD Connector ，您只需將一個服務帳戶新增至您的 Active Directory。AD Connector 也免除了同步目錄的需要，或託管聯合基礎設施的成本和複雜性。

當您將使用者新增至 Amazon QuickSight 等 AWS 應用程式時，AD Connector 會讀取您現有的 Active Directory，以建立要選取的使用者和群組清單。當使用者登入 AWS 應用程式時，AD Connector 會將登入請求轉送至您的現場部署Active Directory網域控制站以進行身分驗證。AD Connector 可與許多 AWS 應用程式和服務搭配使用，包括 Amazon WorkSpaces、Amazon WorkDocs、Amazon QuickSight、Amazon Chime、Amazon Connect 和 Amazon WorkMail。您也可以使用無縫Active Directory網域聯結，透過 AD Connector 將 EC2 Windows執行個體加入內部部署網域。 https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad_connector_launching_instance.htmlAD Connector 也可讓您的使用者使用現有的Active Directory登入資料登入，以存取 AWS Management Console 和管理 AWS 資源。AD Connector 無法與 RDS SQL Server 相容。

您也可以使用 AD Connector，透過將應用程式使用者連線到現有的 RADIUS 型 MFA 基礎設施，為 AWS 應用程式使用者啟用多重驗證 (MFA)。當使用者存取 AWS 應用程式時，這可多提供一層安全保護。

使用 AD Connector，您可以繼續像現在Active Directory一樣管理 。例如，您可以使用內部部署 中的標準Active Directory管理工具來新增使用者和群組，並更新密碼Active Directory。這可協助您持續強制執行安全政策，例如密碼過期、密碼歷史記錄和帳戶鎖定，無論使用者是在內部部署或 AWS 雲端中存取資源。

使用情況

當您想要將現有的內部部署目錄與相容的 AWS 服務搭配使用時，AD Connector 是您的最佳選擇。如需詳細資訊，請參閱AD Connector。

Simple AD

Simple AD 是由 Samba 4 提供支援 AWS Directory Service 的MicrosoftActive Directory相容目錄。Simple AD 支援基本Active Directory功能，例如使用者帳戶、群組成員資格、加入 Linux 網域或 Windows 型 EC2 執行個體、Kerberos 型 SSO 和群組政策。 AWS 提供監控、每日快照和復原做為服務的一部分。

Simple AD 是獨立的雲端目錄，您可在目錄中建立和管理使用者身分與對應用程式的存取。您可以使用許多熟悉Active Directory的應用程式和工具，這些應用程式和工具需要基本Active Directory功能。Simple AD 與下列 AWS 應用程式相容：Amazon WorkSpaces、Amazon WorkDocs、Amazon QuickSight 和 Amazon WorkMail。您也可以 AWS Management Console 使用 Simple AD 使用者帳戶登入 ，並管理 AWS 資源。

Simple AD 不支援多重要素驗證 (MFA)、信任關係、DNS 動態更新、結構描述延伸、透過 LDAPS 的通訊、PowerShell AD cmdlets 或 FSMO 角色傳輸。Simple AD 無法與 RDS SQL Server 相

容。需要實際 Microsoft 功能的客戶Active Directory，或將目錄與 RDS SQL Server 搭配使用的客戶，應該改用 AWS Managed Microsoft AD。請確認在您使用 Simple AD 前，您的必要應用程式與 Samba 4 完全相容。如需詳細資訊，請參閱 https://www.samba.org。

使用情況

您可以使用 Simple AD 做為雲端中的獨立目錄，以支援需要基本Active Directory功能的Windows工作負載、相容的 AWS 應用程式，或支援需要 LDAP 服務的 Linux 工作負載。如需詳細資訊，請參閱Simple AD。

如需每個區域支援的目錄類型清單，請參閱 的區域可用性 AWS Directory Service 。

該選擇哪種

您可以選擇功能和可擴展性最符合您需求的目錄服務。使用下表協助您判斷哪個 AWS Directory Service 目錄選項最適合您的組織。

您需要執行什麼作業？	建議 AWS Directory Service 選項
我的雲端應用程式需要 Active Directory或 LDAP	如果您需要支援Active Directory感知工作負載的 雲端 MicrosoftActive Directory中的 AWS 實際 ，或 AWS Amazon WorkSpaces 和 Amazon QuickSight 等應用程式和服務，或需要 Linux 應用程式的 LDAP 支援，請使用 AWS Directory Service for Microsoft Active Directory (Standard Edition 或 Enterprise Edition)。 使用 AWS Directory Service for Microsoft Active Directory （混合版本）將現有的自我管理 AD 擴展到 AWS 雲端 AWS Directory Service 如果您只需要允許現場部署使用者使用其Active Directory登入資料登入 AWS 應用程式和服務，請使用 AD Connector 。您也可以使用 AD Connector 將 Amazon EC2 執行個體加入現有的Active Directory網域。 如果您需要具有支援 Samba 4 相容應用程式之基本Active Directory相容性的低規模、低成本目錄，或需要 LDAP 感知應用程式的 LDAP 相容，請使用 Simple AD。

您需要執行什麼作業？	建議 AWS Directory Service 選項
我開發 SaaS 應用程式	如果您開發大規模的 SaaS 應用程式，並需要使用具可擴展性的目錄管理和驗證您的訂閱者，且可搭配社交媒體身分運作，請使用 Amazon Cognito。

如需 AWS Directory Service 目錄選項的詳細資訊，請參閱如何選擇 Active Directory解決方案 AWS。

使用 Amazon EC2

了解 Amazon EC2 的基本概念對於使用 AWS Directory Service非常重要。建議您一開始先閱讀下列主題：

- Amazon EC2 使用者指南》中的什麼是 Amazon EC2？。
- 《Amazon EC2 使用者指南》中的啟動 Amazon EC2 執行個體。 Amazon EC2
- 《Amazon EC2 使用者指南》中的 EC2 執行個體的 Amazon EC2 安全群組。 Amazon EC2
- 《Amazon VPC 使用者指南》中的什麼是 Amazon VPC 一節。
- 《Amazon VPC 使用者指南》中的使用 將您的 VPC 連線到遠端網路 AWS Virtual Private Network。

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory，也稱為 AWS Managed Microsoft AD，執行Microsoft Active Directory為採用 Windows Server 2019 技術的受管服務。它會跨不同可用區域在您的Amazon VPC 中建立一對高可用性的網域控制站，並 AWS 自動管理主機監控、復原、資料複寫、快照和軟體更新。此服務可讓您執行目錄感知工作負載、管理使用者和群組、提供單一登入、建立和套用群組政策，以及安全地連線至 Amazon EC2 執行個體。

AWS Directory Service 提供兩種Microsoft Active Directory解決方案： AWS Directory Service for Microsoft Active Directory 在 AWS 雲端中提供全受管Active Directory服務，而 AWS Managed Microsoft AD （混合版本） 會將您現有的自我管理 AD 延伸到 AWS。

AWS Managed Microsoft AD (Standard Edition 和 Enterprise Edition) 建立新的受管 AD 網域，以管理其上的使用者、裝置和電腦 AWS。這些目錄會建立資源樹系，以在內部部署、 AWS或多雲端環境中建立與現有 AD 網域的信任關係。使用者可以使用其現有登入資料，從目前的 AD 網域存取 AWS 資源。使用者身分會保留在現有的 AD 網域中，而資源樹系會管理您的 AWS 資源，在環境之間維持操作隔離，同時提供無縫的單一登入。

AWS Managed Microsoft AD （混合版本） 會將自我管理的 Active Directory 與 AWS Directory Service for Microsoft Active Directory 連線，建立跨越基礎設施和 的整合身分環境 AWS 雲端。此解決方案可將目錄服務擴展至 ， AWS 而無需同步使用者身分、在環境之間建立信任關係，並使用現有的登入資料提供無縫存取。

使用 AWS Managed Microsoft AD，您可以在 AWS 雲端中執行目錄感知工作負載，包括MicrosoftSharePoint和自訂 .NET 和 SQL Server 型應用程式。您也可以設定 AWS Managed Microsoft AD 與現有自我管理 Microsoft 之間的信任關係Active Directory，讓使用者和群組使用 存取任一網域中的資源 AWS IAM Identity Center。

該選擇哪種

您可以選擇兩種具有最符合您需求的功能和可擴展性 AWS Directory Service 的服務。下表可協助您判斷哪個 AWS Directory Service 選項最適合您的組織。

使用案例	建議的解決方案
執行需要 LDAP 支援的目錄感知工作負載、 AWS 應用程式或 Linux 應用程式	AWS Managed Microsoft AD (Standard Edition 和 Enterprise Edition) 建立新的受管 AD 網域，以管理其上的使用者、裝置和電腦 AWS。這些目錄會建立資源樹系，以

使用案例	建議的解決方案
	在內部部署、 AWS或多雲端環境中建立與現有 AD 網域的信任關係。使用者可以使用其現有登入資料，從目前的 AD 網域存取 AWS 資源。使用者身分會保留在現有的 AD 網域中，而資源樹系會管理您的 AWS 資源，在環境之間維持操作隔離，同時提供無縫的單一登入。
將現有 擴展Active Directory至 AWS	AWS Managed Microsoft AD （混合版本） 將您的自我管理 Active Directory 與 AWS Directory Service for Microsoft Active Directory 連線，建立跨越基礎設施和 的整合身分環境 AWS 雲端。此解決方案可將目錄服務擴展至 ， AWS 而無需同步使用者身分、在環境之間建立信任關係，並使用現有的登入資料提供無縫存取。

主題

- Managed AWS Microsoft AD 入門
- 了解 AWS Managed Microsoft AD （混合版本）

了解 AWS Managed Microsoft AD （混合版本）

AWS Managed Microsoft AD （混合版本） 可讓您 AWS 雲端 使用 AWS Managed Microsoft AD 將現有 擴展Active Directory至 。此功能可讓您更輕鬆地將 AD 相依工作負載移至 AWS、採用 AWS 服務，以及提高Active Directory備援。 AWS 將定期在混合目錄上執行目錄評估，您可以在 主控台中 AWS Directory Service 檢視這些評估。

中的混合目錄會將您現有的 Microsoft Active Directory 與 AWS Directory Service for Microsoft Active Directory (AWS 受管 Microsoft AD) AWS Directory Service 連線。這可建立跨內部部署 AWS和多雲端基礎設施的整合身分環境，讓您維護單一身分來源，同時將目錄服務延伸至 AWS。

混合目錄組態提供數種重要功能：

- 將自我管理 AD 延伸到 ， AWS 雲端 而不需要建立信任關係
- 使用現有Active Directory憑證跨環境進行無縫身分驗證和授權
- 跨 AD 環境的一致使用者登入資料和群組成員資格

- AD 存取政策和許可的集中管理

主題

- 混合目錄先決條件
- 建立混合目錄
- 檢視和編輯混合目錄
- 刪除混合目錄
- 混合目錄的目錄評估
- 對混合目錄和目錄評估進行故障診斷

混合目錄先決條件

混合目錄將您的自我管理 Active Directory 延伸到 AWS 雲端。在建立混合目錄之前，請確定您的環境符合下列要求：

Microsoft Active Directory 網域需求

在建立混合目錄之前，請確保您的自我管理 AD 環境和基礎設施符合下列要求，並收集必要的資訊。

網域需求

您的自我管理 AD 環境必須符合下列要求：

- 使用 Windows Server 2012 R2或 2016功能層級。
- 使用標準網域控制站來評估混合目錄的建立。唯讀網域控制站 (RODC) 無法用於建立混合目錄。
- 有兩個網域控制站，所有Active Directory服務都執行中。
- 主要網域控制站 (PDC) 必須隨時可路由。

  具體而言，自我管理 AD 的 PDC 模擬器和 RID 主 IPs 必須位於下列其中一個類別：

  - RFC1918 私有 IP 地址範圍的一部分 (10.0.0.0/8、172.16.0.0/12 或 192.168.0.0/16)
  - 在您的 VPC CIDR 範圍內
  - 比對 目錄自我管理執行個體的 DNS IPs

  您可以在建立混合目錄之後新增目錄的其他 IP 路由。

必要資訊

收集有關自我管理 AD 的下列資訊：

- 目錄 DNS 名稱
- 目錄 DNS IPs
- 具有自我管理 AD 管理員許可的服務帳戶憑證
- AWS 儲存服務帳戶登入資料的秘密 ARN （ 請參閱 AWS 混合目錄的秘密 ARN)

AWS 混合目錄的秘密 ARN

若要使用自我管理 AD 設定混合目錄，您需要建立 KMS 金鑰來加密 AWS 秘密，然後建立秘密本身。這兩個資源都必須在 AWS 帳戶 包含混合目錄的相同 中建立。

建立 KMS 金鑰

KMS 金鑰用於加密您的 AWS 秘密。

> **Important**
>
> 對於加密金鑰，請勿使用 AWS 預設 KMS 金鑰。請務必在相同 中建立 AWS KMS 金鑰 AWS 帳戶 ，其中包含您要建立以加入自我管理 AD 的混合目錄。

建立 AWS KMS 金鑰

1. 在 AWS KMS 主控台中，選擇建立金鑰。
2. 對於金鑰類型，選擇對稱。
3. 對於金鑰用途，選擇加密和解密。
4. 針對 Advanced options (進階選項)：
   a. 對於金鑰材料來源，選擇 KMS。
   b. 針對區域性，選擇單一區域金鑰，然後選擇下一步。
5. 對於別名，提供 KMS 金鑰的名稱。
6. (選用) 對於描述，提供 KMS 金鑰的描述。
7. （選用）針對標籤，新增 KMS 金鑰的標籤，然後選擇下一步。
8. 針對金鑰管理員，選取 IAM 使用者。

9. 針對金鑰刪除，請保留允許金鑰管理員刪除此金鑰的預設選擇，然後選擇下一步。
10. 對於金鑰使用者，從上一個步驟中選取相同的 IAM 使用者，然後選擇下一步。
11. 檢閱組態。
12. 針對金鑰政策，將下列陳述式新增至政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::caller-account:role/role_used_to_create_directory"
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
       "Sid": "Allow use of the KMS key on behalf of Directory Service",
       "Effect": "Allow",
       "Principal": {
         "Service": "ds.amazonaws.com"
       },
       "Action": "kms:Decrypt",
       "Resource": "*"
    }
  ]
}
```

13. 選擇 Finish (完成)。

建立 AWS 秘密

在 Secrets Manager 中建立秘密，以存放自我管理 AD 使用者帳戶的登入資料。

> **Important**
>
> 在包含您要與自我管理 AD 加入之混合目錄 AWS 帳戶 的相同 中建立秘密。

若要建立機密

- 在 Secrets Manager 中，選擇儲存新的秘密
- 針對秘密類型，選擇其他類型的秘密
- 對於金鑰/值對，新增兩個金鑰：

1. 新增使用者名稱金鑰
   a. 對於第一個金鑰，輸入 `customerAdAdminDomainUsername`。
   b. 對於第一個金鑰的值，請僅輸入 AD 使用者的使用者名稱（不含網域字首）。請勿包含網域名稱，因為這會導致執行個體建立失敗。
2. 新增密碼金鑰
   a. 對於第二個金鑰，輸入 `customerAdAdminDomainPassword`。
   b. 對於第二個金鑰的值，輸入您在網域上為 AD 使用者建立的密碼。

完成秘密組態

1. 針對加密金鑰，選取您在 中建立的 KMS 金鑰建立 KMS 金鑰，然後選擇下一步。
2. 針對秘密名稱，輸入秘密的描述。
3. （選用）針對描述，輸入秘密的描述。
4. 選擇下一步。
5. 對於設定輪換設定，保留預設值並選擇下一步。
6. 檢閱秘密的設定，然後選擇儲存。
7. 選擇您建立的秘密，然後複製秘密 ARN 的值。您將在下一個步驟中使用此 ARN 來設定自我管理 Active Directory。

基礎設施需求

準備下列基礎設施元件：

- 具有 SSM 代理程式管理員權限的兩個 AWS Systems Manager 節點
  - 如果您的 Active Directory 是在 外部自我管理 AWS 雲端，則混合多雲端環境將需要兩個 Systems Manager 節點。如需如何佈建這些節點的詳細資訊，請參閱為混合多雲端環境設定 Systems Manager。

- 如果您的 Active Directory 是在 內自我管理 AWS 雲端，您將需要兩個 Systems Manager 受管 EC2 執行個體。如需如何佈建這些執行個體的詳細資訊，請參閱使用 Systems Manager 管理 EC2 執行個體。

必要的 Active Directory 服務

確保您的自我管理 AD 上執行下列服務：

- Active Directory Domain Services
- Active Directory Web Service (ADWS)
- COM+ 事件系統
- 分散式檔案系統複寫 (DFSR)
- 網域名稱系統 (DNS)
- DNS 伺服器
- 群組政策用戶端
- 站台間傳訊
- 遠端程序呼叫 (RPC)
- 安全帳戶管理員
- Windows Time 伺服器

> **Note**
>
> 混合目錄需要同時開啟 UDP 連接埠 123，並啟用和運作 Windows Time Server。我們會與您的網域控制器同步時間，以確保混合目錄複寫正常運作。

Kerberos 身分驗證要求

您的使用者帳戶必須啟用 Kerberos 預先驗證。如需如何啟用此設定的詳細指示，請參閱確定已啟用 Kerberos 預先驗證。如需此設定的一般資訊，請前往 Microsoft TechNet 上的預先驗證。

支援的加密類型

透過 Kerberos 驗證Active Directory網域控制站時，混合目錄支援下列加密類型：

- AES-256-HMAC

網路連接埠需求

若要 AWS 讓 擴展自我管理Active Directory網域控制站，現有網路的防火牆必須CIDRs針對 Amazon VPC 中的兩個子網路，將下列連接埠開放給 ：

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 身分驗證
- UDP 123 - 時間伺服器
- TCP 135 - 遠端程序呼叫
- TCP/UDP 389 - LDAP
- TCP 445 - SMB
- TCP 636 - 僅適用於具有輕量型目錄存取通訊協定安全 (LDAPS) 的環境
- TCP 49152-65535 - RPC 隨機配置的高 TCP 連接埠
- TCP 3268 和 3269 - 全域目錄
- TCP 9389 Active Directory Web Services (ADWS)

這些是建立混合目錄所需的最小連接埠。您特定的組態可能需要開啟其他連接埠。

> **Note**
>
> 為您的網域控制站和 FSMO 角色持有者提供的 DNS IPs，必須對 Amazon VPC 中兩個子網路 CIDRs 開放上述連接埠。

> **Note**
>
> 混合目錄需要同時開啟 UDP 連接埠 123，並啟用和運作 Windows Time Server。我們會與您的網域控制器同步時間，以確保混合目錄複寫正常運作。

AWS 帳戶 許可

您將需要下列動作的許可 AWS 帳戶：

- ec2:AuthorizeSecurityGroupEgress

- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateNetworkInterface
- ec2：CreateSecurityGroup
- ec2:DescribeNetworkInterfaces
- ec2：DescribeSubnets
- ec2：DescribeVpcs
- ec2：CreateTags
- ec2:CreateNetworkInterfacePermission
- ssm:ListCommands
- ssm:GetCommandInvocation
- ssm:GetConnectionStatus
- ssm:SendCommand
- secretsmanager:DescribeSecret
- secretsmanager:GetSecretValue
- iam:GetRole
- iam：CreateServiceLinkedRole

Amazon VPC 網路需求

具有下列項目的 VPC：

- 至少兩個子網路。每個子網路都必須位於不同的可用區域
- VPC 必須具有預設租用

您不能使用 198.18.0.0/15 地址空間中的地址在 VPC 中建立混合目錄。

AWS Directory Service 使用兩個 VPC 結構。組成目錄的 EC2 執行個體會在您的 外部執行 AWS 帳戶，並由 管理 AWS。其使用兩種網路轉接器，ETH0 和 ETH1。ETH0 是管理轉接器，而且位於您的帳戶外部。ETH1 則是建立於您的帳戶內部。

目錄的 ETH0 網路管理 IP 範圍為 198.18.0.0/15。

如需詳細資訊，請參閱 Amazon VPC 使用者指南 中的下列主題：

- 「什麼是 Amazon VPC？」
- 「什麼是 Amazon VPC？」
- VPCs和子網路
- 什麼是 AWS Site-to-Site VPN？

如需詳細資訊 AWS Direct Connect，請參閱什麼是 AWS Direct Connect？

AWS 安全群組組態

根據預設， 會 AWS 連接安全群組，以允許網路存取 VPC AWS Systems Manager 中的受管節點。您可以選擇性地提供自己的安全群組，允許網路流量往返 VPC 外部的自我管理網域控制站。

您可以選擇性地提供自己的安全群組，允許網路流量往返 VPC 外部的自我管理網域控制站。如果您提供自己的安全群組，則需要：

- 允許列出您的VPC CIDR範圍和自我管理的範圍。
- 確保這些範圍不會與AWS 預留 IP 範圍重疊

目錄評估考量事項

以下是建立目錄評估和您可以在 中擁有的評估數量時的考量 AWS 帳戶：

- 當您建立混合目錄時，會自動建立目錄評估。評估有兩種類型： CUSTOMER和 SYSTEM。您的 AWS 帳戶 有 100 個CUSTOMER目錄評估的限制。
- 如果您嘗試建立混合目錄，並且已經有 100 個CUSTOMER目錄評估，則您會遇到錯誤。刪除評估以釋放容量，然後再試一次。
- 您可以聯絡 支援 或刪除現有的 CUSTOMER CUSTOMER目錄評估以釋放容量，請求提高目錄評估配額。

建立混合目錄

建立混合目錄之前，您必須建立並成功傳遞目錄評估，以驗證與自我管理 Active Directory 的連線能力和互通性

使用自我管理 AD 建立混合目錄

請依照下列步驟，使用自我管理 AD 建立混合目錄：

建立混合目錄

1. 開啟所需區域的 AWS Directory Service 主控台。
2. 在選取目錄類型頁面上，選擇 AWS Managed Microsoft AD。
3. 在 AWS Managed Microsoft AD 入門下，選取使用混合目錄擴展 AD 網域 - 新目錄，然後選擇下一步。這會引導您前往建立目錄評估頁面。
4. 您必須先建立並成功通過目錄評估，才能建立混合目錄。若要建立目錄評估，請遵循中的步驟建立目錄評估。成功通過目錄評估後，您可以繼續此程序。
5. 成功通過目錄評估後，請導覽至目錄頁面。
6. 在目錄頁面的試驗混合目錄評估下，選擇狀態為 的評估 IDSUCCESS。然後選取建立混合目錄，以引導您前往評估詳細資訊頁面
7. 在評估詳細資訊頁面上，選取建立混合目錄來確認此動作，這會開啟使用 assessment-id 建立混合目錄頁面。
8. 在使用 assessment-id 建立混合目錄頁面上，檢閱自我管理 Active Directory 資訊。確認資訊後，選取建立混合目錄。

   選擇建立混合目錄後， 會根據此資訊 AWS 執行另一個目錄評估，以確認您的自我管理 AD 組態仍然有效。如果目錄評估成功通過，我們會建立混合目錄。
9. 選擇建立混合目錄會返回目錄頁面。

   a. 成功建立混合目錄後，會出現綠色橫幅。

   b. 如果混合目錄建立失敗，會出現紅色橫幅。完成下列動作以清除混合目錄建立失敗：

      1. 在 主控台中刪除失敗的混合目錄。
      2. 刪除自我管理 AD 中任何剩餘的 AWS 預留 OUs。

   其他資訊

   - 刪除混合目錄
   - 故障診斷

檢視和編輯混合目錄

使用下列程序來檢視或編輯您的混合目錄。

檢視混合目錄

您可以在 AWS Directory Service 主控台中檢視混合目錄。

檢視詳細目錄資訊

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 選擇您目錄的目錄 ID 連結。目錄詳細資訊頁面上會顯示目錄的相關資訊。

自我管理 Active Directory 資訊

本節提供已加入 AWS 基礎設施之自我管理 Active Directory 的相關資訊。

- 目錄類型
- 目錄 ID
- 目錄狀態
- 自我管理 AD 的網路詳細資訊，例如：
  - VPC
  - 子網路
  - DNS 地址
- Systems Manager 受管節點

混合目錄索引標籤

您可以找到有關 AWS Managed Microsoft AD 的下列資訊：

- 在共用與共用索引標籤上，您可以與其他 AWS 帳戶共用 AWS Managed Microsoft AD，並檢視網域控制站的網路詳細資訊。
- 在應用程式管理索引標籤上，您可以為 AWS Managed Microsoft AD 啟用應用程式存取 URL，並為 AWS Managed Microsoft AD 啟用 AWS 應用程式和服務。
- 在維護索引標籤上，您可以讓 SNS 接收 AWS Managed Microsoft AD 狀態的通知，並檢閱 AWS Managed Microsoft AD 的快照。
- 如需 Status (狀態) 欄位的詳細資訊，請參閱「了解 AWS Managed Microsoft AD 目錄狀態」。

更新混合目錄

您可以在 AWS Directory Service 主控台中更新混合目錄，以修改 DNS 設定或復原管理員帳戶存取權。

更新混合目錄資訊

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 選擇目錄的目錄 ID 連結，以開啟目錄詳細資訊頁面。
3. 選擇動作，然後選擇更新混合目錄資訊。
4. 在更新混合目錄資訊頁面上，您可以更新 DNS 設定或復原管理員帳戶。

   更新 DNS 設定 （選用）

   在自我管理 Active Directory 資訊下，您可以變更下列項目：

   a. 目錄 DNS 名稱

   b. DNS IP 地址

   您可以一起或個別更新這兩個設定。更新程序至少需要變更一次。
5. 復原混合目錄管理員帳戶

   若要復原您的混合目錄管理員帳戶，我們需要暫時存取使用者。此存取權是透過 Secrets Manager 的秘密提供。在復原期間，我們只會使用這些登入資料一次，而不會存放這些登入資料。如果您的混合目錄管理員帳戶存在，即使您更新了自我管理的 Active Directory 管理員使用者，也不需要更新此秘密。

   - 管理員登入資料秘密 – 我們在建立混合目錄時建立混合目錄管理員帳戶。如果您刪除此秘密，請輸入自我管理 AD 管理員使用者的 Secrets Manager 秘密。

刪除混合目錄

當您刪除混合目錄時，所有目錄資料和快照都會遭到刪除且無法復原。刪除目錄之後，所有加入目錄的執行個體都會保持不變。不過，您無法使用目錄登入資料來登入這些執行個體。您必須使用本機使用者帳戶登入這些執行個體。

刪除目錄

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。確保您位於部署 AWS 區域 混合目錄的中。如需詳細資訊，請參閱選擇區域。
2. 確定您要刪除的目錄未啟用 AWS 任何應用程式。啟用 AWS 的應用程式將阻止您刪除混合目錄。
3. 在 Directories (目錄) 頁面中，選擇目錄 ID。
4. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。在AWS 應用程式和服務區段中，您會看到您的目錄已啟用哪些 AWS 應用程式。

   a. 停用 AWS Management Console 存取。如需詳細資訊，請參閱停用 AWS 管理主控台存取。

   b. 若要停用 Amazon FSx for Windows File Server，您必須從域中移除 Amazon FSx 檔案系統。如需詳細資訊，請參閱《Amazon FSx for Windows File Server 使用者指南》中的在 FSx for Windows File Server 中使用 Active Directory 一節。

   c. 若要停用 Amazon Relational Database Service，您必須從域中移除 Amazon RDS 執行個體。如需詳細資訊，請參閱《Amazon RDS 使用者指南》中的管理域中的資料庫執行個體一節。
5. 在導覽窗格中，選擇目錄。
6. 僅選取要刪除的目錄，然後選擇刪除。刪除目錄需要幾分鐘的時間。刪除目錄之後，該目錄會從您的目錄清單中移除。
7. 手動刪除任何剩餘的網域控制器物件，包括任何 AWS 預留 OUs。您可以刪除整個 AWS 預留目錄，以完成環境的清除。

混合目錄的目錄評估

目錄評估會檢查您的自我管理 Active Directory 環境，以確保其符合建立混合目錄的要求。此評估會驗證網路連線能力、網域控制站組態和所需的服務，以協助在建立自我管理 AD 和 之間的連線之前識別和解決潛在問題 AWS Directory Service。

目錄評估有兩種類型：

- *CUSTOMER* 評估 – 在您開始設定混合目錄時，由您在 主控台中啟動。即使客戶目錄評估正在進行，您也可以將其刪除。您最多可以有 100 個客戶評估。
- *SYSTEM* 評估 – 由 自動建立 AWS ，並在成功建立後定期執行。您無法刪除SYSTEM評估。

目錄評估可提供有關環境整備度的寶貴資訊，包括：

- 自我管理 AD 與 之間的連線 AWS
- 網域控制站上所需服務的可用性
- 與 AWS Directory Service 需求的組態相容性
- 可能無法成功建立混合目錄的潛在問題

您必須先成功（通過）目錄評估，才能建立混合目錄。如果評估失敗，您可以檢視詳細報告來識別和解決問題，然後再重試。 會在 30 天後 AWS 刪除SYSTEM評估。

主題

- 建立目錄評估
- 檢視目錄評估
- 刪除目錄評估

建立目錄評估

您可以在建立混合目錄時建立目錄評估，也可以手動建立一個評估。若要手動建立評估，請開啟位於 https：//https://console.aws.amazon.com/directoryservicev2/ 的 AWS Directory Service 主控台。在目錄頁面的目錄評估區段下，選擇建立評估。

建立目錄評估

1. 在建立目錄評估頁面上，針對目錄 DNS 名稱，輸入您的自我管理 Active Directory DNS 名稱。
2. 針對 DNS IP 地址，輸入自我管理 AD 的兩個 DNS IP 地址。
3. 混合目錄需要至少有兩個子網路的 Amazon VPC。如果您還沒有這些項目，您可以建立它們。在聯網區段中，提供下列項目：
    a. 針對 VPC，選擇您的 VPC 識別符。
    b. 針對子網路，為每個兩個子網路選擇識別符。每個子網路必須位於不同的可用區域。如需詳細資訊，請參閱Amazon VPC 網路需求。
    c. 針對安全群組，選擇安全群組識別符。根據預設， 會 AWS 連接安全群組，以允許網路存取 Amazon VPC 中的 AWS Secrets Manager 受管節點。您可以選擇性地提供自己的安全群組，允許網路流量進出 Amazon VPC 外部的自我管理網域控制站。
4. 在AWS Systems Manager 節點區段中，根據下列需求選擇兩個 Systems Manager 節點或執行個體：

- 如果您的 Active Directory 是在 外部自我管理 AWS 雲端，則混合多雲端環境將需要兩個 Systems Manager 節點。如需如何佈建這些節點的詳細資訊，請參閱為混合多雲端環境設定 Systems Manager。
- 如果您的 Active Directory 是在 內自我管理 AWS 雲端，您將需要兩個 Systems Manager 受管 EC2 執行個體。如需如何佈建這些執行個體的詳細資訊，請參閱使用 Systems Manager 管理 EC2 執行個體。

5. 選擇下一步以開啟檢閱和建立目錄評估頁面。
6. 在檢閱和建立目錄評估頁面上，檢閱目錄評估資訊並進行任何必要的變更。當資訊正確時，選擇建立評估。建立目錄評估大約需要 30 分鐘。您會返回目錄詳細資訊頁面。當目錄評估成功時，會出現綠色橫幅。

> **Warning**
>
> 若要建立混合目錄，目錄評估必須進入 SUCCESS 狀態。您必須先成功通過目錄評估，才能建立混合目錄。

檢視目錄評估

您可以在 中檢視目錄評估 AWS Management Console ，以檢閱評估結果並管理您的評估報告。

檢視目錄評估

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 在目錄頁面的試用混合目錄評估區段下，選擇您要檢視的評估。這會開啟評估詳細資訊頁面。
3. 在評估詳細資訊頁面上，您可以選擇：
   - 下載 以將目錄評估報告下載為 CSV 檔案。
   - 刪除 以刪除目錄評估報告。
   - 建立評估以建立新的目錄評估。
4. 從評估詳細資訊頁面，您可以檢視下列資訊：
   a. 評估資訊，例如評估 ID、狀態、是否由客戶或系統建立，以及上次更新的時間。
   b. 自我管理 AD 詳細資訊，例如 DNS 名稱、VPC 和子網路。

c. AWS Systems Manager 受管節點資訊，例如 IP 地址、評估狀態，以及通過和失敗的評估測試數量。

d. 網域控制站的評估狀態。您也可以選擇網域控制站來檢閱評估測試詳細資訊。錯誤代碼會出現在失敗評估測試的狀態欄中。

刪除目錄評估

您可以在 中刪除客戶建立的目錄評估 AWS Management Console。您無法刪除 自動 AWS 建立的系統啟動評估。

刪除客戶目錄評估

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 在目錄頁面的目錄評估區段下，選擇您要刪除的客戶評估。或者，您可以選擇要刪除的目錄評估旁的核取方塊，然後從動作功能表中選擇刪除。
3. 系統會將您導向至評估詳細資訊頁面。選擇動作，然後選擇刪除評估。隨即出現刪除目錄評估對話方塊。選擇刪除。

對混合目錄和目錄評估進行故障診斷

需要目錄評估才能建立混合目錄。評估測試會在每個網域控制器上執行。評估測試會檢查不同的區域，並導致通過或失敗狀態。如果您的目錄評估失敗，您可以檢視網域控制站的評估測試，以識別導致失敗的問題。

> **Important**
>
> 當目錄評估的狀態通過並顯示警告時，可以建立混合目錄。我們建議您在建立混合目錄之前解決造成警告的問題

主題

- 故障診斷失敗的混合目錄評估
- 目錄狀態錯誤
- 目錄評估錯誤訊息
- 評估測試錯誤訊息

- 評估測試警告訊息

故障診斷失敗的混合目錄評估

您可以從 中的目錄頁面對失敗的目錄評估進行故障診斷 AWS Management Console。

1. 登入 AWS Management Console 並在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 在目錄評估區段下，選取失敗的混合目錄評估。
3. 在評估詳細資訊頁面上，檢閱目錄評估並識別哪些 test(s) 失敗。
   - 網域控制站的評估測試將提供有關哪些測試成功或失敗的詳細資訊。狀態欄提供失敗測試原因的更多詳細資訊。若要檢視網域控制站的評估測試，請參閱 檢視目錄評估。
4. 解決造成自我管理Active Directory或 AWS Managed Microsoft AD 失敗的問題。如需詳細資訊，請參閱 目錄評估錯誤訊息 和 評估測試錯誤訊息。
5. 在 AWS Directory Service 主控台中返回失敗的評估。在紅色警告訊息中選擇建立評估。使用自我管理 AD 建立混合目錄 如需建立目錄評估的詳細資訊，請參閱 。

目錄狀態錯誤

AWS Directory Service 目錄可能會遇到各種狀態，指出不同類型的問題。了解這些狀態可協助您判斷適當的疑難排解步驟。

目錄狀態類型

狀態	描述	需執行的動作
作用中	目錄建立已成功完成，且正常運作。	不需要採取行動。
Impaired (受損)	目錄已成功建立，但網域控制站之後遇到問題。系統會嘗試自動復原。	監控目錄狀態。如果問題仍然存在，請聯絡 AWS Support。
失敗	目錄建立失敗且無法復原。	刪除失敗的目錄並建立新的目錄。
無法運作 （僅限 Hybrid AD)	AWS 偵測到安全問題，並自動隔離目錄以進行保護。在還原之前，目錄會變成完全無法使用。	AWS 支援 聯絡中心。此狀態需要 支援 介入才能調查和還原目錄。

目錄評估錯誤訊息

若要建立混合目錄，您需要傳遞目錄評估。目錄評估可能會因各種原因而失敗。

下表顯示目錄評估錯誤訊息，以及如何解決這些錯誤訊息。

目錄評估錯誤訊息和解決方案

目錄評估錯誤訊息	Resolution
此評估在兩個受管執行個體上都未通過多項測試。透過選取每個受管執行個體，並在您的內部部署目錄中解決它們，來調查失敗的測試。然後，建立新的評估。	自我管理 AD 的一個或多個目錄評估測試失敗。如需特定測試失敗及其解決方法的詳細資訊，評估測試錯誤訊息請參閱 。
由於內部服務例外狀況，此評估失敗。請建立新的評估或聯絡 服務進行故障診斷，然後重試。	嘗試建立新的目錄評估。如果您持續遇到此錯誤，請聯絡 支援。
由於缺少執行 ec2:CreateSecurityGroup 、、ec2:DeleteSecurityGroup 、ec2:CreateNetworkInterface 、 ec2:DeleteNetworkInterface 和 等動作的許可ec2:DescribeSubnets ，此評估失敗ec2:DescribeNetworkInterface 。	若要建立目錄評估，您的 AWS 帳戶 需要必要的 AWS 帳戶 許可。
由於缺少執行 ssm:GetConnectionStatus 、、ssm:GetCommandInvocation 、 等動作的許可ssm:ListCommands ，此評估失敗ssm:SendCommand 。	若要建立目錄評估，您需要兩個具有必要 的 Systems Manager 節點AWS 帳戶 許可。
此評估失敗，因為您已達到可建立的網路介面數量限制。如需詳細資訊，請參閱 Amazon VPC 配額。	若要建立目錄評估，您必須建立網路介面和安全群組。您可以建立的 VPC 資源數量有限制，但您可以調整其中一些限制。如需詳細資訊，請參閱 Amazon VPC 配額。

目錄評估錯誤訊息	Resolution
此評估失敗，因為您已達到您可以建立或指派給執行個體的安全群組數量限制。如需詳細資訊，請參閱 Amazon VPC 配額。	若要建立目錄評估，您必須建立網路介面和安全群組。您可以建立的 VPC 資源數量有限制，但您可以調整其中一些限制。如需詳細資訊，請參閱 Amazon VPC 配額。
此評估失敗。無法從 連線至客戶執行個體 AWS Systems Manager。	若要建立目錄評估，您將需要兩個具有連線狀態的 AWS Systems Manager 節點。請參閱對 SSM Agent 進行故障診斷。
此評估未通過多項關鍵測試。透過選取每個受管執行個體並在您的內部部署目錄中解決它們，調查失敗的測試。然後，建立新的評估。	自我管理 AD 的一個或多個目錄評估測試失敗。如需詳細資訊，評估測試錯誤訊息請參閱 。

評估測試錯誤訊息

下表說明評估測試期間可能發生的錯誤訊息。這些錯誤表示封鎖在繼續混合目錄設定之前必須解決的問題。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
Active Directory Services 測試	testActiveDirectoryServices	AD_CRITICAL_SERVICES_NOT_RUNNING	Critical AD Services: [service_list] not running on hostname.	如果所需的AD服務未在自我管理 AD 中執行，便會發生。	特定必要AD服務必須在自我管理 AD 中執行。如需詳細資訊，請參閱必要的 Active Directory 服務。
Active Directory Services 測試	testActiveDirectoryServices	DOMAIN_CONTROLLER_NOT_FOUND	No domain controllers found for testActiveDirectoryServices.	Occurs if your self-managed AD domain controllers could not be both detected	確保您的自我管理 AD 網域控制站是可操作的，並且可以到達。驗證自我管理 AD 網域控制器的網路連線能力和DNS解析度。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
				and queried during AD service validation.	
AD 密碼政策測試	testPasswordPolicies	PASSWORD_POLICY_VIOLATIONS	*ErrorMessage*	如果您的自我管理 AD 密碼政策不符合 AWS Managed Microsoft AD 要求，便會發生。	您的自我管理 AD 密碼政策必須符合 AWS Managed Microsoft AD 密碼要求。如需詳細資訊，請參閱了解 AWS Managed Microsoft AD 密碼政策。
AWS 管理員使用者存在測試	testAwsAdminUserExist	ADMINISTRATOR_ACCOUNT_MISSING	AWS Admin user not found or invalid.	如果混合目錄管理員使用者不存在於自我管理 AD OU的 AWS 預留中，則會顯示此訊息。	確保混合目錄管理員使用者存在於自我管理 AD OU的預留中 AWS 。如果使用者遺失，請確認帳戶已在混合目錄設定程序期間正確建立。更新混合目錄。如果您的混合目錄狀態無法運作，請聯絡 支援。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
AWS 管理員使用者SPN測試	testNoSpnOnAwsAdminAccount	SPN_FOUND_ON_AWS_ADMIN	Found *spnCount* Service Principal Names (SPNs) set on AWS admin user *Username*. Please remove all SPNs from this account.	如果混合目錄管理員使用者在自我管理 AD 上SPNs設定了任何 ，就會發生。	從 AWS 混合目錄管理員使用者帳戶中移除所有服務主體名稱 (SPNs)。混合目錄管理員使用者不得SPNs設定任何 ，因為它們可能會干擾混合目錄身分驗證。
AWS 網域控制站非FSMO擁有者測試	testAwsDcNotFsmoOwner	AWS_DC_HOLDS_FSMO_ROLE	AWS Domain Controller owns FSMO roles: *rolesList* . Please remove these roles.	如果您將FSMO角色 (PDC Emulator、RID Master或Infrastructure Master) 從自我管理 AD 轉移到混合目錄網域控制站，則會顯示此訊息。	在繼續之前，將所有FSMO角色 (PDC Emulator、RID Master、Infrastructure Master) 傳輸回自我管理的 AD 網域控制站。如需詳細資訊，請參閱Microsoft傳輸FSMO角色的文件。
AWS 預留群組成員資格測試	testValidateAwsReservedGroupMembership	AWS_RESERVED_OU_NOT_FOUND	AWS Reserved OU not found.	如果自我管理 AD OU上的 AWS 預留不存在，便會發生。	AWS 預留OU必須存在於自我管理 AD 上，才能驗證群組成員資格。請聯絡 支援。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
AWS 預留群組成員資格測試	testValidateAwsReservedGroupMembership	GROUP_MEMBERSHIP_MISMATCH	AWS Reserved OU Group [GroupNameA]: Missing User(s) [Object1], [Object2] and Extra user(s) [Object3].	如果自我管理 AD OU上 AWS 預留的 中的群組包含未經授權的使用者，便會發生。	從自我管理 AD 的 AWS 預留OU 群組中移除任何未經授權的使用者。
AWS 預留 OUACLs 測試	testReservedOuAclsPermissions	RESERVED_OU_NON_COMPLIANT_AC	AWS Reserved OU ACLs permissions are invalid.	如果自我管理 AD OUACLs上的 AWS 預留不會為非AWS 實體強制執行唯讀許可，也不會防止未經授權存取 AWS受管資源，就會發生。	檢閱並更正自我管理 AD OUACLs上 AWS 預留的許可。確定非AWS 實體只有讀取許可 (ListChildren 、ReadProperty 、ListObject 、GenericRead 、、Synchronize)ReadControl ，並移除任何過多的許可。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
AWS 預留 OUGPO 關聯測試	testReservedOuGPOs	AWS_RESERVED_OU_NON_RESERVED_GPO_FOUND	Found non-AWS GPOs attached to the AWS Reserved OU: AWS Reserved OU (*count* unauthorized). Allowed GPOs: [*allowedAwsGpos*]. Domain Controllers OU (*count* unauthorized). Allowed GPOs: [*allowedDcGpos*]. Please, remove extra GPOs from the AWS Reserved OU.	如果自我管理 AD OU上的 AWS 預留OU和網域控制器連結至未經授權的 ，便會發生 GPOs。	（只有 AWS 受管群組政策物件 (GPOs) 可以連結至這些 OUs。移除任何未經授權的GPOs連結至 OU自我管理 AD 上的 AWS 預留 OU和網域控制站。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
AWS 預留OU資源測試	testAwsReservedOUResources	AWS_RESERVED_OU_NOT_FOUND	The AWS Reserved OU does not exist. Please contact AWS Support.	如果自我管理 AD 中OU不存在 AWS Managed Microsoft AD 目錄功能所需的 AWS 預留，則會顯示此訊息。	AWS 預留OU必須在混合目錄設定期間自動建立，不應刪除。如果此錯誤仍然存在，請聯絡 支援。
AWS 預留OU資源測試	testAwsReservedOUResources	AWS_RESERVED_OU_RESOURCES_MISMATCH	The following required resources are missing from AWS Reserved OU - Objects: *missing objects*, GPOs: *missing GPOs*. The following resources should not exist but were found in AWS Reserved OU: Objects: *unexpected objects* , GPOs: *unexpected GPOs*	如果在自我管理 AD 上OU建立的 AWS 預留不包含必要的物件，並GPOs用於適當的混合目錄操作，就會發生。	確保沒有人編輯 AWS 預留 OU。它必須包含必要的 AWS受管資源。移除任何未經授權的物件或 GPOs，如果缺少必要的資源支援，請聯絡 。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
AWS 預留OU測試	testCleanAwsReservedOU	AWS_RESERVED_RESOURCES_STILL_EXIST	AWS Reserved OU or AWS Reserved GPO still exists, please delete.	如果在自我管理 AD 上找到先前混合目錄設定的 AWS 預留資源仍然存在，則會顯示此訊息。	從主控台刪除現有的失敗混合目錄。然後 GPOs，從您的自我管理 AD 刪除任何 AWS 預留OU和相關 ，再繼續。
Bridgehead 命名內容測試	testBridgeheadNamingContext	NAMING_CONTEXT_INCONSISTENT	*failureDetails*	如果使用 的網站之間的自我管理 AD 複寫Bridgehead未如預期運作，則會發生此狀況。如果站台之間的命名內容未同步，也可能發生這種情況。	您的自我管理 AD bridgehead網站必須成功。您可以使用 進一步診斷：repadmin /bridgeheads / verbose。繼續之前，請先解決該評估的問題。
子網域測試	testChildDomain	CHILD_DOMAIN_NOT_SUPPORTED	Child Domains are not supported for Hybrid Directory.	如果您的自我管理 AD 樹系包含 AWS 受管 Microsoft AD 目錄不支援的子網域，則會發生這種情況。	AWS Managed Microsoft AD 目錄不支援子網域。您必須使用自我管理 AD 的單一網域樹系。如需詳細資訊，請參閱Microsoft Active Directory 網域需求。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
DcDiag 測試	testDcDiag	DCDIAG_TEST_FAILED	DCDiag test failed due to issue from [*formatedFailedTests*].	如果自我管理 AD 上有任何MicrosoftDCDiag測試失敗，就會發生。	AWS 使用DCDiag測試您的自我管理 AD。如果發生錯誤，您無法建立混合目錄。如需詳細資訊，請參閱Microsoft 文件。
DNS IP 比對測試	testDnsIpMatch	DNS_IP_MISMATCH	DNS IP address does not match expected IP addresses.	如果自我管理 AD 提供的 DNS IP 地址與使用 啟用的自我管理 AD 網域控制站上的 DNS IP 地址不相符，便會發生 AWS Systems Manager。	提供正確的 DNS IP 地址。
DNS 名稱比對測試	testDnsNameMatch	DOMAIN_DNS_NAME_MISMATCH	DNS name does not match expected domain name.	如果為自我管理 AD 提供DNS的名稱與啟用 的自我管理 AD 網域控制站上的DNS名稱不相符，就會發生 AWS Systems Manager。	提供正確的DNS名稱。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
DNS 記錄測試	testDnsRecords	DNS_RECORD_MISSING	Unable to resolve the following DNS queries: [*missingRecordsString*].	如果未針對類型 A、SOA、 NS 和 設定Windows DNS記錄，SRV 而且可以查詢，則會顯示 。	必須設定地址 (A)、命名空間 (NS)、授權狀態 (SOA) 和服務記錄 (SRV) DNS 的記錄，並且可以查詢。如需詳細資訊，請參閱 Microsoft 文件。
網域樹系功能層級測試	testDomainForestFunctionalLevel	UNSUPPORTED_FUNCTIONAL_LEVEL	Detected unsupported domain functional level: *DomainFunctionalLevel* , we require minimum of *MinimumDomainMode* . Detected unsupported forest functional level: *ForestFunctionalLevel* , we require minimum of *MinimumForestMode* .	如果您的自我管理 AD 網域和樹系功能層級不符合最低要求，便會發生。	您的自我管理 AD 必須使用 Windows2012 R2或 2016 功能層級。如需詳細資訊，請參閱 Microsoft 文件。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
網域運作狀態測試	testOnPremDcNumber	DC_NUMBER_BELOW_LIMIT	On-Prem DC count is lower than required number. DC count is *NumberOfDc* , AWS required number is *DcMinimum* .	如果您的自我管理 AD 沒有所需的網域控制站數量下限，就會發生。	確保您的自我管理 AD 已啟用至少兩個網域控制站 AWS Systems Manager。如需詳細資訊，請參閱Microsoft Active Directory 網域需求。
現有網域測試	testDomainAlreadyJoined	DOMAIN_ALREADY_JOINED	Instance is already joined to a domain.	如果您的自我管理 AD 網域已加入現有的混合目錄，就會發生。	您的自我管理 AD 網域已加入現有的混合目錄。加入混合目錄的每個自我管理 AD 網域必須是唯一的 建立新的自我管理 AD 網域，或從加入它們的混合目錄組態中移除它。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
FSMO 連線測試	testFsmoConnectivity	FSMO_ROLE_HOLDER_NOT_ROUTABLE	(PDCEmulator Ip: 1.1.1.1, RIDMaster Ip: 1.1.1.1) is not in routable ranges: [2.2.0.0/16, 3.3.0.0/16, 4.4.0.0/16, 5.5.0.0/16, 6.6.0.0/16].	如果自我管理 AD 上的FSMO角色 PDC Emulator、和/或 RID Master IPs 無法路由，便會發生。	主要網域控制站 (PDC) 必須隨時可路由。特別是自我管理 AD 的 PDC Emulator和 RID Master IPs。如需詳細資訊，請參閱Microsoft Active Directory 網域需求。
FSMO 連線測試	testFsmoConnectivity	FSMO_ROLE_MISSING	FSMO role(s): [*missingRolesString*] missing or DNS Record not found.	如果您的自我管理 AD 網域控制站無法存取您的FSMO角色，就會發生。	自我管理 AD 中的 Flexible Single Master Operation (FSMO) 角色必須連線至自我管理 AD 網域控制站。如需詳細資訊，請參閱 Microsoft 文件。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
IP 衝突測試	testIpConflict	IP_RANGE_CONFLICT	Conflicting IP address detected: *ipOverlaps*	如果您的自我管理 AD IP 範圍與 AWS 預留範圍重疊，便會發生。	您的自我管理 AD 無法使用與預留 IP 範圍重疊的 AWS IP 地址範圍。如需詳細資訊，請參閱Microsoft Active Directory 網域需求。
Kerberos 測試	testKerberos	KERBEROS_AUTHENTICATION_FAILED	Unable to get kerberos TGT.	如果 Kerberos 未正確設定且正在使用中，則會顯示 。	Kerberos 必須在自我管理 AD 上啟用 。如需詳細資訊，請參閱 Microsoft 文件。
LDAP 連線測試	testLdapConnectivity	LDAP_TEST_FAILED	Unable to query LDAP with rootDSE call.	如果 LDAP 無法運作，便會發生 。	輕量型目錄存取通訊協定 (LDAP) 必須啟用並在自我管理 AD 上運作。如需詳細資訊，請參閱 Microsoft 文件。
不唯讀網域控制器進行測試 FSMO	testNotRodcForFsmo	FSMO_FOUND_ON_RODC	FSMO Role Found on RODC	如果您的自我管理 AD 網域控制站FSMO角色為 ，便會發生 RODC。	自我管理 AD 的網域控制站不得使用唯讀網域控制站 (RODC) Flexible Single Master Operation (FSMO) 角色。如需詳細資訊，請參閱 Microsoft 文件。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
唯讀網域控制站密碼複寫測試	testRodcPasswordReplication	RODC_REPLICATE_ADMIN_PASSWORD	ReadOnly Domain Controller password replication is not explicitly denied for following groups: [*missingGroupsString*].	如果 RODC具有複寫管理員密碼的許可，便會發生。	自我管理 AD RODC的 必須明確拒絕複寫 Admin 密碼的許可。如需詳細資訊，請參閱 Microsoft 文件。
唯讀網域控制站測試	testIsDCRodc	DC_READONLY_MODE	Provided Domain Controller is set to Read-Only mode.	如果您的自我管理 AD 網域控制站處於 ReadOnlyDC 模式，就會發生。	您的自我管理 AD 必須是讀寫網域控制站。如需網域控制器類型的詳細資訊，請參閱 Microsoft 文件。
遠端連接埠連線能力測試	testPortConnectivity	PORT_TEST_FAILED	Connection to *TargetDestination* failed for TCP ports [*failed TCP ports*]. UDP ports [*failed UDP ports*].	如果 AWS 子網路上的必要連接埠，且您的自我管理 AD 網域控制器未開啟，便會發生。	確保 AWS 子網路和自我管理 AD 之間開啟所有必要的連接埠。如需詳細資訊，請參閱網路連接埠需求。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
複寫測試	testReplication	REPLICATION_FAILED	Replication failed for [*failedDSAsString*].	如果您的自我管理 AD 網域控制站複寫失敗，便會發生。	您的自我管理 AD 網域控制站複寫狀態必須成功。如需詳細資訊，請參閱 Microsoft 文件。
SMBV1 測試	testSMBV1	INSECURE_SETTING_SMB	SMBv1 is enabled on the system.	如果自我管理 AD 目前正在使用 SMBv1進行身分驗證，便會發生。	SMBv1 已知不安全，且必須在自我管理 AD 上停用。如需詳細資訊，請參閱 Microsoft 文件。
SSM 使用者許可測試	testSSMUserPermissions	INSUFFICIENT_PERMISSIONS	Systems Manager user does not have required elevated privileges.	如果 使用 Windows的使用者SSM權限不足，就會發生。	您需要自我管理 AD 上 AWS System Manager (SSM) 代理程式的Windows管理員許可。如需詳細資訊，請參閱AWS 帳戶 許可。
Sysvol 複寫測試	testSysvolReplication	DFSR_FAILURE_DETECTED	Failed DFSR event logs: *failedLogsString* .	如果您的自我管理 AD 沒有正確的sysvol複寫方法 (DFSR)，且複DFSR寫事件期間有任何DCs失敗，就會發生。	您的自我管理 AD sysvol複寫方法 (DFSR) 必須成功。如需詳細資訊，請參閱 Microsoft 文件。

測試名稱	短名稱	錯誤碼	錯誤訊息	描述	Resolution
頂層GPO測試	testTopLevelEnforcedGPO	TOP_LEVEL_ENFORCED_GPO_FOUND	GroupPolicy cannot be set to Enforced at the Domain Root, Found GPOs: [*GposEnforced*] set as Enforced.	如果您的自我管理 AD 已將頂層GPOs設定為強制執行，則會顯示此訊息。	確保您的自我管理 AD 網域頂層群組政策物件 (GPO) 未設定為強制執行。如需詳細資訊，請參閱 Microsoft 文件。
信任類型測試	testTrustTypes	INVALID_TRUST_TYPE	Invalid trust types detected: [*InvalidTrustString*], only Uplevel (Microsoft AD) is currently supported.	如果您的自我管理 AD 具有不支援的信任類型，就會發生。	Uplevel 是混合目錄唯一支援的信任類型。您的自我管理 AD 不能有下列信任類型：DCE、MIT、Downlevel。如需信任類型的詳細資訊，請參閱 Microsoft 文件。
有效的網域控制站測試	testValidDC	COMPUTER_NOT_DC	Provided instance is not a domain controller.	如果您提供的自我管理 AD 執行個體不是網域控制站，或它們已經是另一個混合目錄的一部分，就會發生。	提供此混合目錄獨有的自我管理 AD 網域控制站。使用新目錄重試。請確定您已刪除失敗的混合目錄，以及自我管理 AD 中的任何 AWS OU。

評估測試警告訊息

下表說明評估測試期間可能發生的警告訊息。這些警告代表最佳組態的建議，但不阻止混合目錄設定。

測試名稱	短名稱	警告代碼	警告訊息	描述	Resolution
網域運作狀態測試	testDisabledStaleUserNumber	STALE_USERS_FOUND	*StaleUserCount* users were found to be stale, they have not logged in for *StaleThresholdInDays* days.	如果您的自我管理 AD 中有使用者帳戶長時間未登入，而且可能被視為過時或非作用中，則會顯示此訊息。	清除過時的使用者帳戶。
網域控制站資料來源測試	testDCTimeSource	DC_BAD_TIMESOURCE	Time sources not properly configured for PDC, should using an authoritative source. Time sources not properly configured for *dcHostName* , should using PDC as source	如果自我管理 AD 具有正確的時間來源設定，且與時間來源相比沒有很大的時間偏斜，AWS 則會顯示此訊息。	您的主要網域控制器 (PDC) 時間伺服器會導向 169.254.169.123 。您的非主要網域控制站應指向 PDC 做為來源。如需詳細資訊，請參閱使用 保持時間Amazon Time Sync Service。
可用空間測試	testFreeSpace	DISK_SPACE_EXCEEDED	Supported service max capacity	如果您的自我管理 AD 合併NTDS且Sysvol用量超	您的自我管理 AD 應為混合目錄提

測試名稱	短名稱	警告代碼	警告訊息	描述	Resolution
			of 7 GB exceeded; SysVol + NTDS is currently using: 24 GB)	過支援的配額，則會顯示此訊息。	供 24 GB 的磁碟空間。
S 通道 SSP測試	testSchannelSSP	TLS_1_2_NOT_ENABLED	Disabled protocol *DisabledProtocol* is still enabled.	如果自我管理 AD 不使用 TLS1.2和 AES256加密，便會發生。	您的自我管理 AD 必須AES256針對混合目錄使用 TLS 1.2和 。
磁碟損毀測試	testDiskCorruption	DISK_CORRUPT	Disk corruption detected on *Drive*.	如果您的自我管理 AD 發生磁碟損毀，就會發生。	您的自我管理 AD 磁碟不應損毀。

測試名稱	短名稱	警告代碼	警告訊息	描述	Resolution
網域控制站規格測試	testDcSpecs	INSUFFICIENT_RESOURCES	*numAvailableCores* cores detected when *requiredCores* cores recommended. *gbAvailableRam* GB ram detected when *requiredRam* GB recommended.	如果您的自我管理 AD 網域控制站不符合必要的規格，便會發生。	您的自我管理 AD 網域控制器應至少具有 7 GB RAM 和 2 個混合目錄的 CPU 核心。
伺服器層級外掛程式Dll測試	testServerLevelPluginDll	SERVER_LEVEL_PLUGIN_DLL_IS_SET	ServerLevelPluginDll registry configuration is not permitted.	在自我管理 AD 網域控制站上設定 ServerLevelPluginDll 時發生。	您的自我管理 AD 網域控制站不應ServerLevelPluginDll設定。
允許NT4加密測試	testAllowNT4Crypto	NT4_CRYPTO_NOT_ALLOWED	Registry key AllowNt4Crypto is not allowed.	如果自我管理 AD NT4 允許密碼編譯，便會發生。	您的自我管理 AD NT4 不應使用密碼編譯。如需詳細資訊，請參閱 Microsoft 文件。

測試名稱	短名稱	警告代碼	警告訊息	描述	Resolution
孤立的管理員使用者測試	testOrphanedAdminUsers	ORPHANED_ADMIN_USER_FOUND	*OrphanedUsersCount* Orphaned Admin Users Found: [*OrphanedUserNames*].	如果您的自我管理 AD 中存在孤立的管理員使用者，就會發生。	在繼續之前，移除自我管理 AD 上的孤立使用者。
特殊權限使用者計數測試	testPrivilegedUserCount	DOMAIN_ADMIN_COUNT_EXCEEDED	Number of Domain Admins (*daCount*) exceeded allowance of (*allowedDomainAdminCount*).	如果自我管理 AD 上的內建管理員、網域管理員和企業管理員的總計數大於 5，便會發生。	您的自我管理 AD 環境不應有多個特殊權限帳戶。在繼續之前，您應該移除過多的管理員帳戶。
特殊權限使用者計數測試	testPrivilegedUserCount	ENTERPRISE_ADMIN_COUNT_EXCEEDED	Number of Enterprise Admins (*eaCount*) exceeded allowance of (*allowedEnterpriseAdminCount*).	如果自我管理 AD 上的內建管理員、網域管理員和企業管理員的總計數大於 5，便會發生。	您的自我管理 AD 環境不應有多個特殊權限帳戶。在繼續之前，您應該移除過多的管理員帳戶。

測試名稱	短名稱	警告代碼	警告訊息	描述	Resolution
特殊權限使用者計數測試	testPrivilegedUserCount	BUILTIN_ADMIN_COUNT_EXCEEDED	Number of Built-in Admins (*baCount*) exceeded allowance of (*allowedAdminCount*).	如果自我管理 AD 上的內建管理員、網域管理員和企業管理員的總計數大於 5，便會發生。	您的自我管理 AD 環境不應有多個特殊權限帳戶。在繼續之前，您應該移除過多的管理員帳戶。
NTLM 測試	testNTLM	INSECURE_SETTING_NTLM	NTLMv1 is enabled.	如果NTLMv1已啟用自我管理 AD 上的身分驗證，則會顯示 。	NT LAN Manager 第 1 版 (NTLMv1) 具有已知的安全漏洞，不應使用。在自我管理 AD NTLMv1上停用 。如需詳細資訊，請參閱 Microsoft 文件。
Tombstone 生命週期測試	testTombstoneLifetime	TOMBSTONE_LIFETIME_ABOVE_LIMIT	Tombstone Lifetime is too long. DC Tombstone Lifetime is *TombstoneLifeTime* , AWS suggested number is *TombstoneMaximum* days.	如果自我管理 AD 上的 Tombstone 生命週期超過 180 天，就會發生。	Tombstone 生命週期是從 移除已刪除物件之前的天數AD。自我管理 AD 的 Tombstone 生命週期值應為 180 天或更少。如需詳細資訊，請參閱 Microsoft 文件。

Managed AWS Microsoft AD 入門

AWS Managed Microsoft AD 會在 Microsoft Active Directory中建立完全受管的 ， AWS 雲端 並採用 Windows Server 2019 技術，並在 2012 R2 Forest 和 Domain 功能層級運作。當您使用 AWS Managed Microsoft AD 建立目錄時， 會 AWS Directory Service 建立兩個網域控制站，並代表您新增 DNS 服務。網域控制站是在 Amazon VPC 中的不同子網路中建立的，此備援有助於確保您的目錄即使在失敗時仍可存取。如果您需要更多網域控制器，可於稍後新增。如需詳細資訊，請參閱部署 AWS Managed Microsoft AD 的其他網域控制站。

如需 AWS Managed Microsoft AD 的示範和概觀，請參閱下列YouTube影片。

AWS Managed Microsoft AD 示範和概觀

主題

- 建立 AWS Managed Microsoft AD 的先決條件
- AWS IAM Identity Center 先決條件
- 多重要素驗證先決條件
- 建立 AWS Managed Microsoft AD
- 使用 AWS Managed Microsoft AD 建立的內容
- AWS Managed Microsoft AD Administrator 帳戶和群組許可

建立 AWS Managed Microsoft AD 的先決條件

若要建立 AWS Managed Microsoft ADActive Directory，您需要具有下列項目的 Amazon VPC：

- 至少兩個子網路。每個子網路皆必須位於不同的可用區域。
- VPC 必須具有預設硬體租用。
- 您不能使用 198.18.0.0/15 地址空間中的地址在 VPC 中建立 AWS Managed Microsoft AD。

如果您需要將 AWS Managed Microsoft AD 網域與現有的現場部署Active Directory網域整合，則必須將現場部署網域的樹系和網域功能層級設定為 Windows Server 2003 或更高版本。

AWS Directory Service 使用兩個 VPC 結構。組成目錄的 EC2 執行個體會在您的 AWS 帳戶之外執行，並由 管理 AWS。其使用兩種網路轉接器，ETH0 和 ETH1。ETH0 是管理轉接器，而且位於您的帳戶外部。ETH1 則是建立於您的帳戶內部。

您目錄的 ETH0 網路的管理 IP 範圍是 198.18.0.0/15。

如需如何建立 AWS 環境和 AWS Managed Microsoft AD 的教學課程，請參閱 AWS Managed Microsoft AD 測試實驗室教學課程。

AWS IAM Identity Center 先決條件

如果您計劃將 IAM Identity Center 與 AWS Managed Microsoft AD 搭配使用，您需要確保下列項目為真：

- 您的 AWS Managed Microsoft AD 目錄是在 AWS 組織的管理帳戶中設定。
- IAM Identity Center 的執行個體位於設定 AWS Managed Microsoft AD 目錄的相同區域中。

如需詳細資訊，請參閱《 AWS IAM Identity Center 使用者指南》中的 IAM Identity Center 先決條件。

多重要素驗證先決條件

若要使用 AWS Managed Microsoft AD 目錄支援多重驗證，您必須以下列方式設定內部部署或雲端型遠端驗證撥入使用者服務 (RADIUS) 伺服器，以便接受來自 AWS Managed Microsoft AD 目錄的請求 AWS。

1. 在 RADIUS 伺服器上，建立兩個 RADIUS 用戶端來代表其中的兩個 AWS Managed Microsoft AD 網域控制站 DCs) AWS。您必須使用下列一般參數來設定這兩個用戶端 (您的 RADIUS 伺服器可能會有所不同)：
   - 地址 (DNS 或 IP)：這是其中一個 AWS Managed Microsoft AD DCs的 DNS 地址。您可以在您計劃使用 MFA 之 AWS Managed Microsoft AD 目錄的詳細資訊頁面上的 AWS 目錄服務主控台中找到這兩個 DNS 地址。顯示的 DNS 地址代表 所使用的兩個 AWS Managed Microsoft AD DCs的 IP 地址 AWS。

     > **Note**
     >
     > 如果您的 RADIUS 伺服器支援 DNS 地址，您只能建立一個 RADIUS 用戶端組態。否則，您必須為每個 AWS Managed Microsoft AD DC 建立一個 RADIUS 用戶端組態。

   - 連接埠號碼：設定您的 RADIUS 伺服器用來接受 RADIUS 用戶端連線的連接埠號碼。標準 RADIUS 連接埠是 1812。
   - 共用密碼：輸入或產生 RADIUS 伺服器將用來連線到 RADIUS 用戶端的共用密碼。
   - 通訊協定：您可能需要設定 AWS Managed Microsoft AD DCs和 RADIUS 伺服器之間的身分驗證通訊協定。支援的協定包括 PAP、CHAP MS-CHAPv1 和 MS-CHAPv2。建議使用 MS-CHAPv2，因為它提供三種選項當中最強大的安全。

- 應用程式名稱：這在某些 RADIUS 伺服器中可能是選用的，通常用來識別訊息或報告中的應用程式。

2. 設定現有的網路，以允許從 RADIUS 用戶端 (AWS 受管 Microsoft AD DCs DNS 地址，請參閱步驟 1) 到 RADIUS 伺服器連接埠的傳入流量。
3. 將規則新增至 AWS Managed Microsoft AD 網域中的 Amazon EC2 安全群組，以允許來自先前定義的 RADIUS 伺服器 DNS 地址和連接埠號碼的傳入流量。如需詳細資訊，請參閱《EC2 使用者指南》中的「新增規則至安全群組」一節。

如需搭配 MFA 使用 AWS Managed Microsoft AD 的詳細資訊，請參閱 啟用 AWS Managed Microsoft AD 的多重驗證。

建立 AWS Managed Microsoft AD

若要建立新的 AWS Managed Microsoft ADActive Directory，請執行下列步驟。開始此程序之前，請確定您已完成「建立 AWS Managed Microsoft AD 的先決條件」中所示的必要條件。

建立 AWS Managed Microsoft AD

1. 在 AWS Directory Service 主控台中，選擇目錄，然後選擇設定目錄。
2. 在選取目錄類型頁面上，選擇 AWS Managed Microsoft AD，然後選擇下一步。
3. 在 Enter directory information (輸入目錄資訊) 頁面上，提供下列資訊：

   Edition (版本)

   從 AWS Managed Microsoft AD 的標準版本或企業版本中選擇。如需版本的詳細資訊，請參閱 AWS Directory Service for Microsoft Active Directory。

   目錄 DNS 名稱

   目錄的完全合格名稱，例如 `corp.example.com`。

   > **Note**
   >
   > 如果您打算將 Amazon Route 53 用於 DNS， AWS 則 Managed Microsoft AD 的網域名稱必須與 Route 53 網域名稱不同。如果 Route 53 和 AWS Managed Microsoft AD 共用相同的網域名稱，可能會發生 DNS 解析問題。

目錄 NetBIOS 名稱

目錄的簡短名稱，例如：CORP。

目錄描述

選擇填寫其他目錄說明。您可以在建立 AWS Managed Microsoft AD 之後變更此描述。

管理員密碼

目錄管理員的密碼。目錄建立程序會建立含有使用者名稱 Admin 與這組密碼的管理者帳戶。您可以在建立 AWS Managed Microsoft AD 之後變更管理員密碼。

密碼不得包含「admin」一字。

目錄管理者密碼區分大小寫，長度須介於 8 至 64 個字元之間。至少須有一位字元屬於以下四種類型中的三類：

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

Confirm password (確認密碼)

重新輸入管理員密碼。

（選用）使用者和群組管理

若要從 啟用 AWS Managed Microsoft AD 使用者和群組管理 AWS Management Console，請在 中選取管理使用者和群組管理 AWS Management Console。如需如何使用使用者和群組管理的詳細資訊，請參閱 the section called “使用主控台、CLI 或 管理使用者和群組 PowerShell”。

4. 在 Choose VPC and subnets (選擇 VPC 和子網路) 頁面上，提供下列資訊，然後選擇 Next (下一步)。

VPC

目錄的 VPC。

子網路

選擇網域控制站的子網路。這兩個子網路必須位於不同的可用區域。

5. 在 Review & create (檢閱和建立) 頁面上檢閱目錄資訊，並進行必要的變更。若資訊無誤，請選擇 Create directory (建立目錄)。建立目錄需要 20 到 40 分鐘。建立後，Status (狀態) 值會變更為 Active (作用中)。

如需使用 AWS Managed Microsoft AD 建立之項目的詳細資訊，請參閱下列內容：

- 使用 AWS Managed Microsoft AD 建立的內容
- AWS Managed Microsoft AD Administrator 帳戶和群組許可

相關 AWS 安全部落格文章

- 如何將 AWS Managed Microsoft AD 目錄的管理委派給現場部署Active Directory使用者
- 如何使用 AWS Directory Service for AWS Managed Microsoft AD 設定更強大的密碼政策，以協助滿足您的安全標準
- 如何透過新增網域控制站來提高 AWS Managed Microsoft AD AWS Directory Service 的備援和效能
- 如何在 AWS Managed Microsoft AD 上部署遠端桌面授權管理員，以啟用Microsoft遠端桌面的使用
- 如何使用 AWS Management ConsoleAWS Managed Microsoft AD 和您的內部部署憑證存取
- 如何使用 AWS Managed Microsoft AD 和內部部署登入資料啟用 AWS 服務的多重要素驗證
- 如何使用您的內部部署輕鬆登入 AWS 服務 Active Directory

使用 AWS Managed Microsoft AD 建立的內容

當您Active Directory使用 AWS Managed Microsoft AD 建立 時， 會代表您 AWS Directory Service 執行下列任務：

- 自動建立彈性網路介面 (ENI) 並將其與您的每個域控制站建立關聯。這些 ENIs 對 VPC 和 AWS Directory Service 網域控制站之間的連線至關重要，絕不應刪除。您可以透過 AWS Directory Service 描述識別保留給 使用的所有網路介面：「為 directory-idAWS 建立網路介面」。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的彈性網路界面。 AWS Managed Microsoft AD 的預設 DNS 伺服器Active Directory是位於無類別網域間路由 (CIDR)+2 的 VPC DNS 伺服器。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon DNS 伺服器。

> **Note**
>
> 根據預設，網域控制站會部署在一個區域中的兩個可用區域，並連接到您的 Amazon VPC (VPC)。備份每天會自動執行一次，Amazon EBS (EBS) 磁碟區也會加密，以確保靜態資料的安全。一旦域控制站發生故障，將在同一可用區域中使用相同的 IP 地址自動替換，並且可以透過最新的備份執行完整的災難復原。

- VPC Active Directory中的佈建會使用兩個網域控制站來提供容錯能力和高可用性。目錄已成功建立且處於作用中狀態後，便可佈建更多的網域控制器，以取得更高的彈性和效能。如需詳細資訊，請參閱部署 AWS Managed Microsoft AD 的其他網域控制站。

> **Note**
>
> AWS 不允許在 AWS Managed Microsoft AD 網域控制站上安裝監控代理程式。

- 建立AWS 安全群組 *sg-1234567890abcdef0*，為傳入和傳出網域控制站的流量建立網路規則。預設傳出規則允許所有 IPv4 地址的所有流量。預設傳入規則僅允許來自與 AWS Managed Microsoft AD 的 VPC 託管相關聯之主要 IPv4 CIDR 區塊Active Directory的透過連接埠的流量。為了提高安全性，已建立的 ENI 不會連接彈性 IP，且您沒有將彈性 IP 連接到這些 ENI 的許可。因此，根據預設，唯一可以與您的 AWS Managed Microsoft AD 通訊的傳入流量是本機 VPC。您可以變更安全群組規則以允許其他流量來源，例如透過 VPN 連線的其他對等 VPCs CIDRs。嘗試變更這些規則時請格外小心，因為這樣可能會破壞您與網域控制器之間的通訊能力。如需詳細資訊，請參閱AWS Managed Microsoft AD 最佳實務及增強 AWS Managed Microsoft AD 網路安全組態。

  您可以使用字首清單來管理安全群組規則中的 CIDR 區塊。字首清單可讓您更輕鬆地管理和設定安全群組和路由表。您可以使用相同的連接埠和通訊協定來合併多個 CIDR 區塊，以擴展網路流量。

  - 在Windows環境中，用戶端通常會透過伺服器訊息區塊 (SMB) 或連接埠 445 進行通訊。此通訊協定有助於各種動作，例如檔案和印表機共用和一般網路通訊。您會在連接埠 445 看到用戶端流量流向 AWS Managed Microsoft AD 網域控制站的管理介面。

    當 SMB 用戶端依賴 DNS （連接埠 53) 和 NetBIOS （連接埠 138) 名稱解析來尋找 AWS Managed Microsoft AD 網域資源時，就會發生此流量。在尋找網域資源時，這些用戶端會導向網域控制站上任何可用的界面。這種行為是預期的，通常發生在具有多個網路轉接器的環境中，其中SMB 多通道允許用戶端在不同介面之間建立連線，以提高效能和備援。

  預設會建立下列 AWS 安全群組規則：

  傳入規則

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
ICMP	N/A	AWS Managed Microsoft AD VPC IPv4 CIDR	Ping	LDAP Keep Alive、DFS
TCP 和 UDP	53	AWS Managed Microsoft AD VPC IPv4 CIDR	DNS	使用者和電腦身分驗證、名稱解析、信任
TCP 和 UDP	88	AWS Managed Microsoft AD VPC IPv4 CIDR	Kerberos	使用者和電腦身分驗證、森林層級信任
TCP 和 UDP	389	AWS Managed Microsoft AD VPC IPv4 CIDR	LDAP	目錄、複寫、使用者和電腦身分驗證群組政策、信任
TCP 和 UDP	445	AWS Managed Microsoft AD VPC IPv4 CIDR	SMB/CIFS	複寫、使用者和電腦身分驗證、群組政策、信任
TCP 和 UDP	464	AWS Managed Microsoft AD VPC IPv4 CIDR	Kerberos 更改/設定密碼	複寫、使用者和電腦身分驗證、信任
TCP	135	AWS Managed Microsoft AD VPC IPv4 CIDR	複寫	RPC、EPM
TCP	636	AWS Managed Microsoft AD VPC IPv4 CIDR	LDAP SSL	目錄、複寫、使用者和電腦身分驗證、群組政策、信任

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
TCP	1024-65535	AWS Managed Microsoft AD VPC IPv4 CIDR	RPC	複寫、使用者和電腦身分驗證、群組政策、信任
TCP	3268-3269	AWS Managed Microsoft AD VPC IPv4 CIDR	LDAP GC 和 LDAP GC SSL	目錄、複寫、使用者和電腦身分驗證、群組政策、信任
UDP	123	AWS Managed Microsoft AD VPC IPv4 CIDR	Windows 時間	Windows 時間、信任
UDP	138	AWS Managed Microsoft AD VPC IPv4 CIDR	DFSN 和 NetLogon	DFS、群組政策
全部	全部	AWS 為網域控制站建立安全群組 (*sg-1234567890abcdef0*)	所有流量	

傳出規則

通訊協定	連接埠範圍	目的地	流量類型	Active Directory 用量
全部	全部	0.0.0.0/0	所有流量	

- 如需 所使用的連接埠和通訊協定的詳細資訊Active Directory，請參閱 Microsoft 文件中的 Windows 的服務概觀和網路連接埠需求。

- 建立含有使用者名稱 Admin 與指定密碼的目錄管理員帳戶。此帳戶位於 下 Users OU（例如，公司 > 使用者）。您可以使用此帳戶來管理 中的目錄 AWS 雲端。如需詳細資訊，請參閱AWS Managed Microsoft AD Administrator 帳戶和群組許可。

> **Important**
>
> 請務必儲存此密碼。 AWS Directory Service 不會儲存此密碼，而且無法擷取。不過，您可以從 AWS Directory Service 主控台或使用 ResetUserPassword API 重設密碼。

- 在網域根建立以下三個組織單位 (OU)：

OU 名稱	描述
AWS Delegated Groups	存放可用於將 AWS 特定許可委派給使用者的所有群組。
AWS Reserved	存放所有 AWS 管理特定帳戶。

<yourdomainname>	此 OU 的名稱的基礎，是您建立目錄時所輸入的 NetBIOS 名稱。如未指定 NetBIOS 名稱，預設名稱將是您 Directory DNS (目錄 DNS) 的第一個部分 (以 corp.example.com 為例，NetBIOS 名稱就是 corp)。此 OU 由 擁有 AWS ，並包含您所有 AWS相關的目錄物件，這些物件會授予您完全控制。此 OU 下預設存在兩個子 OU：Computers (電腦) 和 Users (使用者)。例如：
	• 公司
	  • 電腦
	  • 使用者

- 在 中建立下列群組AWS Delegated Groups OU：

Group name (群組名稱)	描述
AWS Delegated Account Operators	此安全群組的成員具備有限的帳戶管理功能，例如密碼重設

Group name (群組名稱)	描述
AWS Delegated Active Directory Based Activation Administrators	此權限安全群組成員可以建立 Active Directory 大量授權啟用物件，以便企業透過網域連線來啟用電腦。
AWS Delegated Add Workstations To Domain Users	此安全群組的成員可以將 10 部電腦加入網域。
AWS Delegated Administrators	此安全群組的成員可以管理 AWS Managed Microsoft AD、完全控制 OU 中的所有物件，也可以管理 中包含的群組AWS Delegated Groups OU。
AWS Delegated Allowed to Authenticate Objects	此安全群組的成員能夠對 中的電腦資源進行身分驗證 AWS Reserved OU（僅啟用選擇性身分驗證信任的內部部署物件才需要）。
AWS Delegated Allowed to Authenticate to Domain Controllers	此安全群組的成員能夠對 中的電腦資源進行身分驗證 Domain Controllers OU（僅啟用選擇性身分驗證信任的內部部署物件才需要）。
AWS Delegated Deleted Object Lifetime Administrators	此安全群組的成員可以修改msDS-DeletedObjectLifetime物件，這會定義已刪除物件從 AD 資源回收筒中復原的可用時間。
AWS Delegated Distributed File System Administrators	此安全群組的成員可以新增及移除 FRS、DFS-R 和 DFS 命名空間。
AWS Delegated Domain Name System Administrators	此安全群組的成員可以管理與 DNS 整合的 Active Directory。
AWS Delegated Dynamic Host Configuration Protocol Administrators	此安全群組的成員可以授權企業中的 Windows DHCP 伺服器。
AWS Delegated Enterprise Certificate Authority Administrators	此安全群組的成員可以部署及管理 Microsoft 企業憑證授權機構基礎設施。

Group name (群組名稱)	描述
AWS Delegated Fine Grained Password Policy Administrators	此安全群組的成員可以修改預先建立的微調密碼政策。
AWS Delegated FSx Administrators	此安全群組的成員具備 Amazon FSx 資源的管理能力。
AWS Delegated Group Policy Administrators	此安全群組的成員可以執行群組政策管理任務 (建立、編輯、刪除、連結)。
AWS Delegated Kerberos Delegation Administrators	此安全群組的成員可以在電腦和使用者帳戶物件上啟用委派。
AWS Delegated Managed Service Account Administrators	此安全群組的成員可以建立及刪除受管服務帳戶。
AWS Delegated MS-NPRC Non-Compliant Devices	此安全群組的成員將被排除在需要與域控制站進行安全通道通訊的範圍之外。此群組用於電腦帳戶。
AWS Delegated Remote Access Service Administrators	此安全群組的成員可以在 RAS 和 IAS 伺服器群組中新增及移除 RAS 伺服器。
AWS Delegated Replicate Directory Changes Administrators	此安全群組的成員可以同步 Active Directory 與 SharePoint Server 中的描述檔資訊。
AWS Delegated Server Administrators	所有加入網域之電腦上的本機管理員群組中都包含此安全群組的成員。
AWS Delegated Sites and Services Administrators	此安全群組的成員可以重新命名 Active Directory 網站和服務中的 Default–First–Site–Name 物件。
AWS Delegated System Management Administrators	此權限安全群組成員可以在系統管理容器中建立並管理物件。

Group name (群組名稱)	描述
AWS Delegated Terminal Server Licensing Administrators	此安全群組的成員可以在終端機伺服器的授權伺服器群組中新增及移除終端機伺服器的授權伺服器。
AWS Delegated User Principal Name Suffix Administrators	此安全群組的成員可以新增及移除使用者主體名稱尾碼。

> **Note**
>
> 您可以將 新增至這些 AWS Delegated Groups。

- 建立並套用下列群組政策物件 (GPO)：

> **Note**
>
> 您無權刪除、修改或取消連結這些 GPO。這是設計為保留供 AWS 使用。如果需要，您可以將它們連結到您控制的 OU。

群組政策名稱	適用對象	描述
Default Domain Policy	網域	包含網域密碼和 Kerberos 政策。
ServerAdmins	所有非網域控制器電腦帳戶	將 新增'AWS Delegated Server Administrators'為 的成員BUILTIN\Administrators Group。
AWS Reserved Policy:User	AWS Reserved user accounts	在 中為所有使用者帳戶設定建議的安全性設定AWS Reserved OU。
AWS Managed Active Directory Policy	所有網域控制器	在所有網域控制器上設定建議的安全性設定。

群組政策名稱	適用對象	描述
TimePolicyNT5DS	所有非 PDCe 網域控制器	將所有非 PDCe 網域控制器的時間政策設定為使用 Windows 時間 (NT5DS)。
TimePolicyPDC	PDCe 網域控制器	將 PDCe 網域控制器的時間政策設定為使用網路時間通訊協定 (NTP)。
Default Domain Controllers Policy	未使用	在網域建立期間佈建， AWS 受管 Active Directory 政策會取代其位置。

如果您想要查看每個 GPO 的設定，可以從已啟用群組政策管理主控台 (GPMC) 的已加入域 Windows 執行個體檢視這些設定。

- default local accounts 為 AWS Managed Microsoft AD 管理建立下列項目：

> **Important**
>
> 請務必儲存管理員密碼。 AWS Directory Service 不會儲存此密碼，而且無法擷取。不過，您可以從 AWS Directory Service 主控台或使用 ResetUserPassword API 重設密碼。

Admin

Admin 是第一次directory administrator account建立 AWS Managed Microsoft AD 時建立的 。您在建立 AWS Managed Microsoft AD 時提供此帳戶的密碼。此帳戶位於 下 Users OU（例如，公司 > 使用者）。您可以使用此帳戶在 Active Directory中管理 AWS。如需詳細資訊，請參閱AWS Managed Microsoft AD Administrator 帳戶和群組許可。

AWS_***11111111111***

任何以 開頭， AWS 後面接著底線且位於 的帳戶名稱AWS Reserved OU，都是服務受管帳戶。此服務受管帳戶由 用來與 AWS 互動Active Directory。這些帳戶會在 AWS Directory Service Data 啟用時建立，並使用 上授權的每個新 AWS 應用程式Active Directory。這些帳戶只能由 AWS 服務存取。

krbtgt account

在 AWS Managed Microsoft AD 使用的 Kerberos 票證交換中krbtgt account扮演重要角色。krbtgt account 是用於 Kerberos 票證授權 (TGT) 加密的特殊帳戶，它在 Kerberos 身分驗證通訊協定的安全性中扮演重要角色。如需詳細資訊，請參閱 Microsoft 文件。

AWS 每 90 天會自動輪換 AWS Managed Microsoft AD krbtgt account的密碼兩次。每 90 天兩次連續輪換之間有 24 小時的等待期。

如需管理員帳戶和 建立的其他帳戶的詳細資訊Active Directory，請參閱 Microsoft 文件。

AWS Managed Microsoft AD Administrator 帳戶和群組許可

當您建立 AWS Directory Service for Microsoft Active Directory 目錄時， AWS 會建立組織單位 (OU) 來存放 AWS 所有相關群組和帳戶。如需此 OU 的詳細資訊，請參閱「使用 AWS Managed Microsoft AD 建立的內容」。這包括管理帳戶。管理帳戶具有許可，能夠執行以下對您的 OU 而言常見的管理活動：

- 新增、更新或刪除使用者、群組和電腦。如需詳細資訊，請參閱AWS Managed Microsoft AD 中的使用者和群組管理。
- 新增資源 (例如檔案或列印伺服器) 至您的網域，然後對您 OU 中的使用者和群組指派這些資源的許可。
- 建立額外的 OU 和容器。
- 委派其他 OU 和容器的授權。如需詳細資訊，請參閱委派 AWS Managed Microsoft AD 的目錄聯結權限。
- 建立及連結群組政策。
- 從 Active Directory 資源回收筒還原已刪除的物件。
- 在 Active Directory Web Service 上執行 Active Directory 和 DNS PowerShell模組。
- 建立及設定群組受管服務帳戶。如需詳細資訊，請參閱群組受管服務帳戶。
- 設定 Kerberos 限制委派。如需詳細資訊，請參閱Kerberos 限制委派。

管理帳戶也有權執行下列全網域活動：

- 管理 DNS 組態 (新增、移除或更新記錄、區域和轉寄站)
- 檢視 DNS 事件日誌
- 檢視安全事件日誌

管理帳戶僅允許此處所列的動作。管理帳戶也缺少您特定 OU (例如父 OU) 外部任何目錄相關動作的許可。

考量事項

- AWS 網域管理員擁有 上託管之所有網域的完整管理存取權 AWS。請參閱您與 的協議 AWS 和AWS 資料保護常見問答集，進一步了解 如何處理您儲存在 AWS 系統上 AWS 的內容，包括目錄資訊。
- 建議您不要刪除或重新命名此帳戶。如果不想再使用該帳戶，建議您設定長密碼 (最長為 64 個隨機字元)，然後停用該帳戶。

> **Note**
>
> AWS 擁有網域管理員和企業管理員權限使用者和群組的專屬控制權。這可讓 AWS 執行目錄的操作管理。

企業和域管理員特殊權限帳戶

AWS 每 90 天會自動將內建管理員密碼輪換為隨機密碼。每當請求內建管理員密碼供人工使用時，AWS 就會建立票證，並與 AWS Directory Service 團隊一起記錄。帳戶憑證經過加密並透過安全通道處理。此外，管理員帳戶登入資料只能由 AWS Directory Service 管理團隊請求。

若要執行目錄的操作管理， AWS 擁有具有企業管理員和網域管理員權限帳戶的專屬控制權。這包括 Active Directory 管理員帳戶的獨佔控制權。 透過使用密碼保存庫自動化密碼管理來保護 AWS 此帳戶。在管理員密碼的自動輪換期間， AWS 會建立臨時使用者帳戶，並授予網域管理員權限。此臨時帳戶是管理員帳戶密碼輪換失效時的備用方案。 AWS 成功輪換管理員密碼後， 會 AWS 刪除臨時管理員帳戶。

通常完全透過自動化 AWS 操作目錄。如果自動化程序無法解決操作問題， AWS 可能需要支援工程師登入您的網域控制站 (DC) 來執行診斷。在這些極少數情況下， 會 AWS 實作請求/通知系統來授予存取權。在此程序中， AWS 自動化會在您的目錄中建立具有網域管理員許可的限時使用者帳戶。 會將使用者帳戶與指派在目錄中工作的工程師建立 AWS 關聯。 會在我們的日誌系統中 AWS 記錄此關聯，並為工程師提供要使用的登入資料。工程師採取的所有動作，都會記錄在 Windows 事件日誌。分配之時間結束時，會自動刪除使用者帳戶。

您可以使用目錄的日誌轉寄功能，監督管理帳戶的行動。此功能可讓您將 AD 安全性事件傳送到 CloudWatch 系統，讓您實作監督解決方案。如需詳細資訊，請參閱啟用 AWS Managed Microsoft AD 的 Amazon CloudWatch Logs 日誌轉送。

當有人以互動的方式登入 DC 時，安全事件 ID 4624、4672 和 4648 都會被記錄下來。您可以使用事件檢視器 Microsoft 管理主控台 (MMC)，從加入 Windows 電腦的網域檢視每個 DC 的 Windows 安全事件日誌。您也可以 啟用 AWS Managed Microsoft AD 的 Amazon CloudWatch Logs 日誌轉送 將所有安全事件日誌傳送到您帳戶中的 CloudWatch Logs。

您可能會偶爾看到 AWS 在預留 OU 中建立和刪除的使用者。 AWS 負責此 OU 中所有物件的管理和安全性，以及任何其他 OU 或容器，而我們尚未委派您存取和管理許可。您可能會看到該 OU 中的建立和刪除操作。這是因為 AWS Directory Service 使用自動化定期輪換網域管理員密碼。密碼輪換時會建立備份，以防輪換失敗。輪換成功後，備份帳戶將自動刪除。此外，在極少數情況下，為了進行故障診斷而需要在 DCs上進行互動式存取，則會建立臨時使用者帳戶供 AWS Directory Service 工程師使用。一旦相關工程師完成工作，該臨時使用者帳戶將被刪除。請注意，每次請求目錄的互動式登入資料時，都會通知 AWS Directory Service 管理團隊。

AWS Managed Microsoft AD 的重要概念和最佳實務

您可以熟悉關鍵概念和最佳實務，以充分利用 AWS Managed Microsoft AD。關鍵概念可協助您了解 AWS Managed Microsoft AD 的運作方式。關鍵概念包括進一步了解Active Directory結構描述、修補排程和群組受管服務帳戶。Active Directory結構描述包含屬性、類別和物件等元素，這些元素組成 AWS Managed Microsoft AD. AWS patches your AWS Managed Microsoft AD 網域控制站並代表您進行Microsoft更新。您也可以進一步了解群組受管服務帳戶 (gMSAs)，並將其與 AWS Managed Microsoft AD 搭配使用。

您可以透過考慮最佳實務來避免 AWS Managed Microsoft AD 的問題。其中一些最佳實務包括：

- 設定 AWS Managed Microsoft AD 時，請設定安全群組以符合您的需求、記住您的管理員帳戶 ID 和密碼，並啟用條件式轉寄站設定。
- 使用 AWS Managed Microsoft AD 時，請勿變更建立目錄時 AWS 建立的組織單位、使用 Amazon CloudWatch 和 Amazon SNS 等工具監控效能，以及使用 SMB 2.x 用戶端。
- 程式設計應用程式以使用 AWS Managed Microsoft AD 時，請使用 Windows DC 定位器服務、在將應用程式推展到生產環境之前進行負載測試變更，以及使用有效的 LDAP 查詢，以避免網域控制器中的重大 CPU 週期。

主題

- AWS Managed Microsoft AD 關鍵概念
- AWS Managed Microsoft AD 最佳實務

AWS Managed Microsoft AD 關鍵概念

如果您熟悉下列重要概念，將能充分利用 AWS Managed Microsoft AD。

主題

- Active Directory 結構描述
- AWS Managed Microsoft AD 修補和維護
- 群組受管服務帳戶
- Kerberos 限制委派

Active Directory 結構描述

結構描述是屬於分散式目錄之屬性和類別的定義，類似資料庫中的欄位及表格。結構描述包含一組規則，它們決定資料庫可以新增或包含的資料類型和格式。使用者類別是存放在資料庫中的 類別範例之一。使用者類別屬性的一些範例可以包含使用者的名字、姓氏、電話號碼等。

結構描述元素

屬性、類別和物件是用來建立結構描述中物件定義的基本元素。以下提供結構描述元素的詳細資訊，在您開始擴展 AWS Managed Microsoft AD 結構描述的程序之前，請務必了解這些元素。

Attributes

每個結構描述屬性 (attribute) 類似於資料庫中的欄位，其中包含用來定義屬性 (attribute) 特性的幾個屬性 (property)。例如，LDAP 用戶端用來讀取及寫入屬性 (attribute) 的屬性 (property) 為 `LDAPDisplayName`。`LDAPDisplayName` 屬性 (property) 在所有屬性 (attribute) 和類別中必須是唯一的。如需屬性特性的完整清單，請參閱 MSDN 網站上的 Characteristics of Attributes。如需如何建立新屬性的其他指引，請參閱 MSDN 網站上的 Defining a New Attribute。

類別

類別類似於資料庫中的資料表，也有幾個需要定義的屬性。例如，`objectClassCategory` 會定義類別分類。如需類別特性的完整清單，請參閱 MSDN 網站上的 Characteristics of Object Classes。如需如何建立新類別的詳細資訊，請參閱 MSDN 網站上的 Defining a New Class。

物件識別符 (OID)

每個類別和屬性都必須具有對您所有物件唯一的 OID。軟體廠商必須取得其自己的 OID，以確保唯一性。唯一性可避免當多個應用程式針對不同用途使用相同屬性時發生的衝突。若要確保唯一性，

您可以從 ISO 名稱登錄授權機構取得根 OID。或者，您可以從 Microsoft 取得基底 OID。如需 OID 及如何取得 OID 的詳細資訊，請參閱 MSDN 網站上的 Object Identifiers。

結構描述連結屬性

某些屬性會透過正向與反向連結在兩個類別之間連結。群組是最佳範例。當您檢視群組時，您會看到群組的成員；如果您檢視使用者，您會看到其所屬的群組。當您將使用者新增至群組時，Active Directory 會建立群組的正向連結。然後，Active Directory 會新增從群組到使用者的反向連結。建立要連結的屬性時必須產生唯一的連結 ID。如需詳細資訊，請參閱 MSDN 網站上的 Linked Attributes。

相關主題

- 何時擴展 AWS Managed Microsoft AD 結構描述
- 教學課程：擴展 AWS Managed Microsoft AD 結構描述

AWS Managed Microsoft AD 修補和維護

AWS Directory Service for Microsoft Active Directory，也稱為 AWS DS for AWS Managed Microsoft AD，實際上是 Microsoft Active Directory Domain Services (AD DS)，以受管服務的形式交付。系統會將 Microsoft Windows Server 2019 用於網域控制站 (DCs)，並將軟體 AWS 新增至 DCs以進行服務管理。 AWS 更新 （修補程式） DCs以新增新功能並保持 Microsoft Windows Server 軟體為最新版本。在修補過程中，您的目錄仍然可供使用。

確保可用性

每個目錄預設會包含兩個 DC，分別安裝在不同的可用區域。您可以選擇新增 DCs以進一步提高可用性。對於需要高可用性和容錯能力的關鍵環境，我們建議您依序部署額外的 DCs. AWS patches DCs，在此期間，主動修補 AWS 的 DC 無法使用。如果您的一個或多個 DCs暫時停止服務， 會 AWS 防禦修補，直到您的目錄至少有兩個運作DCs。這可讓您在修補過程中使用其他作業 DC，修補每個 DC 通常需要 30 到 45 分鐘，但此時間可能會有所不同。為了確保您的應用程式可以在一或多個 DC 基於任何原因 (包括修補) 而無法使用時連線到作業 DC，您的應用程式應該使用 Windows DC 定位器服務且不使用靜態 DC 地址。

了解修補排程

為了保持 DCs上的 Microsoft Windows Server 軟體為最新版本， AWS 會利用 Microsoft 更新。隨著 Microsoft 為 Windows Server 提供每月彙總修補程式， AWS 會盡最大努力在三個日曆週內測試並套用彙總至所有客戶 DCs。此外， 會根據 DC 的適用性和緊急性， AWS 檢閱 Microsoft 在每月彙總之外發

行DCs更新。對於 Microsoft 評定為關鍵或重要以及與 DC 相關的安全性修補程式， AWS 會盡可能在五天內測試及部署修補程式。

群組受管服務帳戶

在 Windows Server 2012 中，Microsoft 引進了一個新方法，可供管理員用來管理稱為群組受管服務帳戶 (gMSA) 的服務帳戶。使用 gMSA，服務管理員不再需要手動管理服務執行個體之間的密碼同步。反之，管理員只要在 Active Directory 中建立一個 gMSA，然後設定多個服務執行個體使用該單一 gMSA 即可。

若要授予許可，讓 AWS Managed Microsoft AD 中的使用者可以建立 gMSA，您必須將其帳戶新增為AWS 委派 Managed Service 帳戶管理員安全群組的成員。根據預設，管理帳戶是此群組的成員。如需 gMSA 的詳細資訊，請參閱 Microsoft TechNet 網站上的 Group Managed Service Accounts Overview。

相關 AWS 安全部落格文章

- AWS Managed Microsoft AD 如何協助簡化部署並改善 Active Directory 整合的 .NET 應用程式的安全性

Kerberos 限制委派

Kerberos 限制委派是 Windows Server 功能。此功能可讓服務管理員透過限制應用程式服務可代表使用者採取行動的範圍，來指定和強制執行應用程式信任界限。當您需要設定哪個前端服務帳戶可委派給其後端服務時，這可能會很有用。Kerberos 限制委派也可防止您的 gMSA 代表您的 Active Directory 使用者連線到任何及所有服務，並避免可能遭到惡意開發人員濫用。

例如，假設使用者 jsmith 日誌登入 HR 應用程式。您希望 SQL Server 套用 jsmith 的資料庫許可。不過，根據預設，SQL Server 會使用套用 hr-app-service 許可的服務帳戶憑證開啟資料庫連線，而非 jsmith 設定的許可。您必須讓 HR 薪資應用程式可以使用 jsmith 的登入資料存取 SQL Server 資料庫。若要執行此作業，您可以為 AWS中的 AWS Managed Microsoft AD 目錄中的 hr–app–service 服務帳戶啟用 Kerberos 限制委派。當 jsmith 登入時，Active Directory 會提供 Kerberos 票證，當 jsmith 嘗試存取網路中的其他服務時，Windows 會自動使用此票證。Kerberos 委派可讓 hr-app-service 帳戶在存取資料庫時重複使用 jsmith 的 Kerberos 票證，藉此在開啟資料庫連線時套用 jsmith 的特定許可。

若要授予許可，允許 AWS Managed Microsoft AD 中的使用者設定 Kerberos 限制委派，您必須將其帳戶新增為AWS 委派 Kerberos 委派管理員安全群組的成員。根據預設，管理帳戶是此群組的成員。如需 Kerberos 限制委派的詳細資訊，請參閱 Microsoft TechNet 網站上的 Kerberos Constrained Delegation Overview。

資源型限制委派 已和 Windows Server 2012 一起推出。它提供後端服務管理員設定服務限制委派的能力。

AWS Managed Microsoft AD 最佳實務

以下是您應該考慮的一些建議和指導方針，以避免問題並充分利用 AWS Managed Microsoft AD。

主題

- 設定 AWS Managed Microsoft AD 的最佳實務
- 使用 AWS Managed Microsoft AD 目錄時的最佳實務
- 程式設計 AWS Managed Microsoft AD 應用程式時的最佳實務

設定 AWS Managed Microsoft AD 的最佳實務

以下是設定 AWS Managed Microsoft AD 時的一些建議和準則：

主題

- 先決條件
- 建立 AWS Managed Microsoft AD

先決條件

建立目錄之前，請考量這些準則。

確認目錄類型是否正確

AWS Directory Service 提供多種方式可Microsoft Active Directory與其他 AWS 服務搭配使用。您可以依所需功能及成本預算，選擇目錄服務：

- AWS Directory Service for Microsoft Active Directory 是一種功能豐富的受Microsoft Active Directory管 AWS 雲端託管。如果您有超過 5，000 名使用者，且需要在託管目錄和內部部署目錄之間 AWS 設定信任關係，則 AWS 受管 Microsoft AD 是您的最佳選擇。
- AD Connector 只會將您現有的現場部署連線到 Active Directory AWS。如果您想要將現有的內部部署目錄用於 AWS 服務，AD Connector 會是您的最佳選擇。
- Simple AD 是具有基本Active Directory相容性的低規模、低成本目錄。它支援最多 5,000 名使用者、Samba 4 相容應用程式，以及 LDAP 感知應用程式的 LDAP 相容性。

如需 AWS Directory Service 選項的更詳細比較，請參閱 該選擇哪種。

確認已正確設定您的 VPC 和執行個體

為了連線、管理及使用您的目錄，您必須正確設定與目錄相關聯的 VPC。如需 VPC 安全與聯網需求的資訊，請參閱「建立 AWS Managed Microsoft AD 的先決條件 」、「AD Connector 事前準備 」或「Simple AD 先決條件」。

如果您想要將執行個體新增至網域，請確定您具備連線能力並可遠端存取您的執行個體，如「將 Amazon EC2 執行個體加入 AWS Managed Microsoft AD 的方法」中所述。

留意您的限制

了解特定目錄類型的不同限制。您可以在目錄中儲存的物件數量僅受限於可用儲存空間和物件的彙總大小。有關所選目錄的詳細資訊，請參閱「AWS Managed Microsoft AD 配額」、「AD Connector 配額」或「Simple AD 配額」。

了解目錄 AWS 的安全群組組態和使用

AWS 會建立安全群組，並將其連接至目錄的網域控制器彈性網路介面。此安全群組會封鎖網域控制器不必要的流量，並允許Active Directory通訊所需的流量。 AWS 會設定安全群組只開啟Active Directory通訊所需的連接埠。在預設組態中，安全群組接受從 AWS Managed Microsoft AD VPC IPv4 CIDR 地址到這些連接埠的流量。 會將安全群組 AWS 連接到您的網域控制器界面，這些界面可從對等或調整大小VPCs 內存取。這些界面無法從網際網路存取，縱使您修改路由表、變更到 VPC 的網路連線與設定 NAT 閘道服務。因此，只有包含 VPC 網路路徑的執行個體和電腦才能存取目錄。由於您不需要設定特定地址範圍，因此簡化了設定作業。反之，您會設定在 VPC 的路由和安全群組，只允許來自信任執行個體和電腦的流量。

修改目錄安全群組

如果您想要提高目錄安全群組的安全性，您可以修改它們以接受來自更嚴格 IP 地址清單的流量。例如，您可以將接受的地址從 VPC IPv4 CIDR 範圍變更為單一子網路或電腦特定的 CIDR 範圍。同樣地，您可以選擇將目標地址限制為您的網域控制站可通訊的地址。請只在您完全了解安全群組篩選的運作方式時才進行這類變更。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的適用於 Linux 執行個體的 Amazon EC2 安全群組一節。不當變更可能會導致與預期電腦和執行個體的通訊中斷。 AWS 建議您不要嘗試開啟網域控制器的其他連接埠，因為這會降低目錄的安全性。請仔細檢閱 AWS 共同的責任模型。

> **Warning**
>
> 就技術而言，您可以將目錄所使用的安全群組與您所建立的其他 EC2 執行個體產生關聯。不過，針對此實務 AWS 的建議。 AWS 可能有理由修改安全群組，而不另行通知，以解決受管目錄的功能或安全需求。這類變更會影響任何與目錄安全群組相關聯的執行個體。此外，將目錄安全群組與您的 EC2 執行個體產生關聯可能會對您的 EC2 執行個體帶來安全風險。目錄安全群組接受來自 AWS Managed Microsoft AD VPC IPv4 CIDR 地址之必要Active Directory連接埠上的流量。如果您將此安全群組與具有連接到網際網路之公有 IP 地址的 EC2 執行個體產生關聯，則網際網路上的任何電腦都可以透過已開啟的連接埠與 EC2 執行個體通訊。

建立 AWS Managed Microsoft AD

以下是建立 AWS Managed Microsoft AD 時需要考慮的一些建議。

主題

- 記住您的管理員 ID 和密碼
- 建立 DHCP 選項集
- 啟用條件式轉寄站設定
- 部署其他網域控制器
- 了解 AWS 應用程式的使用者名稱限制

記住您的管理員 ID 和密碼

在您設定目錄時，您會提供管理員帳戶的密碼。該帳戶 ID 是 AWS Managed Microsoft AD 的 Admin。請記住您為此帳戶建立的密碼，否則您將無法新增物件至目錄。

建立 DHCP 選項集

我們建議您為 AWS Directory Service 目錄建立 DHCP 選項集，並將 DHCP 選項集指派給目錄所在的 VPC。如此一來，該 VPC 中的任何執行個體可以指向指定的網域，而且 DNS 伺服器可以解析其網域名稱。

如需 DHCP 選項集的詳細資訊，請參閱「建立或變更 AWS Managed Microsoft AD 的 DHCP 選項集」。

啟用條件式轉寄站設定

下列條件式轉送設定 將此條件式轉送器存放在 Active Directory 中，複寫如下：應啟用。當節點因基礎設施故障或過載故障而遭到取代時，啟用這些設定將確保條件式轉寄站設定持續存在。

條件式轉寄站應在已啟用先前設定的網域控制站上建立。這將允許複寫到其他網域控制站。

部署其他網域控制器

根據預設， 會 AWS 建立存在於不同可用區域中的兩個網域控制站。如此可在軟體修補期間，以及可能讓一個網域控制器無法連線或無法使用的其他事件期間，提供錯誤復原力。我們建議部署其他網域控制器，以進一步增加復原力，並在影響網域控制器或可用區域存取的長期事件發生時，確保向外擴展效能。

如需詳細資訊，請參閱使用 Windows DC 定位器服務。

了解 AWS 應用程式的使用者名稱限制

AWS Directory Service 支援可用於建構使用者名稱的大多數字元格式。不過，在用於登入 AWS 應用程式的使用者名稱上會強制執行字元限制，例如 WorkSpaces、WorkDocs、Amazon WorkMail 或 QuickSight。這些限制要求不使用下列字元：

- 空格
- 多位元組字元
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> @ 符號只可位於 UPN 尾碼之前。

使用 AWS Managed Microsoft AD 目錄時的最佳實務

以下是使用 AWS Managed Microsoft AD 時需要記住的一些建議。

主題

- 請勿改變預先定義的使用者、群組和組織單位
- 自動加入域

- 正確設定信任
- 追蹤域控制站效能
- 仔細規劃結構描述延伸
- 關於負載平衡器
- 備份您的執行個體
- 設定 SNS 簡訊
- 應用程式目錄服務設定
- 刪除目錄前先移除 Amazon 企業應用程式
- 存取 SYSVOL 和 NETLOGON 共用時，請使用 SMB 2.x 用戶端

請勿改變預先定義的使用者、群組和組織單位

當您使用 AWS Directory Service 啟動目錄時， AWS 會建立組織單位 (OU)，其中包含您目錄的所有物件。此 OU 有您在建立目錄時所輸入的 NetBIOS 名稱，位於根網域中。網域根由 擁有和管理 AWS。這也會建立數個群組和管理使用者。

請勿移動、刪除或透過其他方式來改變這些預先定義的物件。這樣做會使您自己和 無法存取您的目錄 AWS。如需詳細資訊，請參閱使用 AWS Managed Microsoft AD 建立的內容。

自動加入域

啟動要成為 AWS Directory Service 網域一部分的 Windows 執行個體時，通常最容易將網域加入執行個體建立程序，而不是稍後手動新增執行個體。若要自動加入網域，只要在啟動新的執行個體時，針對 Domain join directory (網域加入目錄) 選取正確的目錄即可。您可以在「將 Amazon EC2 Windows 執行個體加入您的 AWS Managed Microsoft AD Active Directory」中找到詳細資訊。

正確設定信任

在 AWS Managed Microsoft AD 目錄和另一個目錄之間設定信任關係時，請記住下列準則：

- 信任類型必須在雙方比對 (樹系或外部)
- 如果使用單向信任 (信任網域上的外寄、可信任網域上的傳入)，請確定已正確設定信任方向
- 完整網域名稱 (FQDN) 和 NetBIOS 名稱在樹系/網域之間必須是唯一的

如需設定信任關係的詳細資訊與特定說明，請參閱「在 AWS Managed Microsoft AD 和自我管理 AD 之間建立信任關係」。

追蹤域控制站效能

為了協助最佳化擴展決策，並提高目錄彈性和效能，我們建議您使用 CloudWatch 指標。如需詳細資訊，請參閱使用 CloudWatch 監控 AWS Managed Microsoft AD 網域控制站的效能。

如需如何使用 CloudWatch 主控台設定網域控制器指標的指示，請參閱 安全部落格中的 AWS 如何根據使用率指標自動化 AWS Managed Microsoft AD 擴展。

仔細規劃結構描述延伸

經仔細考量後，套用結構描述延伸以建立目錄索引，供重要及頻繁查詢。請小心避免建立過多索引，因為索引會佔用目錄空間，而快速變更索引值會導致效能問題。若要新增索引，您必須建立輕量型目錄存取協定 (LDAP) 目錄交換格式 (LDIF) 檔案，並延伸您的結構描述變更。如需詳細資訊，請參閱擴展您的 AWS Managed Microsoft AD 結構描述。

關於負載平衡器

請勿在 AWS Managed Microsoft AD 端點前面使用負載平衡器。 Microsoft設計 Active Directory(AD) 用於與網域控制器 (DC) 探索演算法搭配使用，該演算法會尋找反應最靈敏的操作 DC，無需外部負載平衡。外部網路負載平衡器會錯誤偵測作用中的 DC，進而將您的應用程式傳送到尚未投入使用的 DC。如需詳細資訊，請參閱 Microsoft TechNet 上的負載平衡器和 Active Directory，其建議修正應用程式以正確使用 Active Directory，而不是實作外部負載平衡器。

備份您的執行個體

如果您決定手動將執行個體新增至現有 AWS Directory Service 網域，請先備份或拍攝該執行個體的快照。這在加入 Linux 執行個體時特別重要。某些用來新增執行個體的程序若未正確執行，可能會導致您的執行個體無法連線或無法使用。如需詳細資訊，請參閱使用快照還原 AWS Managed Microsoft AD。

設定 SNS 簡訊

使用 Amazon Simple Notification Service (Amazon SNS)，當目錄狀態有所變更時，您便可以收到電子郵件或文字 (SMS) 簡訊。如果您的目錄從 Active (作用中) 狀態變成 Impaired (受損) 或 Inoperable (無法操作) 狀態，您就會收到通知。當目錄恢復到 Active (作用中) 狀態時，您也會收到通知。

另外請記住，如果您有接收訊息的 SNS 主題 AWS Directory Service，在從 Amazon SNS 主控台刪除該主題之前，您應該將目錄與不同的 SNS 主題建立關聯。否則會有遺漏重要目錄狀態訊息的風險。如需如何設定 Amazon SNS 的資訊，請參閱 使用 Amazon Simple Notification Service 啟用 AWS Managed Microsoft AD 目錄狀態通知。

應用程式目錄服務設定

AWS Managed Microsoft AD 可讓您量身打造安全組態以符合您的合規和安全需求。 AWS Managed Microsoft AD 會將組態部署和維護到目錄中的所有網域控制站，包括新增區域或其他網域控制站時。您可以為所有新目錄和現有目錄設定和套用這些安全設定。您可以在主控台中按照 編輯目錄安全設定 中描述的步驟或透過 UpdateSettings API 執行此操作。

如需詳細資訊，請參閱編輯 AWS Managed Microsoft AD 目錄安全設定。

刪除目錄前先移除 Amazon 企業應用程式

在刪除與一或多個 Amazon Enterprise 應用程式相關聯的目錄之前，例如 WorkSpaces、Amazon WorkSpaces Application Manager、WorkDocs AWS Management Console、Amazon WorkMail 或 Amazon Relational Database Service (Amazon RDS)，您必須先移除每個應用程式。如需移除應用程式的詳細資訊，請參閱刪除您的 AWS Managed Microsoft AD相關文章。

存取 SYSVOL 和 NETLOGON 共用時，請使用 SMB 2.x 用戶端

用戶端電腦使用伺服器訊息區塊 (SMB) 來存取 AWS Managed Microsoft AD 網域控制站上的 SYSVOL 和 NETLOGON 共用，適用於群組政策、登入指令碼和其他檔案。 AWS Managed Microsoft AD 僅支援 SMB 2.0 版 (SMBv2) 和更新版本。

SMBv2 和較新版本通訊協定會新增多項功能，以改善用戶端效能，並增加網域控制器和用戶端的安全性。這項變更遵循美國電腦緊急應變小組和 Microsoft 的建議來停用 SMBv1。

> **Important**
>
> 如果您目前使用 SMBv1 用戶端來存取網域控制器的 SYSVOL 和 NETLOGON 共用，您必須更新那些用戶端，以使用 SMBv2 或更新版本。您的目錄將正常運作，但 SMBv1 用戶端將無法連線至 AWS Managed Microsoft AD 網域控制站的 SYSVOL 和 NETLOGON 共用，也無法處理群組政策。

SMBv1 用戶端將使用您擁有的任何其他 SMBv1 相容檔案伺服器。不過， AWS 建議您將所有 SMB 伺服器和用戶端更新為 SMBv2 或更新版本。若要進一步了解如何在系統上停用 SMBv1 並將其更新為較新的 SMB 版本，請參閱 Microsoft TechNet 和 Microsoft 文件上的這些文章。

追蹤 SMBv1 遠端連線

您可以檢閱從遠端連線至 AWS Managed Microsoft AD 網域控制器的 Microsoft-Windows-SMBServer/Audit Windows 事件日誌，此日誌中的任何事件都會指出 SMBv1 連線。以下是您在其中一個日誌中可能會看到的資訊範例：

SMB1 存取權

客戶地址：###.###.###.###

指導：

此事件表示用戶端嘗試使用 SMB1 存取伺服器。若要停止稽核 SMB1 存取，請使用 PowerShell cmdlet Set-SmbServerConfiguration。

程式設計 AWS Managed Microsoft AD 應用程式時的最佳實務

在您編寫應用程式以使用 AWS Managed Microsoft AD 之前，請考慮下列事項：

主題

- 使用 Windows DC 定位器服務
- 投入生產前先進行負載測試
- 使用高效 LDAP 查詢

使用 Windows DC 定位器服務

開發應用程式時，請使用 Windows DC 定位器服務，或使用 AWS Managed Microsoft AD 的動態 DNS (DDNS) 服務來尋找網域控制站 DCs)。請勿使用 DC 地址將應用程式寫死在程式碼中。DC 定位器服務可新增網域控制站到您的部署，協助確保目錄負載分散並讓您充分利用水平擴展。如果您將應用程式繫結到固定的 DC，而該 DC 正在進行修補或復原，則您的應用程式將無法存取該 DC，而不會使用其中一個剩餘的 DC。此外，DC 硬編碼會導致單一 DC 產生熱點。在嚴重的情況下，熱點可能會導致您的 DC 無法回應。這類情況也可能導致 AWS 目錄自動化將目錄標記為受損，並可能觸發取代無回應 DC 的復原程序。

投入生產前先進行負載測試

請務必針對代表您的生產工作負載的物件與請求執行實驗室測試，以確認目錄擴展至您的應用程式負載。如果您需要更多容量，請測試額外的 DC 並在 DC 之間發佈請求。如需詳細資訊，請參閱部署 AWS Managed Microsoft AD 的其他網域控制站。

使用高效 LDAP 查詢

從上萬個物件針對網域控制站執行廣泛 LDAP 查詢，會佔用單一 DC 的大量 CPU 周期，進而產生熱點現象。這可能會導致查詢期間使用相同 DC 的應用程式受到影響。

AWS Managed Microsoft AD 的使用案例

使用 AWS Managed Microsoft AD，您可以針對多個使用案例共用單一目錄。例如，您可以共用目錄來驗證和授權 .NET 應用程式、Amazon RDS for SQL Server (已啟用 Windows 驗證) 以及 Amazon Chime (用於傳訊及視訊會議) 的存取。

下圖顯示 AWS Managed Microsoft AD 目錄的一些使用案例。這包括授予使用者存取外部雲端應用程式的能力，並允許內部部署 Active Directory 使用者管理和存取 AWS 雲端中的資源。

將 AWS Managed Microsoft AD 用於下列任一商業使用案例。

主題

- 使用案例 1：使用Active Directory登入資料登入 AWS 應用程式和服務
- 使用案例 2：管理 Amazon EC2 執行個體
- 使用案例 3：為您的 Active Directory感知工作負載提供目錄服務
- 使用案例 4： AWS IAM Identity Center 至 Office 365 和其他雲端應用程式
- 使用案例 5：將您的內部部署擴展Active Directory到 AWS 雲端
- 使用案例 6：共用您的目錄，以順暢地將 Amazon EC2 執行個體加入跨 AWS 帳戶的網域

使用案例 1：使用Active Directory登入資料登入 AWS 應用程式和服務

您可以啟用多個 AWS 應用程式和服務，例如 AWS Client VPN、AWS Management Console、AWS IAM Identity Center、Amazon Chime、Amazon Connect、Amazon FSx、QuickSight、Amazon RDS for SQL Server、WorkDocs、Amazon WorkMail 和 WorkSpaces，以使用您的 AWS Managed Microsoft AD 目錄。當您在目錄中啟用 AWS 應用程式或服務時，您的使用者可以使用其Active Directory登入資料來存取應用程式或服務。

例如，您可以讓使用者AWS Management Console 使用其Active Directory登入資料登入 。若要這樣做，請在 目錄中啟用 AWS Management Console 做為應用程式，然後將您的Active Directory使用者和群組指派給 IAM 角色。當您的使用者登入 時 AWS Management Console，他們會擔任 IAM 角色來

管理 AWS 資源。這讓您能夠輕鬆地授予使用者對 AWS Management Console 的存取權，無需另外設定和管理 SAML 基礎設施。

若要進一步增強最終使用者體驗，您可以為 WorkDocs 啟用單一登入功能，這可讓您的使用者從加入目錄的電腦存取 WorkDocs，而不必另外輸入登入資料。

您可以授予目錄或內部部署 Active Directory 中使用者帳戶的存取權，讓他們可以使用 AWS CLI 現有的登入資料和許可登入 AWS Management Console ，或透過 將 IAM 角色直接指派給現有的使用者帳戶來管理 AWS 資源。

FSx for Windows File Server 與 AWS Managed Microsoft AD 整合

整合 FSx for Windows File Server 與 AWS Managed Microsoft AD 提供全受管的原生 Microsoft Windows 型伺服器訊息區塊 (SMB) 通訊協定檔案系統，可讓您輕鬆地將 Windows 型應用程式和用戶端（使用共用檔案儲存）移至其中 AWS。儘管 FSx for Windows File Server 可以與自我管理的 Microsoft Active Directory 整合，但我們在此不討論這一主題。

Amazon FSx 常見使用案例和資源

本節提供常見 FSx for Windows File Server 與 AWS Managed Microsoft AD 使用案例整合的資源參考。本節中的每個使用案例均從基本的 AWS Managed Microsoft AD 和 FSx for Windows File Server 組態出發。如需建立這些組態的詳細資訊，請參閱：

- Managed AWS Microsoft AD 入門
- Amazon FSx 入門

FSx for Windows File Server 作為 Windows 容器上的持久性儲存

Amazon Elastic Container Service (ECS) 現已於使用 Amazon ECS 最佳化 Windows AMI 啟動的容器執行個體上支援 Windows 容器。Windows 容器執行個體使用其專屬的 Amazon ECS 容器代理程式的版本。在 Amazon ECS 最佳化 Windows AMI 上，Amazon ECS 容器代理程式做為一項服務在主機上執行。

Amazon ECS 透過名為群組受管服務帳戶 (gMSA) 的特殊類型的服務帳戶，支援對 Windows 容器的 Active Directory 身分驗證。由於以 Windows 為基礎的容器無法加入網域，因此您必須將 Windows 容器設定為與 gMSA 搭配執行。

相關項目

- 將 FSx for Windows File Server 作為 Windows 容器上的持久性儲存

- 群組受管服務帳戶

Amazon AppStream 2.0 支援

Amazon AppStream 2.0 是一項全受管的應用程式串流服務。它為使用者透過應用程式儲存和存取資料提供了一系列解決方案。Amazon FSx 與 AppStream 2.0 搭配使用提供使用 Amazon FSx 的個人持久性儲存磁碟機，並且可以設定為提供共用資料夾用於存取常見檔案。

相關項目

- Walkthrough 4: Using Amazon FSx with Amazon AppStream 2.0
- Using Amazon FSx with Amazon AppStream 2.0
- Using Active Directory with AppStream 2.0

Microsoft SQL Server 支援

FSx for Windows File Server 可用作 Microsoft SQL Server 2012 (從 2012 版本 11.x 開始) 和較新的系統資料庫 (包括 Master、Model、MSDB 和 TempDB)，以及資料庫引擎使用者資料庫的儲存選項。

相關項目

- 安裝 SQL Server 與 SMB 檔案共用儲存體
- Simplify your Microsoft SQL Server high availability deployments using FSx for Windows File Server
- 群組受管服務帳戶

主資料夾和漫遊使用者設定檔支援

FSx for Windows File Server 可用來將Active Directory使用者主資料夾和我的文件的資料存放在中央位置。FSx for Windows File Server 還可用於儲存漫遊使用者設定檔中的資料。

相關項目

- Windows home directories made easy with Amazon FSx
- 部署漫遊使用者設定檔
- Using FSx for Windows File Server with WorkSpaces

網路檔案共用支援

FSx for Windows File Server 上的網路檔案共用提供受管且可擴展的檔案共用解決方案。一種使用案例是用作可以手動或透過群組政策建立的用戶端的映射磁碟機。

相關項目

- Walkthrough 6: Scaling out performance with Shards
- Drive mapping
- Using FSx for Windows File Server with WorkSpaces

群組政策軟體安裝支援

由於 SYSVOL 資料夾的大小和效能有限，因此最佳實務是避免在該資料夾中儲存軟體安裝檔案等資料。此問題的一種可能解決方案是，將 FSx for Windows File Server 設定為儲存使用群組政策安裝的所有軟體檔案。

相關項目

- 使用群組政策遠端安裝軟體

Windows Server Backup 目標支援

可以將 FSx for Windows File Server 設定為 Windows Server Backup 中使用 UNC 檔案共用的目標磁碟機。在這種情況下，您將指定 FSx for Windows File Server 而不是連接的 EBS 磁碟區的 UNC 路徑。

相關項目

- Perform a system state recovery of your server

Amazon FSx 也支援 AWS Managed Microsoft AD Directory Sharing。如需詳細資訊，請參閱：

- 共用您的 AWS Managed Microsoft AD
- 在不同的 VPC 或帳戶中使用 Amazon FSx 搭配 AWS Managed Microsoft AD

Amazon RDS 與 AWS Managed Microsoft AD 整合

Amazon RDS 支援透過 Kerberos 與 Microsoft Active Directory 對資料庫使用者進行外部身分驗證。Kerberos 是網路身分驗證通訊協定，使用票證和對稱式金鑰加密技術，免除透過網路傳輸密碼的需要。Amazon RDS 對 Kerberos 和 Active Directory 的支援，提供了資料庫使用者的單一登入和集中式身分驗證優點，讓您可以將使用者憑證存放在 Active Directory 中。

若要開始使用此使用案例，您必須先設定基本的 AWS Managed Microsoft AD 和 Amazon RDS 組態。

- Managed AWS Microsoft AD 入門
- Amazon RDS 入門

以下參考的所有使用案例將從基礎 AWS Managed Microsoft AD 和 Amazon RDS 開始，並涵蓋如何整合 Amazon RDS 與 AWS Managed Microsoft AD。

- 為 Amazon RDS for SQL Server 資料庫執行個體設定 Windows 身分驗證
- 為 MySQL 設定 Kerberos 身分驗證
- 為 Amazon RDS for Oracle 設定 Kerberos 身分驗證
- 為 Amazon RDS for PostgreSQL 設定 Kerberos 身分驗證

Amazon RDS 也支援 AWS Managed Microsoft AD Directory Sharing。如需詳細資訊，請參閱：

- 共用您的 AWS Managed Microsoft AD
- 在多個帳戶之間將 Amazon RDS 資料庫執行個體加入單一共用域

如需有關將 Amazon RDS for SQL Server 加入到 Active Directory 的詳細資訊，請參閱 Join Amazon RDS for SQL Server to your self-managed Active Directory 一文。

使用 Amazon RDS for SQL Server 和群組受管服務帳戶的 .NET 應用程式

您可以將 Amazon RDS for SQL Server 與基本 .NET 應用程式和群組受管服務帳戶 (gMSA) 整合。如需詳細資訊，請參閱 AWS Managed Microsoft AD 如何協助簡化部署並改善 Active Directory 整合的 .NET 應用程式的安全性

使用案例 2：管理 Amazon EC2 執行個體

使用熟悉的Active Directory管理工具，您可以將執行個體加入 Managed Microsoft AD 網域，以套用Active Directory群組政策物件 (GPOs) 來集中管理 Amazon EC2 for Windows 或 Linux 執行個體。AWS

此外，您的使用者可以使用其Active Directory登入資料登入您的執行個體。如此一來，您不需要使用個別執行個體登入資料或分佈私有金鑰 (PEM) 檔案。這可讓您使用已使用的使用者管理工具，更輕鬆地立即授予或撤銷Active Directory使用者存取權。

使用案例 3：為您的 Active Directory感知工作負載提供目錄服務

AWS Managed Microsoft AD 是實際可讓您在 AWS 雲端執行傳統 Active Directory感知工作負載MicrosoftActive Directory，例如遠端桌面授權管理員、MicrosoftSharePoint 和 Microsoft SQL Server Always On。 AWS 受管 Microsoft AD 也可協助您使用群組受管服務帳戶 (gMSAs) 和 Kerberos 限制委派 (KCD)，簡化並改善 Active Directory 整合 .NET 應用程式的安全性。

使用案例 4： AWS IAM Identity Center 至 Office 365 和其他雲端應用程式

您可以使用 AWS Managed Microsoft AD 為雲端應用程式 AWS IAM Identity Center 提供服務。您可以使用 Microsoft Entra Connect（先前稱為 Azure Active Directory Connect) 將使用者同步至 Microsoft Entra（先前稱為 Azure Active Directory(Azure AD))，然後使用Active Directory聯合服務 (AD FS)，以便您的使用者能夠使用其Active Directory憑證存取 Microsoft Office 365 和其他 SAML 2.0 雲端應用程式。

整合 AWS Managed Microsoft AD 與 IAM Identity Center 會將 SAML 功能新增至 AWS Managed Microsoft AD 和/或內部部署信任網域。整合之後，您的使用者可以將 IAM Identity Center 與支援 SAML 的服務搭配使用，包括 AWS Management Console 和第三方雲端應用程式，例如 Office 365、Concur 和 Salesforce，而無需設定 SAML 基礎設施。如需允許內部部署使用者使用 IAM Identity Center 的流程示範，請觀賞下面的 YouTube 影片。

> **Note**
>
> AWS 單一登入已重新命名為 IAM Identity Center。

使用案例 5：將您的內部部署擴展Active Directory到 AWS 雲端

如果您已經有 Active Directory基礎設施，並想要在將 Active Directory感知工作負載遷移至 時使用它 AWS 雲端， AWS 受管 Microsoft AD 可以提供協助。您可以使用Active Directory信任將 AWS Managed Microsoft AD 連線到現有的 Active Directory。這表示您的使用者可以使用其內部部署Active Directory登入資料存取 Active Directory感知和 AWS 應用程式，而不需要您同步使用者、群組或密碼。

例如，您的使用者可以使用現有的Active Directory使用者名稱和密碼登入 和 AWS Management Console Amazon WorkSpaces。此外，當您使用 Active Directory感知應用程式，例如 SharePoint 搭配 AWS Managed Microsoft AD 時，您的登入Windows使用者可以存取這些應用程式，而不需要再次輸入登入資料。

您也可以使用 Active Directory Migration Toolkit (ADMT) 和 Password Export Service (PES) 來執行遷移，將內部部署Active Directory網域遷移 AWS 至 ，以避免Active Directory基礎設施的操作負擔。

使用案例 6：共用您的目錄，以順暢地將 Amazon EC2 執行個體加入跨 AWS 帳戶的網域

跨多個 AWS 帳戶共用目錄可讓您輕鬆管理 Amazon EC2 等 AWS 服務，而無需為每個帳戶和每個 VPC 操作目錄。您可以從任何 AWS 帳戶、以及從任何 Amazon VPC (位於 AWS 區域) 來使用目錄。運用這個功能，您可以使用跨多個帳戶和 VPC 的單一目錄，管理目錄感知的工作負載，過程更為輕鬆，更符合成本效益。例如，您現在可以使用單一 AWS Managed Microsoft AD 目錄輕鬆管理跨多個帳戶和 VPC 部署在 EC2 執行個體中的 Windows 工作負載。

當您與另一個 AWS 帳戶共用 AWS Managed Microsoft AD 目錄時，您可以使用 Amazon EC2 主控台AWS Systems Manager，或從帳戶和 AWS 區域中的任何 Amazon VPC 無縫加入執行個體。省去手動將您的執行個體加入網域、或是在各個帳戶及 VPC 中部署目錄的必要作業，您就能在 EC2 執行個體上快速部署目錄感知的工作負載。如需詳細資訊，請參閱共用您的 AWS Managed Microsoft AD。

維護您的 AWS Managed Microsoft AD

您可以使用 AWS Management Console 來維護 AWS Managed Microsoft AD day-to-day管理任務。您可以維護目錄的方式包括：

- 檢視 AWS Managed Microsoft AD 目錄詳細資訊，以了解 AWS Managed Microsoft AD 目錄類型、目錄 ID、目錄狀態和聯網詳細資訊，例如其 Amazon VPC、子網路和可用區域。

- 使用快照還原 AWS Managed Microsoft AD。您也可以建立快照和刪除快照。
- 部署其他網域控制站，以改善 AWS Managed Microsoft AD 效能和可用性。
- 將您的 AWS Managed Microsoft AD 從標準版本升級至支援更多目錄物件的企業版本。
- 新增備用使用者主體名稱 (UPN)，以改善使用者登入體驗。
- 重新命名您的 AWS Managed Microsoft AD 網站名稱，以改善 AWS Managed Microsoft AD 在內部部署目錄中尋找和驗證現有 Active Directory 使用者的能力。
- 當您不再需要 AWS Managed Microsoft AD 時將其刪除。

檢視 AWS Managed Microsoft AD 目錄資訊

您可以使用 檢視 AWS Managed Microsoft AD 目錄詳細資訊 AWS Management Console ，例如：

- 目錄類型
- 目錄 ID
- 目錄狀態
- AWS Managed Microsoft AD 的網路詳細資訊，例如：
  - Amazon VPC
  - 子網路
  - 可用區域
  - DNS 地址

您可以找到有關 AWS Managed Microsoft AD 的下列資訊：

- 在共用與共用索引標籤下，您可以與其他 共用 AWS Managed Microsoft AD， AWS 帳戶 並了解網域控制站的網路詳細資訊。
- 在應用程式管理索引標籤下，您可以為 AWS Managed Microsoft AD 啟用應用程式存取 URL，並為 AWS Managed Microsoft AD 啟用 AWS 應用程式和服務。
- 在維護索引標籤下，您可以讓 Amazon Simple Notification Service 接收 AWS Managed Microsoft AD 狀態的通知，並檢閱 AWS Managed Microsoft AD 的快照。
- 如需 Status (狀態) 欄位的詳細資訊，請參閱「了解 AWS Managed Microsoft AD 目錄狀態」。

您可以使用 AWS Management Console AWS CLI或 來檢視 AWS Managed Microsoft AD 目錄資訊 PowerShell：

AWS Management Console

檢視詳細目錄資訊

1. 在AWS Directory Service 主控台導覽窗格中的 下Active Directory，選取目錄。
2. 選擇您目錄的目錄 ID 連結。目錄的相關資訊會顯示在目錄詳細資訊頁面。

AWS CLI

使用 檢視詳細目錄資訊 AWS CLI

- 開啟 AWS CLI。若要檢視 AWS Managed Microsoft AD 目錄資訊，請執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
aws ds describe-directories --directory-id d-1234567890 --output table
```

如需詳細資訊，請參閱describe-directories。

PowerShell

使用 檢視詳細目錄資訊 PowerShell

- 打開 PowerShell. 若要檢視 AWS Managed Microsoft AD 目錄資訊，請執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
(Get-DSDirectory -DirectoryId d-1234567890 |
    ForEach-Object {$_, $_.RegionsInfo, $_.VpcSettings}) |
Format-List *
```

如需詳細資訊，請參閱Get-DSDirectory。

使用快照還原 AWS Managed Microsoft AD

AWS Directory Service 提供自動化每日快照，並能夠為 AWS Managed Microsoft AD 手動拍攝資料快照Active Directory。這些快照可用來為您的 執行point-in-time還原Active Directory。每個 AWS Managed Microsoft AD 限制為五個手動快照Active Directory。如果您已達到此上限，則必須刪除其中一個現有的手動快照，才能建立其他手動快照。您無法擷取 AD Connector 目錄的快照。

> **Note**
>
> 快照是 AWS Managed Microsoft AD 的全域功能。如果您使用 設定 AWS Managed Microsoft AD 的多區域複寫，則必須在 主要區域 中執行下列步驟。變更將自動套用至所有複寫區域。如需詳細資訊，請參閱全域與區域功能。

主題

- 建立目錄的快照
- 從快照還原您的目錄
- 刪除快照

建立目錄的快照

您可以使用快照，將目錄還原到擷取快照的時間點。若要建立您目錄的手動快照，請執行下列步驟。

> **Note**
>
> 每個目錄只能建立 5 個手動快照。如果您已達到此上限，則必須刪除其中一個現有的手動快照，才能建立其他手動快照。

使用下列程序，透過 AWS CLI AWS Management Console、 或 建立 AWS Managed Microsoft AD 的手動快照PowerShell：

AWS Management Console

在 中建立手動快照 AWS Management Console

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，選擇維護 索引標籤。
4. 在快照區段中，選擇動作，然後選取建立快照。
5. 在 建立目錄快照對話方塊中，提供快照的名稱 (如果需要)。準備就緒時，選擇建立。

AWS CLI

使用 建立手動快照 AWS CLI

- 開啟 AWS CLI。若要建立 AWS Managed Microsoft AD 的快照，請執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
aws ds create-snapshot --directory-id d-1234567890 --name ManualSnapshot
```

如需詳細資訊，請參閱create-snapshot。

PowerShell

使用 建立手動快照 PowerShell

- 打開 PowerShell. 若要建立 AWS Managed Microsoft AD 的快照，請執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
New-DSSnapshot -DirectoryId d-1234567890 -Name ManualSnapshot
```

如需詳細資訊，請參閱New-DSSnapshot。

根據您的目錄大小，建立快照可能需要幾分鐘。快照準備就緒時，Status (狀態) 值會變更為 Completed (已完成)。

從快照還原您的目錄

從快照還原目錄等同於回到過去的目錄。目錄快照對於它們的建立來源目錄而言是唯一的。一個快照只能還原到建立它的來源目錄。此外，手動快照的支援保留期限上限為 180 天。如需詳細資訊，請參閱 Microsoft 網站上的 系統狀態備份的實用保存期限Active Directory。

> **Warning**
>
> 我們建議您在進行任何快照還原之前聯絡 AWS 支援 中心；我們也許能夠協助您避免執行快照還原。系統會從時間點進行還原，因此快照還原可能導致資料遺失。請務必了解在完成還原操作之前，所有與目錄相關聯的 DC 和 DNS 伺服器都會處於離線狀態。

使用下列程序，使用 AWS CLI、 AWS Management Console或 從快照還原您的目錄PowerShell：

AWS Management Console

從 中的快照還原目錄 AWS Management Console

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，選擇維護 索引標籤。
4. 在快照區段中，選取清單中的快照，選擇動作，然後選取還原快照。
5. 檢閱還原目錄快照對話方塊中的資訊，然後選擇還原。

AWS CLI

使用 從快照還原目錄 AWS CLI

1. 開啟 AWS CLI。若要列出 AWS Managed Microsoft AD 的快照，請執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
aws ds describe-snapshots --directory-id d-1234567890 \
  --query '(sort_by(Snapshots[*].
{ID:SnapshotId,Status:Status,Type:Type,StartTime:StartTime}, &StartTime))' \
  --output table
```

2. 若要從快照還原 AWS Managed Microsoft AD，您可以使用 restore-from-snapshot命令。請確定以您要用來還原 AWS Managed Microsoft AD 的快照 ID 取代 `snapshot-id` 參數：

```
aws ds restore-from-snapshot --snapshot-id s-1234567890
```

PowerShell

使用 從快照還原目錄 PowerShell

1. 打開 PowerShell. 若要列出 AWS Managed Microsoft AD 的快照，請執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
Get-DSSnapshot -DirectoryId d-1234567890 | Sort-Object StartTime | Format-Table
```

2. 若要從快照還原 AWS Managed Microsoft AD，您可以使用 Restore-DSFromSnapshot命令。請確定以您要用來還原 AWS Managed Microsoft AD 的快照 ID 取代 snapshot-id 參數：

```
Restore-DSFromSnapshot -SnapshotId s-1234567890
```

對於 AWS Managed Microsoft AD 目錄，目錄可能需要兩到三小時才能還原。成功還原之後，目錄的狀態值會變更為 Active。快照日期之後所進行的任何目錄變更都會遭到覆寫。

刪除快照

使用下列程序，透過 AWS CLI AWS Management Console、 或 刪除 AWS Managed Microsoft AD 的快照PowerShell：

AWS Management Console

在 中刪除快照 AWS Management Console

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，選擇維護 索引標籤。
4. 在快照區段中，選擇動作，然後選取刪除快照。
5. 確認您要刪除快照，然後選擇刪除。

AWS CLI

使用 刪除快照 AWS CLI

1. 開啟 AWS CLI。若要列出 AWS Managed Microsoft AD 的快照，請執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
aws ds describe-snapshots --directory-id d-1234567890 \
  --query '(sort_by(Snapshots[*].
{ID:SnapshotId,Status:Status,Type:Type,StartTime:StartTime}, &StartTime))' \
  --output table
```

2. 若要刪除 AWS Managed Microsoft AD 的快照，您可以使用 delete-snapshot命令。請確定以您要刪除的快照 ID 取代 snapshot-id 參數：

```
aws ds delete-snapshot --snapshot-id s-1234567890
```

PowerShell

使用 刪除快照 PowerShell

1. 打開 PowerShell. 若要列出 AWS Managed Microsoft AD 的快照，請執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
Get-DSSnapshot -DirectoryId d-1234567890 | Sort-Object StartTime | Format-Table
```

2. 若要從快照還原 AWS Managed Microsoft AD，您可以使用 Remove-DSnapshot命令。請確定以您要刪除的快照 ID 取代 `snapshot-id` 參數：

```
Remove-DSSnapshot -SnapshotId s-1234567890
```

部署 AWS Managed Microsoft AD 的其他網域控制站

部署 AWS Managed Microsoft AD 的其他網域控制站會增加備援，進而產生更高的彈性和更高的可用性。這也支援更多Active Directory請求來改善目錄的效能。例如，您現在可以使用 AWS Managed Microsoft AD 來支援部署在 Amazon EC2 和 Amazon RDS for SQL Server 執行個體的大型機群上的多個 .NET 應用程式。

當您第一次建立目錄時， AWS 受管 Microsoft AD 會在多個可用區域之間部署兩個網域控制站，這是高可用性用途的必要項目。稍後，您只需指定所需的網域控制站總數，即可透過 AWS Directory Service 主控台輕鬆部署其他網域控制站。 AWS 受管 Microsoft AD 會將其他網域控制站分發到執行目錄的可用區域和 Amazon VPC 子網路。

例如，在下圖中，DC-1 和 DC-2 代表最初使用您的目錄建立的兩個網域控制器。 AWS Directory Service 主控台會將這些預設網域控制站稱為必要。 AWS 受管 Microsoft AD 會在目錄建立程序期間，刻意將每個網域控制站定位在個別的可用區域中。稍後，您可能決定新增其他兩個網域控制器，以協助分發尖峰登入時的驗證負載。DC-3 和 DC-4 代表新的網域控制器，主控台現在將其稱為 Additional (其他)。如同之前， AWS 受管 Microsoft AD 會自動將新的網域控制站放在不同的可用區域，以確保您網域的高可用性。

此程序讓您不需要手動設定目錄資料複寫、自動化每日快照，或監控其他網域控制器。您也可以更輕鬆地在 中 AWS 雲端 遷移和執行關鍵任務Active Directory整合工作負載，而不必部署和維護自己的Active Directory基礎設施。

您可以使用下列任一工具，將其他網域控制站部署或移除至 AWS Managed Microsoft AD：

- `update-number-of-domain-controllers` AWS CLI 命令
- UpdateNumberOfDomainControllers API
- 使用 新增或移除其他網域控制站 AWS Management Console

> **Note**
>
> 其他網域控制站是 AWS Managed Microsoft AD 的區域功能。如果您使用的是多區域複寫，則必須在每個區域中分別套用下列程序。如需詳細資訊，請參閱全域與區域功能。

使用 新增或移除其他網域控制站 AWS Management Console

您可以使用 AWS Management Console 來新增或移除 AWS Managed Microsoft AD 的其他網域控制站。

先決條件

在將其他網域控制站新增至 AWS Managed Microsoft AD 或移除其他網域控制站之前，以下是網域控制站需求的詳細資訊：

- 部署其他網域控制器之後，您可以將網域控制器數量減少為兩個，這是達到容錯能力和高可用性目的所需的下限。
- 刪除的域控制站將從其他域控制站清單中刪除。主要域控制站和輔助域控制站是必要的且無法刪除。
- 如果您已將 AWS Managed Microsoft AD 設定為啟用 LDAPS，則您新增的任何其他網域控制站也會自動啟用 LDAPS。如需詳細資訊，請參閱啟用安全 LDAP 或 LDAPS。

程序

使用下列程序，透過 或 來部署或移除 AWS Managed Microsoft AD AWS Management Console AWS CLI中的其他網域控制站PowerShell。

AWS Management Console

使用 新增或移除其他網域控制站 AWS Management Console

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要新增或移除域控制站的區域，然後選擇擴展和共享索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇擴展和共享索引標籤。
4. 在 Domain controllers (網域控制器) 區段，選擇 Edit (編輯)。
5. 指定要在您的目錄中新增或移除的網域控制器數量，然後選擇 Modify (修改)。
6. 當 AWS Managed Microsoft AD 完成部署程序時，所有網域控制站都會顯示作用中狀態，並同時顯示指派的可用區域和 Amazon VPC 子網路。新的網域控制器會平均分發到已部署您目錄的可用區域和子網路。

AWS CLI

使用 新增或移除其他網域控制站 AWS CLI

1. 開啟 AWS CLI。若要檢查目前網域控制站的數量，請執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
aws ds describe-directories --directory-id d-1234567890 | grep
 DesiredNumberOfDomainControllers
```

2. 若要新增或移除網域控制站，您可以使用 update-number-of-domain-controllers命令。例如，您可以使用下列命令，將網域控制站的總數設定為 4。請確定您將目錄 ID 取代為 AWS Managed Microsoft AD Directory ID，並將 desired-number 參數取代為您要部署的網域控制站數目。

```
aws ds update-number-of-domain-controllers --directory-id d-1234567890 --
desired-number 4
```

PowerShell

使用 新增或移除其他網域控制站 PowerShell

1. 打開 PowerShell. 若要檢查目前網域控制站的數量，請執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
Get-DSDirectory -DirectoryId d-1234567890 | Select-Object
 DesiredNumberOfDomainControllers
```

2. 若要新增或移除網域控制站，您可以使用 Set-DSDomainControllerCount命令。例如，您可以使用下列命令，將網域控制站的總數設定為 4。請確定您將目錄 ID 取代為 AWS Managed Microsoft AD Directory ID，並將 DesiredNumber 參數取代為您要部署的網域控制站數目。

```
Set-DSDomainControllerCount -DirectoryId d-1234567890 -DesiredNumber 4
```

相關 AWS 安全部落格文章

- 如何透過新增網域控制站來提高 AWS Managed Microsoft AD AWS Directory Service 的備援和效能

升級您的 AWS Managed Microsoft AD

您可以將 Standard Edition AWS Managed Microsoft AD 升級到 Enterprise Edition。以下概述標準版和企業版之間的差異：

- 標準版本：AWS Managed Microsoft AD (標準版) 經過最佳化，適合擁有多達 5,000 名員工的中小型企業做為主要目錄使用。其提供您足夠的儲存容量，可支援最多 30,000* 個目錄物件，例如使用者、群組和電腦。
- 企業版本：AWS Managed Microsoft AD (企業版) 可支援擁有多達 500,000* 個目錄物件的企業組織。

* 上限為約略值。您的目錄可支援更多或更少個目錄物件，這取決於您物件的大小和您應用程式的行為和效能需求。

若要將 Standard Edition AWS Managed Microsoft AD 升級Active Directory到 Enterprise Edition，您需要聯絡 支援。如需詳細資訊，請參閱AWS 支援 《 使用者指南》中的建立支援案例和案例管理。

Note

多區域複寫僅適用於下列區域的 AWS Managed Microsoft AD Enterprise Edition：

- 美國東部 (俄亥俄)
- 美國東部 (維吉尼亞北部)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)
- 亞太區域 (孟買)
- 亞太區域 (大阪)
- 亞太區域 (首爾)
- 亞太區域 (新加坡)
- 亞太區域 (悉尼)
- 亞太區域 （ 泰國 ）
- 亞太區域 (東京)
- 加拿大 (中部)
- 中國 (北京)
- 中國 (寧夏)
- 墨西哥 （ 中部 ）
- 歐洲 (法蘭克福)
- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)
- 歐洲 (巴黎)
- 歐洲 (斯德哥爾摩)
- 南美洲 (聖保羅)
- AWS GovCloud （ 美國西部 ）
- AWS GovCloud （ 美國東部 ）

升級 AWS Managed Microsoft AD 時，需要注意一些限制。這些類別為：

- 升級會產生額外費用。如需詳細資訊，請參閱 AWS Directory Service 定價。
- 您的 Active Directory 升級後，就無法還原至先前的版本。

- 之前的快照無法在升級Active Directory後用來還原 。
- 升級會在與 約定的排程日期和時間進行 支援。升級時間是太平洋標準時間週一至週五上午 9 點至下午 5 點。
- 升級程序需要四到五小時。
- 在升級過程中，您 AWS Managed Microsoft AD 的網域控制站會一次升級一個。這可能會對您的效能產生負面影響，並在維護時段期間造成停機時間。
- 升級程序將變更每個網域控制器執行個體的主機名稱，但其 IP 地址將保持不變。
- 如果您透過 SSL 使用 LDAPS （輕量型目錄存取通訊協定），網域控制站將需要新的憑證。

將備用 UPN 尾碼新增至 AWS Managed Microsoft AD

您可以新增替代使用者主體名稱 Active Directory(UPN) 尾碼至 AWS Managed Microsoft AD 目錄，以簡化 (AD) 登入名稱的管理並改善使用者登入體驗。若要這麼做，您必須使用 Admin 帳戶登入，或者您登入的帳戶須為 AWS 委派的使用者主要名稱尾碼管理員群組的成員。如需此群組的詳細資訊，請參閱使用 AWS Managed Microsoft AD 建立的內容相關文章。

新增替代 UPN 尾碼

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 尋找已加入 AWS Managed Microsoft AD 目錄的 Amazon EC2 執行個體。選取執行個體，然後選取 Connect (連線)。
3. 在 Server Manager (伺服器管理員) 視窗，選擇 Tools (工具)。接著，選擇 Active Directory Domains and Trusts (Active Directory 網域及信任)。
4. 在左側窗格的 Active Directory Domains and Trusts (Active Directory 網域和信任) 按下滑鼠右鍵，然後選擇 Properties (屬性)。
5. 在 UPN Suffixes (UPN 尾碼) 索引標籤，輸入替代 UPN 尾碼 (例如 **`sales.example.com`**)。選擇 Add (新增)，然後選擇 Apply (套用)。
6. 如果您需要新增額外的替代 UPN 尾碼，請重複步驟 5，直到您取得所需的 UPN 尾碼。

重新命名 AWS Managed Microsoft AD 目錄的網站名稱

您可以重新命名 AWS Managed Microsoft AD 目錄的預設網站名稱，使其與您現有的 MicrosoftActive Directory(AD) 網站名稱相符。這可讓 AWS Managed Microsoft AD 更快在內部部署目錄中尋找和驗證現有的 AD 使用者。當使用者登入您已加入 AWS Managed Microsoft AD 目錄的 Amazon EC2 和 Amazon RDS for SQL Server 執行個體等 AWS 資源時，效果會更好。

若要這麼做，您必須使用 Admin 帳戶登入，或者您登入的帳戶須為 AWS 委派的使用者站點與服務管理員群組的成員。如需此群組的詳細資訊，請參閱使用 AWS Managed Microsoft AD 建立的內容相關文章。

如需有關重新命名網站與信任相關的其他優點，請參閱 Microsoft 網站上的 Domain Locator Across a Forest Trust。

重新命名 AWS Managed Microsoft AD 網站名稱

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 尋找已加入 AWS Managed Microsoft AD 目錄的 Amazon EC2 執行個體。選取執行個體，然後選取 Connect (連線)。
3. 在 Server Manager (伺服器管理員) 視窗，選擇 Tools (工具)。接著，選擇 Active Directory Sites and Services (Active Directory 站點與服務)。
4. 在左側窗格中，展開 Sites (站點) 資料夾，在站點名稱上按一下滑鼠右鍵 (預設為 Default-Site-Name)，然後選擇 Rename (重新命名)。
5. 輸入新的站點名稱，然後選擇 Enter (輸入)。

刪除您的 AWS Managed Microsoft AD

刪除 AWS Managed Microsoft AD、Simple AD 或混合目錄時，會刪除所有目錄資料和快照，且無法復原。刪除目錄之後，所有加入目錄的執行個體會保持不變。不過，您無法使用目錄憑證來登入這些執行個體。您需要使用執行個體的本機使用者帳戶來登入這些執行個體。

刪除 AD Connector 時，您的內部部署目錄會保持不變。所有加入目錄的執行個體也會保持不變，並保持在已加入您內部部署目錄的狀態。您仍然可以使用目錄登入資料來登入這些執行個體。

刪除目錄

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。請確定您在部署 Active Directory AWS 區域 的 中。如需詳細資訊，請參閱選擇區域。
2. 確定您要刪除的目錄未啟用 AWS 任何應用程式。啟用 AWS 的應用程式會阻止您刪除 AWS Managed Microsoft AD 或 Simple AD。
   a. 在 Directories (目錄) 頁面中，選擇目錄 ID。
   b. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。在AWS 應用程式和服務區段中，您會看到您的目錄已啟用哪些 AWS 應用程式。

- 停用 AWS Management Console 存取。如需詳細資訊，請參閱停用 AWS Management Console 存取。
- 若要停用 Amazon WorkSpaces，您必須從 WorkSpaces 主控台的目錄中取消登錄該服務。如需詳細資訊，請參閱《Amazon WorkSpaces 管理指南》中的刪除目錄。
- 若要停用 WorkDocs，您必須在 WorkDocs 主控台中刪除 WorkDocs 網站。如需詳細資訊，請參閱《Amazon WorkDocs 管理指南》中的刪除網站一節。
- 若要停用 Amazon WorkMail，您必須在 Amazon WorkMail 主控台中移除 Amazon WorkMail 組織。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的移除組織一節。
- 若要停用 Amazon FSx for Windows File Server，您必須從域中移除 Amazon FSx 檔案系統。如需詳細資訊，請參閱《Amazon FSx for Windows File Server 使用者指南》中的Active Directory在 FSx for Windows File Server 中使用 。 FSx
- 若要停用 Amazon Relational Database Service，您必須從域中移除 Amazon RDS 執行個體。如需詳細資訊，請參閱《Amazon RDS 使用者指南》中的管理域中的資料庫執行個體一節。
- 若要停用 AWS Client VPN 服務，您必須從 Client VPN 端點移除目錄服務。如需詳細資訊，請參閱《 AWS Client VPN 管理員指南》中的使用 Client VPN。
- 若要停用 Amazon Connect，您必須刪除 Amazon Connect 執行個體。如需詳細資訊，請參閱《Amazon Connect 管理指南》中的刪除 Amazon Connect 執行個體。 Amazon Connect
- 若要停用 Amazon QuickSight，您必須取消訂閱 Amazon QuickSight。如需詳細資訊，請參閱《Amazon QuickSight 使用者指南》中的關閉 Amazon QuickSight 您的帳戶。

> **Note**
>
> 如果您正在使用 ， AWS IAM Identity Center 且先前已將其連線至您計劃刪除的 AWS Managed Microsoft AD 目錄，您必須先變更身分來源，才能將其刪除。如需詳細資訊，請參閱《IAM Identity Center 使用者指南》中的變更身分來源一節。

3. 在導覽窗格中，選擇目錄。
4. 只選取要刪除的目錄，然後按一下刪除。刪除目錄需要幾分鐘的時間。刪除目錄之後，該目錄會從您的目錄清單中移除。

保護您的 AWS Managed Microsoft AD

您可以使用密碼政策、多重要素驗證 (MFA) 等功能，以及設定來保護 AWS Managed Microsoft AD。您可以保護目錄的方式包括：

- 了解 中的密碼政策如何Active Directory運作，以便將其套用至 AWS Managed Microsoft AD 使用者。您也可以委派哪些使用者可以管理您的 AWS Managed Microsoft AD 密碼政策。
- 啟用 MFA 以增加您的 AWS Managed Microsoft AD 安全性。
- > 透過 Secure Socket Layer (SSL)/Transport Layer Security (TLS) (LDAPS) 啟用輕量型目錄存取通訊協定，以便透過 LDAP 進行通訊加密並改善安全性。
- 使用聯邦風險與授權管理計劃 (FedRAMP) 和支付卡產業 (PCI) 資料安全標準 (DSS) 等標準來管理 AWS Managed Microsoft AD 合規。
- 修改安全 AWS 群組以滿足您的環境需求，藉此增強 AWS Managed Microsoft AD 網路安全組態 >。
- 編輯您的 AWS Managed Microsoft AD 目錄安全設定，例如 Certificate Base Authentication、Secure Channel Cipher 和 Protocol，以滿足您的需求。
- 設定 AWS Private Certificate Authority Connector for AD，以便您可以發行和管理 AWS Managed Microsoft AD 的憑證 AWS Private CA。

了解 AWS Managed Microsoft AD 密碼政策

AWS Managed Microsoft AD 可讓您為 AWS Managed Microsoft AD 網域中管理的使用者群組定義和指派不同的密碼和帳戶鎖定政策 （ 也稱為精細密碼政策)。當您建立 AWS Managed Microsoft AD 目錄時，會建立預設網域政策並套用至 Active Directory。此政策包括以下設定：

政策	設定
強制密碼歷史記錄	記住 24 組密碼
密碼最長使用期限	42 天 *
密碼最短使用期限	1 天
密碼長度下限	7 個字元
密碼必須符合複雜性需求	已啟用

政策	設定
使用可還原的加密來存放密碼	已停用

> **Note**
>
> * 42 天密碼最長存留期包含管理員密碼。

例如，您可以將較不嚴格的政策設定指派給只能存取低敏感度資訊的員工。對於定期存取機密資訊的資深經理，您可以套用更嚴格的設定。

下列資源提供有關MicrosoftActive Directory精細密碼政策和安全政策的詳細資訊：

- 設定安全政策設定
- 密碼複雜性要求
- 密碼複雜性安全性考量事項

AWS 在 AWS Managed Microsoft AD 中提供一組精細的密碼政策，您可以設定並指派給您的群組。若要設定政策，您可以使用標準Microsoft政策工具，例如 Active Directory Administrative Center。若要開始使用Microsoft政策工具，請參閱 安裝 AWS Managed Microsoft AD 的 Active Directory 管理工具。

如何套用密碼政策

根據密碼是否重設或變更，套用精細密碼政策的方式有所不同。網域使用者可以變更自己的密碼。具有必要許可的Active Directory管理員或使用者可以重設使用者密碼。如需詳細資訊，請參閱下表。

政策	密碼重設	密碼變更
強制密碼歷史記錄	否	是

政策	密碼重設	密碼變更
密碼最長使用期限	是	是
密碼最短使用期限	否	是
密碼長度下限	是	是
密碼必須符合複雜性需求	是	是

這些差異會對安全性產生影響。例如，每當使用者的密碼重設時，強制執行密碼歷史記錄和最低密碼存留期政策不會強制執行。如需詳細資訊，請參閱 Microsoft 文件，了解與強制執行密碼歷史記錄和密碼存留期最低政策相關的安全考量。

支援的政策設定

AWS Managed Microsoft AD 包含五個具有不可編輯優先順序值的精細政策。這些政策具有一些屬性，您可以予以設定來強制執行密碼強度，以及登入失敗時的帳戶鎖定動作。您可以將政策指派給零個或多個 Active Directory 群組。如果最終使用者是多個群組的成員並收到多個密碼政策，Active Directory 會強制執行具有最低優先順序值的政策。

AWS 預先定義的密碼政策

下表列出 AWS Managed Microsoft AD 目錄中包含的五個政策及其指派的優先順序值。如需詳細資訊，請參閱優先順序。

政策名稱	優先順序
CustomerPSO-01	10
CustomerPSO-02	20
CustomerPSO-03	30
CustomerPSO-04	40
CustomerPSO-05	50

密碼政策屬性

您可以編輯密碼政策中的下列屬性，以符合滿足您業務需求的合規標準。

- 政策名稱
- 強制密碼歷史記錄
- 密碼長度下限
- 密碼最短使用期限
- 密碼最長使用期限
- 使用可還原的加密來存放密碼
- 密碼必須符合複雜性需求

您無法修改這些政策的優先順序值。如需這些設定如何影響密碼強制執行的詳細資訊，請參閱 Microsoft TechNet 網站上的 AD DS: Fine-grained password policies 相關內容。如需這些政策的一般資訊，請參閱 Microsoft TechNet 網站上的密碼政策相關內容。

帳戶鎖定政策

您也可以修改密碼政策的下列屬性，以指定 Active Directory 是否應該在登入失敗之後鎖定帳戶及其做法：

- 允許的失敗登入嘗試次數
- 帳戶鎖定期間
- 經過一些時間後重設失敗登入嘗試次數

如需這些政策的一般資訊，請參閱 Microsoft TechNet 網站上的帳戶鎖定政策相關內容。

優先順序

具有較低優先順序值之政策的優先順序較高。您可以將密碼政策指派給 Active Directory 安全群組。雖然您應該對安全群組套用單一政策，但單一使用者可能會收到多個密碼政策。例如，假設 `jsmith` 是 HR 群組的成員，也是 MANAGERS 群組的成員。如果您將 CustomerPSO-05 (優先順序為 50) 指派給 HR 群組，並將 CustomerPSO-04 (優先順序為 40) 指派給 MANAGERS，CustomerPSO-04 的優先順序較高，因此 Active Directory 會將該政策套用至 `jsmith`。

如果您將多個政策指派給一個使用者或群組，Active Directory 會決定產生的政策如下：

1. 套用您直接指派給使用者物件的政策。
2. 如果未直接對使用者物件指派政策，則會套用使用者所收到之所有政策中具有較低優先順序值的政策，做為群組成員資格的結果。

如需其他詳細資訊，請參閱 Microsoft TechNet 網站上的 AD DS: Fine-grained password policies 相關內容。

主題

- 將密碼政策指派給 AWS Managed Microsoft AD 使用者
- 委派誰可以管理您的 AWS Managed Microsoft AD 密碼政策

相關 AWS 安全部落格文章

- 如何使用 AWS Directory Service for AWS Managed Microsoft AD 設定更強大的密碼政策，以協助滿足您的安全標準

將密碼政策指派給 AWS Managed Microsoft AD 使用者

AWS Delegated Fine Grained Password Policy Administrators 安全群組成員的使用者帳戶可以使用下列程序，將政策指派給使用者和安全群組。

將密碼政策指派給您的使用者

1. 從您加入 Managed Microsoft AD 網域的任何受管 EC2 執行個體啟動 Active Directory 管理中心 (ADAC)。 AWS

2. 切換至 Tree View (樹狀檢視)，然後導覽至 System\Password Settings Container (系統\密碼設定容器)。
3. 按兩下您要編輯的微調政策。按一下 Add (新增) 編輯政策屬性，然後將使用者或安全群組新增至政策。如需 AWS Managed Microsoft AD 隨附之預設精細政策的詳細資訊，請參閱 AWS 預先定義的密碼政策。
4. 若要驗證已套用密碼政策，請執行下列 PowerShell 命令：

```
Get-ADUserResultantPasswordPolicy -Identity 'username'
```

> **Note**
>
> 避免使用 `net user` 指令，因為其結果可能不準確。

如果您未在 AWS Managed Microsoft AD 目錄中設定五個密碼政策中的任何一個，Active Directory 會使用預設網域群組政策。如需使用 Password Settings Container (密碼設定容器) 的其他詳細資訊，請參閱這篇 Microsoft 部落格文章。

委派誰可以管理您的 AWS Managed Microsoft AD 密碼政策

您可以將管理密碼政策的許可委派給 Managed Microsoft AD AWS 中建立的特定使用者帳戶，方法是將帳戶新增至AWS 委派的精細分割密碼政策管理員安全群組。當帳戶成為此群組的成員時，即具有編輯及執行之前所列任何密碼政策的許可。

委派可管理密碼政策的人員

1. 從您加入 Managed Microsoft AD 網域的任何受管 EC2 執行個體啟動 Active Directory 管理中心 (ADAC)。 AWS
2. 切換至樹狀檢視，然後導覽至 AWS 委派群組 OU。如需此 OU 的詳細資訊，請參閱「使用 AWS Managed Microsoft AD 建立的內容」。
3. 找到 AWS Delegated Fine Grained Password Policy Administrators 使用者群組。將您網域中的任何使用者或群組新增至此群組。

啟用 AWS Managed Microsoft AD 的多重驗證

您可以為 AWS Managed Microsoft AD 目錄啟用多重要素驗證 (MFA)，以在使用者指定其 AD 登入資料以存取支援的 Amazon Enterprise 應用程式時提高安全性。當您啟用 MFA 時，使用者除了像平常一樣輸入使用者名稱和密碼 (第一重因素)，還必須輸入身分驗證碼 (第二重因素)，該驗證碼由您的虛擬或硬體 MFA 解決方案提供。這兩項因素結合後，可防止使用者在未提供有效使用者登入資料及 MFA 代碼的情況下存取您的 Amazon 企業應用程式，讓您能多一層安全保護。

若要啟用 MFA，您必須擁有本身是一種遠端驗證撥號使用者服務 (RADIUS) 伺服器的 MFA 解決方案，或者擁有已在您的內部部署基礎設施上實作之 RADIUS 伺服器的 MFA 外掛程式。您的 MFA 解決方案必須實作使用者從硬體裝置，或是手機等裝置上執行的軟體所取得的一次性密碼 (OTP)。

RADIUS 是業界標準的用戶端/伺服器通訊協定，可提供身分驗證、授權和會計管理，讓使用者能夠連線至網路服務。 AWS Managed Microsoft AD 包含 RADIUS 用戶端，可連線至您已實作 MFA 解決方案的 RADIUS 伺服器。您的 RADIUS 伺服器驗證使用者名稱和 OTP 代碼。如果您的 RADIUS 伺服器成功驗證使用者，則 AWS 受管 Microsoft AD 會根據 Active Directory 驗證使用者。成功進行 Active Directory 身分驗證後，使用者可以存取 AWS 應用程式。 AWS Managed Microsoft AD RADIUS 用戶端和 RADIUS 伺服器之間的通訊需要您設定 AWS 安全群組，以透過連接埠 1812 啟用通訊。

您可以執行下列程序，為 AWS Managed Microsoft AD 目錄啟用多重驗證。如需有關如何設定您 RADIUS 伺服器以使用 AWS Directory Service 和 MFA 的詳細資訊，請參閱多重要素驗證先決條件。

考量事項

以下是 AWS Managed Microsoft AD 多重要素驗證的一些考量：

- 多重要素驗證不可用於 Simple AD。不過，您可以在 AD Connector 目錄啟用 MFA。如需詳細資訊，請參閱啟用 AD Connector 的多重要素身分驗證。
- MFA 是 AWS Managed Microsoft AD 的區域功能。如果您使用的是多區域複寫，則只能在 AWS Managed Microsoft AD 的主要區域中使用 MFA。
- 如果您想要使用 AWS Managed Microsoft AD 進行外部通訊，建議您為這些通訊設定網路外 AWS 的網路位址轉譯 (NAT) 網際網路閘道或網際網路閘道。
  - 如果您想要支援 AWS Managed Microsoft AD 與託管在 AWS 網路上的 RADIUS 伺服器之間的外部通訊，請聯絡 支援。
- 使用 AWS Managed Microsoft AD 和 AD Connector 搭配 MFA 時， AWS IAM Identity Center AWS Management Console 支援所有 Amazon Enterprise IT 應用程式，包括 WorkSpaces、WorkDocs、Amazon WorkMail、Amazon QuickSight，以及對 和 的存取。多區域不支援這些使用 MFA AWS 的應用程式。

如需詳細資訊，請參閱如何使用 AWS Managed Microsoft AD 和內部部署憑證啟用 AWS 服務的多重要素驗證。

- 如需有關如何設定基本使用者存取 Amazon Enterprise 應用程式、 AWS 單一登入和 AWS Management Console 使用 的資訊 AWS Directory Service，請參閱 從 AWS Managed Microsoft AD 存取 AWS 應用程式和服務和 使用 AWS Managed Microsoft AD 登入資料啟用 AWS Management Console 存取。
- 請參閱以下 AWS 安全部落格文章，了解如何在 AWS Managed Microsoft AD 上啟用 Amazon WorkSpaces 使用者的 MFA、如何使用 AWS Managed Microsoft AD 和內部部署憑證啟用 AWS 服務的多重要素驗證

為 AWS Managed Microsoft AD 啟用多重要素驗證

下列程序說明如何啟用 AWS Managed Microsoft AD 的多重要素驗證。

1. 識別 RADIUS MFA 伺服器和 AWS Managed Microsoft AD 目錄的 IP 地址。
2. 編輯您的 Virtual Private Cloud (VPC) 安全群組，以在 AWS Managed Microsoft AD IP 端點和 RADIUS MFA 伺服器之間透過連接埠 1812 啟用通訊。
3. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
4. 選擇 AWS Managed Microsoft AD 目錄的目錄 ID 連結。
5. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要啟用 MFA 的區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
6. 在 Multi-factor authentication (多重因素認證) 區段中，選擇 Actions (動作)，然後選擇 Enable (啟用)。
7. 在 Enable multi-factor authentication (MFA) (啟用多重因素認證 (MFA)) 頁面上，提供下列值：

   Display label (顯示標籤)

   提供標籤名稱。

   RADIUS server DNS name or IP addresses (RADIUS 伺服器 DNS 名稱或 IP 地址)

   您的 RADIUS 伺服器端點的 IP 地址，或您的 RADIUS 伺服器負載平衡器的 IP 地址。您可以輸入多個 IP 地址，中間以英文逗號分隔 (例如 `192.0.0.0,192.0.0.12`)。

> **Note**
>
> RADIUS MFA 僅適用於驗證對 或 Amazon Enterprise 應用程式和服務的存取 AWS Management Console，例如 WorkSpaces、Amazon QuickSight 或 Amazon Chime。只有在針對 AWS Managed Microsoft AD 設定多區域複寫時，主要區域才支援 Amazon Enterprise 應用程式和服務。它不會將 MFA 提供給在 EC2 執行個體上執行的 Windows 工作負載，或用於登入 EC2 執行個體。 AWS Directory Service 不支援 RADIUS 挑戰/回應身分驗證。
> 使用者在輸入使用者名稱與密碼時，必須有自己的 MFA 碼。或者，您必須使用為使用者執行 MFA out-of-band功能的解決方案，例如推播通知或驗證器一次性密碼 (OTP)。在頻外 MFA 解決方案中，務必為您的解決方案適當地設定 RADIUS 逾時值。使用頻外 MFA 解決方案時，登入頁面會提示使用者輸入 MFA 代碼。在此情況下，使用者必須在密碼欄位和 MFA 欄位中均輸入其密碼。

連接埠

RADIUS 伺服器用於通訊的連接埠。您的內部部署網路必須允許透過預設 RADIUS 伺服器連接埠 (UDP：1812) 從 AWS Directory Service 伺服器傳入流量。

共用秘密代碼

您的 RADIUS 端點建立時所指定的共用秘密代碼。

確認共用秘密代碼

確認您的 RADIUS 端點的共用秘密代碼。

通訊協定

選擇您的 RADIUS 端點建立時所指定的通訊協定。

Server timeout (in seconds) (伺服器逾時 (以秒為單位))

等待 RADIUS 伺服器回應的時間 (以秒為單位)。此值必須介於 1 到 50。

> **Note**
>
> 我們建議將 RADIUS 伺服器逾時設定為 20 秒或更短。如果逾時超過 20 秒，系統將無法重試其他 RADIUS 伺服器，並可能導致逾時失敗。

Max RADIUS request retries (RADIUS 請求重試次數上限)

嘗試與 RADIUS 伺服器進行通訊的次數。此值必須介於 0 到 10。

當 RADIUS Status (RADIUS 狀態) 變更為 Enabled (啟用) 時，即可使用 Multi-Factor Authentication。

8. 選擇 啟用 。

啟用安全 LDAP 或 LDAPS

輕量型目錄存取協定 (LDAP) 是用來從 Active Directory 讀取資料，及將資料寫入 Active Directory 的標準協定。某些應用程式使用 LDAP 新增、移除或搜尋 Active Directory 中的使用者和群組，或是傳輸登入資料來驗證 Active Directory 中的使用者。每個 LDAP 通訊都包括用戶端 (如應用程式) 和伺服器 (例如 Active Directory)。

預設不會加密透過 LDAP 的通訊。如此易讓惡意使用者能夠利用網路監控軟體，來檢視網路上的資料封包。這也是為什麼許多企業安全政策通常會要求組織加密所有 LDAP 通訊。

為了減輕這種資料暴露，受 AWS 管 Microsoft AD 提供了一個選項：您可以透過 Secure Sockets Layer (SSL)/Transport Layer Security (TLS) 啟用 LDAP，也稱為 LDAPS。您可以使用 LDAPS 改善網路上的安全。您也可以加密啟用 LDAP 的應用程式與 AWS Managed Microsoft AD 之間的所有通訊，以符合合規要求。

AWS Managed Microsoft AD 在下列部署案例中提供 LDAPS 支援：

- 伺服器端 LDAPS 會將您的商業或自製可運用 LDAP 的應用程式 (做為 LDAP 用戶端) 與 AWS Managed Microsoft AD (做為 LDAP 伺服器) 之間的 LDAP 通訊加密。如需詳細資訊，請參閱使用 AWS Managed Microsoft AD 啟用伺服器端 LDAPS。
- 用戶端 LDAPS 會加密 WorkSpaces （做為 LDAP 用戶端） 和自我管理 （內部部署） Active Directory （做為 LDAP 伺服器） 等 AWS 應用程式之間的 LDAP 通訊。如需詳細資訊，請參閱使用 AWS Managed Microsoft AD 啟用用戶端 LDAPS。

如需保護 實作的最佳實務的詳細資訊MicrosoftActive DirectoryCertificate Services，請參閱 Microsoft 文件。

主題

- 使用 AWS Managed Microsoft AD 啟用伺服器端 LDAPS
- 使用 AWS Managed Microsoft AD 啟用用戶端 LDAPS

使用 AWS Managed Microsoft AD 啟用伺服器端 LDAPS

伺服器端輕量型目錄存取通訊協定 Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (LDAPS) 支援加密商業或自有 LDAP 感知應用程式與 AWS Managed Microsoft AD 目錄之間的 LDAP 通訊。這有助於使用 Secure Sockets Layer (SSL) 加密通訊協定提升網路上的安全，並符合合規要求。

啟用伺服器端 LDAPS

如需如何設定伺服器端 LDAPS 和憑證授權機構 (CA) 伺服器的詳細指示，請參閱 AWS 安全部落格中的如何為您的 AWS 受管 Microsoft AD 目錄啟用伺服器端 LDAPS。

您必須從用來管理 AWS Managed Microsoft AD 域控制站的 Amazon EC2 執行個體，進行大部分的設定。下列步驟會引導您在 AWS 雲端中為網域啟用 LDAPS。

如果您想要使用自動化來設定 PKI 基礎設施，您可以使用 Microsoft Public Key Infrastructure on AWS QuickStart 指南。具體而言，您可以遵循指南中的指示，載入 Deploy Microsoft PKI into an existing VPC on AWS 的範本。載入範本之後，針對 Active Directory Domain Services Type 選項，請務必選擇 **AWSManaged**。如果您使用快速指南，則可以直接跳至 步驟 3：建立憑證範本。

主題

- 步驟 1：委派可啟用 LDAPS 的人員
- 步驟 2：設定您的憑證授權機構
- 步驟 3：建立憑證範本
- 步驟 4：新增安全群組規則

步驟 1：委派可啟用 LDAPS 的人員

若要啟用伺服器端 LDAPS，您必須是 AWS Managed Microsoft AD 目錄中管理員或 AWS 委派企業憑證授權機構管理員群組的成員。或者，您可以是預設管理使用者 (Admin 帳戶)。如果您想要的話，您可以讓 Admin 帳戶以外的使用者設定 LDAPS。在這種情況下，請將該使用者新增至 AWS Managed Microsoft AD AWS 目錄中的管理員或委派企業憑證授權機構管理員群組。

步驟 2：設定您的憑證授權機構

啟用伺服器端 LDAPS 之前，必須先建立憑證。此憑證必須由加入 AWS Managed Microsoft AD 網域的 Microsoft 企業 CA 伺服器發行。建立後，您必須在該網域中的每個網域控制站上安裝此憑證。此憑證可讓網域控制站上的 LDAP 服務接聽並自動接受來自 LDAP 用戶端的 SSL 連線。

> **Note**
>
> 具有 AWS Managed Microsoft AD 的伺服器端 LDAPS 不支援由獨立 CA 發行的憑證。它也不支援第三方認證機構發行的憑證。

根據您的業務需求，您有以下選擇可設定或連線到網域中的 CA：

- 建立次級 Microsoft Enterprise CA –（建議）使用此選項，您可以在 AWS 雲端中部署次級 Microsoft Enterprise CA 伺服器。伺服器可以使用 Amazon EC2，以便與您現有的根 Microsoft CA 使用。如需如何設定次級 Microsoft 企業 CA 的詳細資訊，請參閱如何為 Managed Microsoft AWS AD Directory 啟用伺服器端 LDAPS 中的步驟 4：將 Microsoft 企業 CA 新增至 Microsoft AD 目錄。AWS
- 建立根 Microsoft 企業 CA – 使用此選項，您可以使用 Amazon EC2 在 AWS 雲端中建立根 Microsoft 企業 CA，並將其加入您的 AWS Managed Microsoft AD 網域。此根 CA 可以對您的網域控制站發出憑證。如需設定新根 CA 的詳細資訊，請參閱AWS如何為 Managed Microsoft AD Directory 啟用伺服器端 LDAPS 中的步驟 3：安裝和設定離線 CA。

如需如何將您的 EC2 執行個體加入網域的詳細資訊，請參閱「將 Amazon EC2 執行個體加入 AWS Managed Microsoft AD 的方法」。

步驟 3：建立憑證範本

設定企業 CA 之後，您可以設定 Kerberos 身分驗證憑證範本。

建立憑證範本

1. 啟動 Microsoft Windows Server Manager。選取工具 > 憑證授權機構。
2. 在憑證授權機構視窗中，展開左窗格中的憑證授權機構樹狀目錄。在憑證範本上按一下滑鼠右鍵，然後選擇管理。
3. 在憑證範本主控台視窗中，在 Kerberos 身分驗證上按一下滑鼠右鍵，然後選擇複製範本。
4. 新模板的屬性視窗將彈出。

5. 在新範本的屬性視窗中，前往相容性索引標籤，然後執行下列動作：

   a. 將憑證授權機構變更為符合 CA 的作業系統。

   b. 如果彈出產生的變更視窗，請選取確定。

   c. 將認證收件人變更為 Windows 10 / Windows Server 2016。

   > **Note**
   >
   > AWS Managed Microsoft AD 採用 Windows Server 2019 技術。

   d. 如果彈出產生的變更視窗，請選取確定。

6. 按一下一般索引標籤，然後將範本顯示名稱變更為 LDAPOverSSL 或您想要的任何其他名稱。
7. 按一下安全性索引標籤，然後在群組或使用者名稱區段中選擇域控制站。在域控制站權限區段中，確認已核取讀取、登錄和自動註冊的允許核取方塊。
8. 選擇確定以建立 LDAPOverSSL (或您在上面指定的名稱) 憑證範本。關閉憑證範本主控台視窗。
9. 在憑證授權機構視窗中，在憑證範本上按一下滑鼠右鍵，然後選擇新增 > 要發出的憑證範本。
10. 在啟用憑證範本視窗中，選擇 LDAPOverSSL (或您在上面指定的名稱)，然後選擇確定。

步驟 4：新增安全群組規則

在最後一個步驟中，您必須開啟 Amazon EC2 主控台並新增安全群組規則。這些規則允許您的網域控制站連線到企業 CA，以請求憑證。若要執行此作業，您可以新增輸入規則，讓企業 CA 可以接受來自網域控制站的連入流量。然後，您可以新增輸出規則，允許從網域控制站到企業 CA 的流量。

設定這兩項規則之後，您的網域控制站就會自動向企業 CA 請求憑證，並為您的目錄啟用 LDAPS。您網域控制站上的 LDAP 服務現在可以接受 LDAPS 連線。

設定安全群組規則

1. 導覽至位於 https://console.aws.amazon.com/ec2 的 Amazon EC2 主控台，然後使用管理員憑證進行登入。
2. 在左窗格的 Network & Security (網路與安全) 下，選擇 Security Groups (安全群組)。
3. 在主窗格中，選擇 CA AWS 的安全群組。
4. 選擇 Inbound (入站) 標籤，然後選擇 Edit (編輯)。
5. 在 Edit inbound rules (編輯輸入規則) 對話方塊中，執行下列動作：

   - 選擇 Add Rule (新增規則)。

- 在 Type (類型) 選擇 All traffic (所有流量)，並在 Source (來源) 選擇 Custom (自訂)。
- 在來源旁的方塊中輸入目錄 AWS 的安全群組 （ 例如 sg-123456789)。
- 選擇儲存。

6. 現在選擇 AWS Managed Microsoft AD 目錄 AWS 的安全群組。選擇 Outbound (輸出) 標籤，然後選擇 Edit (編輯)。
7. 在 Edit outbound rules (編輯輸出規則) 對話方塊中，執行下列動作：

- 選擇 Add Rule (新增規則)。
- 在 Type (類型) 選擇 All traffic (所有流量)，並在 Destination (目標) 選擇 Custom (自訂)。
- 在目的地旁的方塊中輸入 CA AWS 的安全群組。
- 選擇儲存。

您可以使用 LDP 工具測試與 AWS Managed Microsoft AD 目錄的 LDAPS 連線。LDP 工具隨附於 Active Directory 管理工具。如需詳細資訊，請參閱安裝 AWS Managed Microsoft AD 的 Active Directory 管理工具。

> **Note**
>
> 測試 LDAPS 連線之前，您最多必須等候 30 分鐘，直到次級 CA 對您的域控制站發出憑證。

如需伺服器端 LDAPS 的其他詳細資訊，並查看如何設定的範例使用案例，請參閱 AWS 安全部落格中的如何為 AWS Managed Microsoft AD Directory 啟用伺服器端 LDAPS。

使用 AWS Managed Microsoft AD 啟用用戶端 LDAPS

AWS Managed Microsoft AD 中的用戶端輕量型目錄存取協定 Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (LDAPS) 支援會加密自我管理 （ 內部部署 ） Microsoft Active Directory (AD) 和 AWS 應用程式之間的通訊。這類應用程式的範例包括 WorkSpaces AWS IAM Identity Center、QuickSight 和 Amazon Chime。此加密可協助您更完善地保護組織的身分資料，並滿足您的安全需求。

先決條件

啟用用戶端 LDAPS 前，您必須符合以下要求。

主題

- 在 AWS Managed Microsoft AD 與自我管理之間建立信任關係 Microsoft Active Directory
- 在 Active Directory 中部署伺服器憑證
- 憑證授權單位憑證需求
- 網路要求

在 AWS Managed Microsoft AD 與自我管理之間建立信任關係 Microsoft Active Directory

首先，您需要在 AWS Managed Microsoft AD 與自我管理之間建立信任關係MicrosoftActive Directory，以啟用用戶端 LDAPS。如需詳細資訊，請參閱the section called “建立信任關係”。

在 Active Directory 中部署伺服器憑證

若要啟用用戶端 LDAPS，您需要為 Active Directory 中的每個網域控制站取得並安裝伺服器憑證。LDAP 服務將使用這些憑證接聽並自動接受來自 LDAP 用戶端的 SSL 連線。您可以使用內部 Active Directory Certificate Services (ADCS) 部署發行或從商業發行者購買的 SSL 憑證。如需 Active Directory 伺服器憑證要求的詳細資訊，請參閱 Microsoft 網站上透過 SSL 的 LDAP (LDAPS) 憑證。

憑證授權單位憑證需求

用戶端 LDAPS 操作須使用憑證授權機構 (CA) 的憑證 (代表您伺服器憑證的發行者)。憑證授權機構憑證會以 Active Directory 網域控制站出示的伺服器憑證進行比對，以加密 LDAP 通訊。請注意下列 CA 憑證要求：

- 需要企業認證授權機構 (CA) 才能啟用用戶端 LDAPS。您可以使用 Active Directory Certificate Service、第三方商業憑證授權機構或 AWS Certificate Manager。如需Microsoft企業憑證授權單位的詳細資訊，請參閱 Microsoft 文件。
- 若要登錄憑證，憑證的過期日期必須在 90 天以上。
- 憑證必須是隱私權增強式郵件 (PEM) 格式。如果從 Active Directory 內部匯出 CA 憑證，選擇 base64 編碼的 X.509 (.CER) 做為匯出檔案格式。
- 每個 AWS Managed Microsoft AD 目錄最多可儲存五 (5) 個 CA 憑證。
- 不支援使用 RSASSA-PSS 簽章演算法的憑證。
- 鏈結至每個信任網域中每個伺服器憑證的 CA 憑證皆須登錄。

網路要求

AWS 應用程式 LDAP 流量只會在 TCP 連接埠 636 上執行，而不會回復至 LDAP 連接埠 389。不過，支援複寫、信任等等的 Windows LDAP 通訊將繼續使用具備 Windows 原生安全性的 LDAP 連接埠

389。設定 AWS 安全群組和網路防火牆，以允許 AWS Managed Microsoft AD （傳出） 和自我管理 Active Directory （傳入） 中連接埠 636 上的 TCP 通訊。讓 LDAP 連接埠 389 在 AWS Managed Microsoft AD 與自我管理 Active Directory 之間維持開啟狀態。

啟用用戶端 LDAPS

若要啟用用戶端 LDAPS，您只需將憑證授權機構 (CA) 憑證匯入 AWS Managed Microsoft AD ，然後在目錄上啟用 LDAPS。啟用後， AWS 應用程式與您的自我管理 Active Directory 之間的所有 LDAP 通訊將透過安全通訊端層 (SSL) 通道加密進行傳輸。

您可以使用兩種不同的方法，為您的目錄啟用用戶端 LDAPS。您可以使用 AWS Management Console 方法或 AWS CLI 方法。

> **Note**
>
> 用戶端 LDAPS 是 AWS Managed Microsoft AD 的區域功能。如果您使用的是多區域複寫，則必須在每個區域中分別套用下列程序。如需詳細資訊，請參閱全域與區域功能。

主題

- 步驟 1：在 中註冊憑證 AWS Directory Service
- 步驟 2：檢查登錄狀態
- 步驟 3：啟用用戶端 LDAPS
- 步驟 4：查看 LDAPS 狀態

步驟 1：在 中註冊憑證 AWS Directory Service

使用下列其中一種方法來註冊憑證 AWS Directory Service。

方法 1：在 AWS Directory Service (AWS Management Console) 中註冊您的憑證

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 選擇您目錄的目錄 ID 連結。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要登錄憑證的區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。

4. 在 Client-side LDAPS (用戶端 LDAPS) 畫面中，選取 Actions (動作) 功能表，然後選取 Register certificate (登錄憑證)。
5. 在 Register a CA certificate (登錄憑證授權機構憑證) 對話方塊中，選取 Browse (瀏覽)，然後選取憑證並選擇 Open (開啟)。
6. 選擇 Register certificate (登錄憑證)。

方法 2：在 AWS Directory Service (AWS CLI) 中註冊您的憑證

- 執行下列命令。對於憑證資料，請指向您 CA 憑證檔案的位置。憑證 ID 會在回應中提供。

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

步驟 2：檢查登錄狀態

若要查看憑證登錄狀態或登錄的憑證清單，請使用以下任一方法。

方法 1：檢查 AWS Directory Service (AWS Management Console) 中的憑證註冊狀態

1. 前往目錄詳細資訊頁面上的用戶端 LDAPS 區段。
2. 檢閱 Registration status (登錄狀態) 欄下方顯示的目前憑證登錄狀態。當登錄狀態值變更為 Registered (已登錄)，表示您的憑證已成功登錄。

方法 2：檢查 AWS Directory Service (AWS CLI) 中的憑證註冊狀態

- 執行下列命令。如果狀態值傳回 `Registered`，表示您的憑證已成功登錄。

```
aws ds list-certificates --directory-id your_directory_id
```

步驟 3：啟用用戶端 LDAPS

使用下列其中一種方法在 中啟用用戶端 LDAPS AWS Directory Service。

> **Note**
>
> 您必須先成功登錄至少一個憑證，才能啟用用戶端 LDAPS。

方法 1：在 AWS Directory Service (AWS Management Console) 中啟用用戶端 LDAPS

1. 前往目錄詳細資訊頁面上的用戶端 LDAPS 區段。
2. 選擇 啟用 。如果無法使用此選項，請確認已成功登錄有效憑證，然後再試一次。
3. 在 Enable client-side LDAPS (啟用用戶端 LDAPS) 對話方塊中，選擇 Enable (啟用)。

方法 2：在 AWS Directory Service (AWS CLI) 中啟用用戶端 LDAPS

- 執行下列命令。

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

步驟 4：查看 LDAPS 狀態

使用下列其中一種方法來檢查 中的 LDAPS 狀態 AWS Directory Service。

方法 1：在 AWS Directory Service (AWS Management Console) 中檢查 LDAPS 狀態

1. 前往目錄詳細資訊頁面上的用戶端 LDAPS 區段。
2. 如果狀態值顯示為 Enabled (已啟用)，表示 LDAPS 已成功設定。

方法 2：在 AWS Directory Service (AWS CLI) 中檢查 LDAPS 狀態

- 執行下列命令。如果狀態值傳回 `Enabled`，表示 LDAPS 已成功設定。

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

管理用戶端 LDAPS

使用這些命令來管理您的 LDAPS 組態。

您可以使用兩種不同的方法來管理用戶端 LDAPS 設定。您可以使用 AWS Management Console 方法或 AWS CLI 方法。

檢視憑證詳細資訊

使用下列其中一種方法來查看憑證設為過期的時間。

方法 1：在 AWS Directory Service (AWS Management Console) 中檢視憑證詳細資訊

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 選擇您目錄的目錄 ID 連結。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要檢視憑證的區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
4. 在 Client-side LDAPS (用戶端 LDAPS) 區段中，在 CA certificates (憑證授權機構憑證) 下方，將顯示憑證相關資訊。

方法 2：在 AWS Directory Service (AWS CLI) 中檢視憑證詳細資訊

- 執行下列命令。對於憑證 ID，使用 `register-certificate` 或 `list-certificates` 傳回的識別符。

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

取消登錄憑證

使用下列其中一種方法來取消登錄憑證。

> **Note**
>
> 如果只登錄一個憑證，必須先停用 LDAPS，才能取消登錄憑證。

方法 1：在 AWS Directory Service (AWS Management Console) 中取消註冊憑證

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 選擇您目錄的目錄 ID 連結。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要取消登錄憑證的區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。

- 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。

4. 在 Client-side LDAPS (用戶端 LDAPS) 區段中，選擇 Actions (動作)，然後選擇 Deregister certificate (取消登錄憑證)。
5. 在 Deregister a CA certificate (取消登錄憑證授權機構憑證) 對話方塊中，選擇 Deregister (取消登錄)。

方法 2：在 AWS Directory Service (AWS CLI) 中取消註冊憑證

- 執行下列命令。對於憑證 ID，使用 `register-certificate` 或 `list-certificates` 傳回的識別符。

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

停用用戶端 LDAPS

使用以下其中一個方法來停用用戶端 LDAPS。

方法 1：在 AWS Directory Service (AWS Management Console) 中停用用戶端 LDAPS

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 選擇您目錄的目錄 ID 連結。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要停用用戶端 LDAPS 的區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
4. 在 Client-side LDAPS (用戶端 LDAPS) 區段中，選擇 Disable (停用)。
5. 在 Disable client-side LDAPS (停用用戶端 LDAPS) 對話方塊中，選擇 Disable (停用)。

方法 2：在 AWS Directory Service (AWS CLI) 中停用用戶端 LDAPS

- 執行下列命令。

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

憑證註冊問題

使用 CA 憑證註冊 AWS Managed Microsoft AD 網域控制站的程序最多可能需要 30 分鐘。如果您遇到憑證註冊問題，並想要重新啟動 AWS Managed Microsoft AD 網域控制站，您可以聯絡 支援。若要建立支援案例，請參閱建立支援案例和案例管理。

管理 AWS Managed Microsoft AD 的合規

您可以使用 AWS Managed Microsoft AD 在 AWS 雲端中支援 Active Directory 感知應用程式，這些應用程式受下列合規要求約束。不過，如果您使用 Simple AD，您的應用程式將不會符合合規需求。

支援的合規標準

AWS Managed Microsoft AD 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 Managed Microsoft AD 符合聯邦風險與授權管理計劃 (FedRAMP) 安全要求，並已在 FedRAMP 中高基準收到 FedRAMP 聯合授權委員會 (JAB) 臨時操作授權機構 (P-ATO)。如需 FedRAMP 合規的詳細資訊，請參閱 FedRAMP 合規。
	AWS Managed Microsoft AD 在服務提供者層級 1 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，可以使用 AWS Managed Microsoft AD 管理自己的 PCI DSS 合規認證。 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。重要的是，您必須在 AWS Managed Microsoft AD 中設定精細的密碼政策，以符合 PCI DSS 3.2 版標準。如需必須強制執行哪些政策的詳細資訊，請參閱以下標題為啟用 AWS 受管 Microsoft AD 目錄的 PCI 合規一節。
	AWS 已擴展其健康保險可攜性和責任法案 (HIPAA) 合規計劃，以將 AWS Managed Microsoft AD 納入為符合 HIPAA 資格的服務。如果您與 簽署了商業夥伴協議 (BAA) AWS，

	您可以使用 AWS Managed Microsoft AD 協助建置符合 HIPAA 規定的應用程式。 AWS 為有興趣進一步了解如何利用處理 AWS 和儲存健康資訊的客戶提供以 HIPAA 為中心的白皮書。如需詳細資訊，請參閱 HIPAA 合規。

共同的責任

涵蓋 FedRAMP、HIPAA 及 PCI 合規的安全性是全體共同責任。請務必了解 AWS Managed Microsoft AD 合規狀態不會自動套用到您在 AWS 雲端中執行的應用程式。您需要確保使用 AWS 服務符合 標準。

如需 AWS Managed Microsoft AD 支援的所有各種 AWS 合規計劃的完整清單，請參閱AWS 合規計劃範圍內的服務。

為您的 AWS Managed Microsoft AD 目錄啟用 PCI 合規

若要啟用 AWS Managed Microsoft AD 目錄的 PCI 合規，您必須設定精細的密碼政策，如 提供的 PCI DSS 合規證明 (AOC) 和責任摘要文件中所指定 AWS Artifact。

如需使用微調密碼政策的詳細資訊，請參閱「了解 AWS Managed Microsoft AD 密碼政策」。

增強 AWS Managed Microsoft AD 網路安全組態

針對 AWS Managed Microsoft AD 目錄佈建 AWS 的安全群組已設定最低傳入網路連接埠，以支援 AWS Managed Microsoft AD 目錄的所有已知使用案例。如需佈建 AWS 安全群組的詳細資訊，請參閱使用 AWS Managed Microsoft AD 建立的內容。

若要進一步增強 AWS Managed Microsoft AD 目錄的網路安全，您可以根據下列常見案例修改 AWS 安全群組。

客戶網域控制站 CIDR - 此 CIDR 區塊是您網域內部部署網域控制站所在的位置。

客戶用戶端 CIDR - 此 CIDR 區塊是電腦或使用者等用戶端向 AWS Managed Microsoft AD 進行身分驗證的地方。您的 AWS Managed Microsoft AD 網域控制站也位於此 CIDR 區塊中。

案例

- AWS 應用程式僅支援
- AWS 僅支援信任的應用程式

- AWS 應用程式和原生 Active Directory 工作負載支援
- AWS 應用程式和原生 Active Directory 工作負載支援與信任支援

AWS 應用程式僅支援

所有使用者帳戶只會在您的 AWS Managed Microsoft AD 中佈建，以便與支援 AWS 的應用程式搭配使用，如下所示：

- Amazon Chime
- Amazon Connect
- QuickSight
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS Management Console

您可以使用下列 AWS 安全群組組態來封鎖 Managed Microsoft AD AWS 網域控制站的所有非必要流量。

> **Note**
>
> - 下列項目與此 AWS 安全群組組態不相容：
>   - Amazon EC2 執行個體
>   - Amazon FSx
>   - Amazon RDS for MySQL
>   - Amazon RDS for Oracle
>   - Amazon RDS for PostgreSQL
>   - Amazon RDS for SQL Server
>   - WorkSpaces
>   - Active Directory 信任
>   - 加入網域的用戶端或伺服器

傳入規則

無。

傳出規則

無。

AWS 僅支援信任的應用程式

所有使用者帳戶都會佈建在您的 AWS Managed Microsoft AD 或受信任的 Active Directory 中，以便與支援 AWS 的應用程式搭配使用，如下所示：

- Amazon Chime
- Amazon Connect
- QuickSight
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Client VPN
- AWS Management Console

您可以修改佈建 AWS 的安全群組組態，以封鎖對 AWS Managed Microsoft AD 網域控制站的所有非必要流量。

> **Note**
>
> - 下列項目與此 AWS 安全群組組態不相容：
> - Amazon EC2 執行個體
> - Amazon FSx
> - Amazon RDS for MySQL
> - Amazon RDS for Oracle
> - Amazon RDS for PostgreSQL
> - Amazon RDS for SQL Server
> - WorkSpaces

  - Active Directory 信任
  - 加入網域的用戶端或伺服器
- 此組態需要您確保「客戶網域控制站 CIDR」網路是安全的。
- TCP 445 僅用於建立信任，並且可以在建立信任之後移除。
- 只有在使用透過 SSL 的 LDAP 時，才需要 TCP 636。

傳入規則

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
TCP 和 UDP	53	客戶網域控制站 CIDR	DNS	使用者和電腦身分驗證、名稱解析、信任
TCP 和 UDP	88	客戶網域控制站 CIDR	Kerberos	使用者和電腦身分驗證、森林層級信任
TCP 和 UDP	389	客戶網域控制站 CIDR	LDAP	目錄、複寫、使用者和電腦身分驗證群組政策、信任
TCP 和 UDP	464	客戶網域控制站 CIDR	Kerberos 更改/設定密碼	複寫、使用者和電腦身分驗證、信任
TCP	445	客戶網域控制站 CIDR	SMB/CIFS	複寫、使用者和電腦身分驗證群組政策、信任
TCP	135	客戶網域控制站 CIDR	複寫	RPC、EPM
TCP	636	客戶網域控制站 CIDR	LDAP SSL	目錄、複寫、使用者和電腦身分

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
				驗證群組政策、信任
TCP	49152 - 65535	客戶網域控制站 CIDR	RPC	複寫、使用者和電腦身分驗證、群組政策、信任
TCP	3268-3269	客戶網域控制站 CIDR	LDAP GC 和 LDAP GC SSL	目錄、複寫、使用者和電腦身分驗證群組政策、信任
UDP	123	客戶網域控制站 CIDR	Windows 時間	Windows 時間、信任

傳出規則

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
全部	全部	客戶網域控制站 CIDR	所有流量	

AWS 應用程式和原生 Active Directory 工作負載支援

使用者帳戶只會在您的 AWS Managed Microsoft AD 中佈建，以搭配支援 AWS 的應用程式使用，如下所示：

- Amazon Chime
- Amazon Connect
- Amazon EC2 執行個體
- Amazon FSx
- QuickSight

- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

您可以修改佈建 AWS 的安全群組組態，以封鎖對 AWS Managed Microsoft AD 網域控制站的所有非必要流量。

> **Note**
>
> - Active Directory 無法在 AWS Managed Microsoft AD 目錄與客戶網域控制站 CIDR 之間建立和維護信任。
> - 它要求您確保「客戶用戶端 CIDR」網路是安全的。
> - 只有在使用透過 SSL 的 LDAP 時，才需要 TCP 636。
> - 如果您想要搭配此組態使用企業 CA，則需要建立傳出規則 "TCP， 443， CA CIDR"。

傳入規則

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
TCP 和 UDP	53	客戶用戶端 CIDR	DNS	使用者和電腦身分驗證、名稱解析、信任

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
TCP 和 UDP	88	客戶用戶端 CIDR	Kerberos	使用者和電腦身分驗證、森林層級信任
TCP 和 UDP	389	客戶用戶端 CIDR	LDAP	目錄、複寫、使用者和電腦身分驗證群組政策、信任
TCP 和 UDP	445	客戶用戶端 CIDR	SMB/CIFS	複寫、使用者和電腦身分驗證群組政策、信任
TCP 和 UDP	464	客戶用戶端 CIDR	Kerberos 更改/設定密碼	複寫、使用者和電腦身分驗證、信任
TCP	135	客戶用戶端 CIDR	複寫	RPC、EPM
TCP	636	客戶用戶端 CIDR	LDAP SSL	目錄、複寫、使用者和電腦身分驗證群組政策、信任
TCP	49152 - 65535	客戶用戶端 CIDR	RPC	複寫、使用者和電腦身分驗證、群組政策、信任
TCP	3268-3269	客戶用戶端 CIDR	LDAP GC 和 LDAP GC SSL	目錄、複寫、使用者和電腦身分驗證群組政策、信任
TCP	9389	客戶用戶端 CIDR	SOAP	AD DS 網路服務

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
UDP	123	客戶用戶端 CIDR	Windows 時間	Windows 時間、信任
UDP	138	客戶用戶端 CIDR	DFSN 和 NetLogon	DFS、群組政策

傳出規則

無。

AWS 應用程式和原生 Active Directory 工作負載支援與信任支援

所有使用者帳戶都會佈建在您的 AWS Managed Microsoft AD 或受信任的 Active Directory 中，以便與支援 AWS 的應用程式搭配使用，如下所示：

- Amazon Chime
- Amazon Connect
- Amazon EC2 執行個體
- Amazon FSx
- QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

您可以修改佈建 AWS 的安全群組組態，以封鎖對 AWS Managed Microsoft AD 網域控制站的所有非必要流量。

> **Note**
>
> - 它要求您確保「客戶網域控制站 CIDR」和「客戶用戶端 CIDR」網路是安全的。
> - 具有「客戶網域控制站 CIDR」的 TCP 445 僅用於建立信任，並且可以在建立信任之後移除。
> - 具有「客戶用戶端 CIDR」的 TCP 445 應保持開啟狀態，因為群組政策處理需要它。
> - 只有在使用透過 SSL 的 LDAP 時，才需要 TCP 636。
> - 如果您想要搭配此組態使用企業 CA，則需要建立傳出規則 "TCP， 443， CA CIDR"。

傳入規則

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
TCP 和 UDP	53	客戶網域控制站 CIDR	DNS	使用者和電腦身分驗證、名稱解析、信任
TCP 和 UDP	88	客戶網域控制站 CIDR	Kerberos	使用者和電腦身分驗證、森林層級信任
TCP 和 UDP	389	客戶網域控制站 CIDR	LDAP	目錄、複寫、使用者和電腦身分驗證群組政策、信任
TCP 和 UDP	464	客戶網域控制站 CIDR	Kerberos 更改/設定密碼	複寫、使用者和電腦身分驗證、信任

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
TCP	445	客戶網域控制站 CIDR	SMB/CIFS	複寫、使用者和電腦身分驗證群組政策、信任
TCP	135	客戶網域控制站 CIDR	複寫	RPC、EPM
TCP	636	客戶網域控制站 CIDR	LDAP SSL	目錄、複寫、使用者和電腦身分驗證群組政策、信任
TCP	49152 - 65535	客戶網域控制站 CIDR	RPC	複寫、使用者和電腦身分驗證、群組政策、信任
TCP	3268-3269	客戶網域控制站 CIDR	LDAP GC 和 LDAP GC SSL	目錄、複寫、使用者和電腦身分驗證群組政策、信任
UDP	123	客戶網域控制站 CIDR	Windows 時間	Windows 時間、信任
TCP 和 UDP	53	客戶網域控制站 CIDR	DNS	使用者和電腦身分驗證、名稱解析、信任
TCP 和 UDP	88	客戶網域控制站 CIDR	Kerberos	使用者和電腦身分驗證、森林層級信任
TCP 和 UDP	389	客戶網域控制站 CIDR	LDAP	目錄、複寫、使用者和電腦身分驗證群組政策、信任

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
TCP 和 UDP	445	客戶網域控制站 CIDR	SMB/CIFS	複寫、使用者和電腦身分驗證群組政策、信任
TCP 和 UDP	464	客戶網域控制站 CIDR	Kerberos 更改/設定密碼	複寫、使用者和電腦身分驗證、信任
TCP	135	客戶網域控制站 CIDR	複寫	RPC、EPM
TCP	636	客戶網域控制站 CIDR	LDAP SSL	目錄、複寫、使用者和電腦身分驗證群組政策、信任
TCP	49152 - 65535	客戶網域控制站 CIDR	RPC	複寫、使用者和電腦身分驗證、群組政策、信任
TCP	3268-3269	客戶網域控制站 CIDR	LDAP GC 和 LDAP GC SSL	目錄、複寫、使用者和電腦身分驗證群組政策、信任
TCP	9389	客戶網域控制站 CIDR	SOAP	AD DS 網路服務
UDP	123	客戶網域控制站 CIDR	Windows 時間	Windows 時間、信任
UDP	138	客戶網域控制站 CIDR	DFSN 和 NetLogon	DFS、群組政策

傳出規則

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
全部	全部	客戶網域控制站 CIDR	所有流量	

編輯 AWS Managed Microsoft AD 目錄安全設定

您可以為 AWS Managed Microsoft AD 設定精細目錄設定，以符合您的合規和安全性需求，而不會增加操作工作負載。在目錄設定中，您可以更新目錄中使用的協定和加密方式的安全通道組態。例如，您可以靈活地停用個別舊版密碼，例如 RC4 或 DES，以及 SSL 2.0/3.0 和 TLS 1.0/1.1 等通訊協定。AWS 受管 Microsoft AD 接著會將組態部署到目錄中的所有網域控制站，管理網域控制站重新啟動，並在橫向擴展或部署其他 時維護此組態 AWS 區域。如需所有可用設定的詳細資訊，請參閱 目錄安全設定清單。

編輯目錄安全設定

您可以設定和編輯任何目錄的設定。

編輯目錄設定

1. 登入 AWS 管理主控台，並在 開啟 AWS Directory Service 主控台https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在聯網和安全下，找到目錄設定，然後選擇編輯設定。
4. 在編輯設定中，變更要編輯的設定的值。當您編輯設定時，其狀態將從預設變更為準備更新。如果您之前編輯過設定，其狀態將從已更新變更為準備更新。接著選擇檢閱。
5. 在檢閱和更新設定中，請檢查目錄設定並確認新的值均正確無誤。如果您想對設定進行任何其他變更，請選擇編輯設定。當您對變更感到滿意並準備好實作新值時，請選擇更新設定。然後，您會回到目錄 ID 頁面。

> **Note**
>
> 在目錄設定下，您可以檢視更新設定的狀態。實作設定時，狀態顯示正在更新。當某項設定的狀態顯示為正在更新時，您無法編輯其他設定。如果設定編輯成功並更新，其狀態將顯示已更新。如果設定無法按照編輯成功更新，其狀態將顯示失敗。

目錄安全設定失敗

如果設定更新期間發生錯誤，狀態將顯示為失敗。在失敗狀態下，設定不會更新為新值，仍保留原始值。您可以重試更新這些設定，或將它們還原為先前的值。

解決更新設定失敗的問題

- 在目錄設定下，選擇解決失敗的設定。然後執行下列其中一項：
  - 若要將設定還原為失敗狀態之前的原始值，請選擇還原失敗的設定。然後，在彈出的視窗中選擇還原。
  - 若要重試更新目錄設定，請選擇重試失敗的設定。如果您想在重試失敗的更新之前，對目錄設定進行其他變更，請選擇繼續編輯。在檢閱和重試失敗的更新上，選擇更新設定。

目錄安全設定清單

以下清單顯示所有可用目錄安全設定的類型、設定名稱、API 名稱、可能的值和設定描述。

如果停用所有其他安全設定，則 TLS 1.2 和 AES 256/256 是預設目錄安全設定。它們不能被停用。

Type	設定名稱	API 名稱	可能的值	設定說明
憑證型身分驗證	憑證回溯認證	CERTIFICATE_BACKDATING_COMPENSATION	年：0 至 50 月：0 至 11 天：0 至 30 時：0 至 23 分：0 至 59 秒：0 到 59	指定一個值來指示憑證可以早於 Active Directory 中的使用者存取時間並且仍可用於 Active Directory 中的身分驗證的時間長度。預設值為 10 分鐘。您可以將此值設定為 1 秒到 50 年。

Type	設定名稱	API 名稱	可能的值	設定說明
				若要進行此設定，您必須為強式憑證繫結強制執行選取相容性類型。 如需詳細資訊，請參閱 Microsoft 支援文件中的 KB5014754 – Windows 域控制站上的憑證式驗證變更一文。

Type	設定名稱	API 名稱	可能的值	設定說明
	憑證強式強制執行	CERTIFICATE_STRONG_ENFORCEMENT	相容性、完整強制執行	指定下列任一強制執行類型： • 相容性：如果憑證無法強烈映射至使用者，則允許身分驗證。如果憑證早於 Active Directory 中的使用者帳戶，則還必須設定憑證回溯認證，否則身分驗證會失敗。 • Full Enforcement（預設）：如果憑證無法強烈對應至使用者，則不允許身分驗證。如果您選擇此強制執行類型，則無法設定憑證回溯認證。

Type	設定名稱	API 名稱	可能的值	設定說明
				如需詳細資訊，請參閱 Microsoft 支援文件中的 KB5014754 – Windows 域控制站上的憑證式驗證變更一文。
安全通道：加密方式	AES 128/128	AES_128_128	啟用、停用	啟用或停用目錄中域控制站之間用於安全通道通訊的 AES 128/128 加密方式。
	DES 56/56	DES_56_56	啟用、停用	啟用或停用目錄中域控制站之間用於安全通道通訊的 DES 56/56 加密方式。
	RC2 40/128	RC2_40_128	啟用、停用	啟用或停用目錄中域控制站之間用於安全通道通訊的 RC2 40/128 加密方式。

Type	設定名稱	API 名稱	可能的值	設定說明
	RC2 56/128	RC2_56_128	啟用、停用	啟用或停用目錄中域控制站之間用於安全通道通訊的 RC2 56/128 加密方式。
	RC2 128/128	RC2_128_128	啟用、停用	啟用或停用目錄中域控制站之間用於安全通道通訊的 RC2 128/128 加密方式。
	RC4 40/128	RC4_40_128	啟用、停用	啟用或停用目錄中域控制站之間用於安全通道通訊的 RC4 40/128 加密方式。
	RC4 56/128	RC4_56_128	啟用、停用	啟用或停用目錄中域控制站之間用於安全通道通訊的 RC4 56/128 加密方式。
	RC4 64/128	RC4_64_128	啟用、停用	啟用或停用目錄中域控制站之間用於安全通道通訊的 RC4 64/128 加密方式。

Type	設定名稱	API 名稱	可能的值	設定說明
安全通道：協定	RC4 128/128	RC4_128_128	啟用、停用	啟用或停用目錄中域控制站之間用於安全通道通訊的 RC4 128/128 加密方式。
	三重 DES 168/168	3DES_168_168	啟用、停用	啟用或停用三重 DES 168/168 加密方式，以確保目錄中域控制站之間的安全通道通訊。
	PCT 1.0	PCT_1_0	啟用、停用	啟用或停用目錄中域控制站用於安全通道通訊 (伺服器和用戶端) 的 PCT 1.0 協定。
	SSL 2.0	SSL_2_0	啟用、停用	啟用或停用目錄中域控制站用於安全通道通訊 (伺服器和用戶端) 的 SSL 2.0 協定。

Type	設定名稱	API 名稱	可能的值	設定說明
	SSL 3.0	SSL_3_0	啟用、停用	啟用或停用目錄中域控制站用於安全通道通訊 (伺服器和用戶端) 的 SSL 3.0 協定。
	TLS 1.0	TLS_1_0	啟用、停用	啟用或停用目錄中域控制站用於安全通道通訊 (伺服器和用戶端) 的 TLS 1.0 協定。
	TLS 1.1	TLS_1_1	啟用、停用	啟用或停用目錄中域控制站用於安全通道通訊 (伺服器和用戶端) 的 TLS 1.1 協定。

設定適用於 AD 的 AWS Private CA Connector for AWS Managed Microsoft AD

您可以整合 AWS Managed Microsoft AD 與 AWS Private Certificate Authority (CA)，為加入Active Directory網域的使用者、群組和機器發行和管理憑證。 AWS Private CA Connector for Active Directory可讓您為自我管理的企業 CA 使用完全受管 AWS Private CA 的插入式取代，而不需要部署、修補或更新本機代理程式或代理伺服器。 CAs

> **Note**
>
> 目前Active Directory不支援使用 AWS Private CA Connector for 為 AWS Managed Microsoft AD 網域控制站註冊伺服器端 LDAPS 憑證。若要為您的目錄啟用伺服器端 LDAPS，請參閱如何為您的 AWS Managed Microsoft AD 目錄啟用伺服器端 LDAPS。

您可以透過 AWS Directory Service 主控台、 AWS Private CA Connector for Active Directory 主控台或呼叫 `CreateTemplate` API 來設定與 目錄的 AWS Private CA 整合。若要透過 AWS Private CA Connector for Active Directory主控台設定私有 CA 整合，請參閱建立連接器範本。請參閱下列步驟，了解如何從 AWS Directory Service 主控台設定此整合。

設定 AWS Private CA Connector for AD

1. 登入 AWS Management Console ，並在 開啟 AWS Directory Service 主控台https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在應用程式管理索引標籤和AWS 應用程式與服務區段下，選擇 AWS Private CA Connector for AD。隨即顯示為 建立私有 CA 憑證Active Directory頁面。遵循主控台上的步驟，為Active Directory連接器建立私有 CA，以註冊私有 CA。如需詳細資訊，請參閱建立連接器。
4. 建立連接器後，下列步驟會逐步引導您檢視 AWS Private CA Connector for AD 的詳細資訊，包括連接器的狀態和相關聯的 Private CA 狀態。

接著，您將設定 AWS Managed Microsoft AD 的群組政策物件，以便 AWS Private CA Connector for AD 可以發行憑證。

檢視適用於 AD 的 AWS Private CA Connector

1. 登入 AWS Management Console ，並在 開啟 AWS Directory Service 主控台https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在應用程式管理索引標籤和AWS 應用程式與服務區段下，您可以檢視私有 CA 連接器和相關聯的私有 CA。依預設，您會看到下列欄位：

    a. AWS Private CA 連接器 ID — AWS Private CA 連接器的唯一識別符。選取它會導致該 AWS Private CA 連接器的詳細資訊頁面。

b. AWS Private CA subject — CA 辨別名稱的相關資訊。按一下它會進入相應 AWS Private CA 的詳細資訊頁面。

c. 狀態 — 根據 AWS Private CA Connector 和 的狀態檢查 AWS Private CA。如果兩項檢查均透過，則會顯示作用中。如果其中一項檢查失敗，則會顯示 1/2 檢查失敗。如果兩項檢查均失敗，則會顯示失敗。如需失敗狀態的更多資訊，請將滑鼠懸停在超連結上以了解哪個檢查失敗。然後按照主控台中的說明進行修復。

d. 建立日期 — AWS Private CA 連接器的建立日期。

如需詳細資訊，請參閱檢視連接器詳細資訊。

設定 AD 政策

需要設定 CA Connector for AD，以便 AWS Managed Microsoft AD 物件可以請求和接收憑證。在此程序中，您將設定群組政策物件 (GPO)，以便 AWS Private CA 可以向 AWS Managed Microsoft AD 物件發行憑證。

1. 連線至 AWS Managed Microsoft AD 管理員執行個體，並從開始功能表開啟 Server Manager。
2. 在工具下，選取群組政策管理。
3. 在樹系和網域下，尋找子網域組織單位 (OU)（例如，如果您遵循 中概述的程序，則 `corp` 會是子網域組織單位建立 AWS Managed Microsoft AD)，然後在子網域 OU 上按一下滑鼠右鍵。選取在此網域中建立 GPO，並在此處連結...，然後輸入 PCA GPO 做為名稱。選取 OK (確定)。
4. 新建立的 GPO 會顯示在子網域名稱後面。按一下滑鼠右鍵`PCA GPO`，然後選取編輯。如果對話方塊開啟並顯示提醒訊息 This is a link and that changes will be globally propagated，請選取確定以繼續來確認訊息。應開啟群組政策管理編輯器視窗。
5. 在群組政策管理編輯器視窗中，前往電腦組態 > 政策 > Windows 設定 > 安全設定 > 公有金鑰政策（選擇 資料夾）。
6. 在物件類型下，選擇憑證服務用戶端 - 憑證註冊政策。
7. 在憑證服務用戶端 - 憑證註冊政策視窗中，將組態模型變更為已啟用。
8. 確認已勾選並啟用Active Directory註冊政策。選擇新增。
9. Certificate Enrollment Policy Server 對話方塊應開啟。在輸入註冊伺服器政策 URI 欄位中輸入您建立連接器時產生的憑證註冊政策伺服器端點。將身分驗證類型保持為 Windows 整合狀態。
10. 選擇驗證。驗證成功後，選取新增。
11. 返回 Certificate Services 用戶端 - 憑證註冊政策對話方塊，並勾選新建立連接器旁的核取方塊，以確保連接器是預設的註冊政策。

12. 選擇 Active Directory 註冊政策，然後選取移除。
13. 在確認對話方塊中，選擇是以刪除 LDAP 型身分驗證。
14. 在憑證服務用戶端 - 憑證註冊政策視窗中選擇套用，然後選擇確定。然後關閉視窗。
15. 在公有金鑰政策資料夾的物件類型下，選擇憑證服務用戶端 - 自動註冊。
16. 將組態模型選項變更為已啟用。
17. 確認已檢查續約過期憑證和更新憑證選項。讓其他設定保持不變。
18. 選擇套用，然後選擇確定，然後關閉對話方塊。

接著，您將設定使用者組態的公有金鑰政策。

- 前往使用者組態 > 政策 > Windows 設定 > 安全設定 > 公有金鑰政策。請遵循步驟 6 到步驟 21 的先前程序來設定使用者組態的公有金鑰政策。

完成設定 GPOs和公有金鑰政策後，網域中的物件會從 AWS Private CA Connector for AD 請求憑證，並取得 發行的憑證 AWS Private CA。

確認已 AWS Private CA 發行憑證

更新 AWS Private CA 為 AWS Managed Microsoft AD 發行憑證的程序最多可能需要 8 小時。

您可以執行下列任一作業：

- 您可以等待這段時間。
- 您可以重新啟動已設定為從 接收憑證的 AWS Managed Microsoft AD 網域加入機器 AWS Private CA。然後，您可以遵循 Microsoft 文件中的程序，確認 AWS Private CA 已向 AWS Managed Microsoft AD 網域的成員發出憑證。
- 您可以使用下列PowerShell命令來更新 AWS Managed Microsoft AD 的憑證：

```
certutil -pulse
```

監控您的 AWS Managed Microsoft AD

您可以進一步了解不同的 AWS Managed Microsoft AD 狀態及其對 AWS Managed Microsoft AD 的意義，以充分利用 AWS Managed Microsoft AD。您也可以使用 Amazon Simple Notification Service 和 Amazon CloudWatch 等 AWS 服務來監控 AWS Managed Microsoft AD。Amazon Simple Notification

Service 可以傳送 AWS Managed Microsoft AD 目錄狀態的通知給您。Amazon CloudWatch 可以監控 AWS Managed Microsoft AD 網域控制站的效能。

監控 AWS Managed Microsoft AD 的任務

- 了解 AWS Managed Microsoft AD 目錄狀態
- 使用 Amazon Simple Notification Service 啟用 AWS Managed Microsoft AD 目錄狀態通知
- 了解 AWS Managed Microsoft AD 目錄日誌
- 啟用 AWS Managed Microsoft AD 的 Amazon CloudWatch Logs 日誌轉送
- 使用 CloudWatch 監控 AWS Managed Microsoft AD 網域控制站的效能
- 停用 AWS Managed Microsoft AD 的 Amazon CloudWatch 日誌轉送
- 使用 Microsoft 事件檢視器監控 DNS 伺服器

了解 AWS Managed Microsoft AD 目錄狀態

下列是各種目錄狀態。

Active (作用中)

此目錄運作正常。 AWS Directory Service 未在目錄中偵測到任何問題。

正在建立

目前正在建立目錄。建立目錄通常需要 20 到 45 分鐘，但所需時間可能因系統負載而不同。

Deleted (已刪除)

目錄已刪除。目錄的所有資源皆已釋出。一旦目錄進入此狀態，便無法復原。

正在刪除

目前正在刪除目錄。目錄會保持這個狀態，直到完全刪除為止。一旦目錄進入此狀態，將無法取消刪除操作，且目錄無法復原。

失敗

無法建立目錄。請刪除此目錄。如果此問題仍存在，請聯絡 AWS 支援 中心 。

Impaired (受損)

目錄正在降級狀態下執行。已偵測到一個或多個問題，且並非所有目錄操作都能以完整的操作容量運作；目前處於狀態有許多可能的原因。其中包括正常的運作維護活動 (例如修補或 EC2 執行個體輪換)、應用程式在您的其中一個網域控制站上的暫時作用區，或您對不慎中斷目錄通訊的網路所

做的變更。如需詳細資訊，請參閱 Managed AWS Microsoft AD 故障診斷、AD Connector 疑難排解、Simple AD 疑難排解。對於正常維護相關問題， 會在 40 分鐘內 AWS 解決這些問題。在檢閱疑難排解主題之後，如果您的目錄處於「受損」 狀態超過 40 分鐘，建議您聯絡 AWS 支援 中心。

> **Important**
>
> 目錄處於 Impaired (受損) 狀態時，請勿還原快照。還原快照很難解決受損問題。如需詳細資訊，請參閱使用快照還原 AWS Managed Microsoft AD。

Requested (已請求)

目錄的建立請求目前待定中。

RestoreFailed (還原失敗)

從快照中還原目錄失敗，請重試還原操作。如果此情況持續發生，請嘗試其他快照，或聯絡 AWS 支援 中心。

Restoring (正在還原)

目前正從自動或手動快照中還原目錄。從快照中還原目錄通常需要幾分鐘的時間，取決於快照中目錄資料的大小。

使用 Amazon Simple Notification Service 啟用 AWS Managed Microsoft AD 目錄狀態通知

使用 Amazon Simple Notification Service (Amazon SNS)，當目錄狀態有所變更時，您便可以收到電子郵件或文字 (SMS) 簡訊。如果您的目錄從作用中狀態變為受損狀態，您會收到通知。當目錄恢復到 Active (作用中) 狀態時，您也會收到通知。

運作方式

Amazon SNS 使用「主題」來收集和分發訊息。每個主題都有一或多個訂閱者，接收發佈到該主題的訊息。您可以使用下列步驟，將 AWS Directory Service 做為發佈者新增至 Amazon SNS 主題。當 AWS Directory Service 偵測到目錄狀態變更時，它會發佈訊息到該主題，然後傳送給主題的訂閱者。

您可以將多個目錄當成發布者，建立它們與單一主題的關聯性。您也可以將目錄狀態訊息新增至您先前在 Amazon SNS 中建立的主題。您對可以發佈和訂閱主題的人有精細的控制權。如需 Amazon SNS 的完整資訊，請參閱「什麼是 Amazon SNS？」。

> **Note**
>
> 目錄狀態通知是 AWS Managed Microsoft AD 的區域功能。如果您使用的是多區域複寫，則必須在每個區域中分別套用下列程序。如需詳細資訊，請參閱全域與區域功能。

啟用 Amazon SNS

以下將逐步解說如何為 AWS Managed Microsoft AD 啟用 Amazon SNS：

1. 登入 AWS Management Console 並開啟 AWS Directory Service 主控台。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要啟用 SNS 簡訊的區域，然後選擇維護索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇維護索引標籤。
4. 在目錄監控區段中，選擇動作，然後選取建立通知。
5. 在建立通知頁面上，選取選擇通知類型，然後選擇建立新通知。或者，如果您已有現有的 SNS 主題，您可以選擇與現有的 SNS 主題建立關聯性從這個目錄傳送狀態訊息到該主題。

   > **Note**
   >
   > 如果您選擇建立新的通知，但接著卻為已存在的 SNS 主題使用了相同的主題名稱，則 Amazon SNS 不會建立新的主題，只會在現有的主題中新增新的訂閱資訊。
   > 如果您選擇與現有的 SNS 主題建立關聯性，您只能選擇和目錄同一個區域的 SNS 主題。

6. 選擇收件人類型，然後輸入收件人聯絡資訊。如果您輸入適用於 SMS 的電話號碼，請只使用數字。不要包含破折號、空格或括號。
7. (選用) 提供主題的名稱和 SNS 顯示名稱。顯示名稱為不超過 10 個字元的簡稱，包含在這個主題的所有 SMS 訊息中。當您使用 SMS 選項時，需要有顯示名稱。

   > **Note**
   >
   > 如果您使用只有 DirectoryServiceFullAccess 受管政策的 IAM 使用者或角色登入，您的主題名稱必須以「DirectoryMonitoring」開頭。如果您想要進一步自訂主題名稱，則需要 SNS 的其他權限。

8. 選擇建立。

如果您想要指定其他 SNS 訂閱者，例如額外的電子郵件地址、Amazon SQS 佇列或 AWS Lambda，您可以從 Amazon SNS 主控台執行此操作。

從 Amazon SNS 主題移除目錄狀態訊息

以下將逐步解說如何從 Amazon SNS 主題移除 AWS Managed Microsoft AD 目錄狀態訊息：

1. 登入 AWS Management Console 並開啟 AWS Directory Service 主控台。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要移除狀態訊息的區域，然後選擇維護索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇維護索引標籤。
4. 在目錄監控區段中，選取清單中的相應 SNS 主題名稱，選擇動作，然後選取移除。
5. 選擇移除。

這會移除您在選取的 SNS 主題中做為發布者的目錄。

刪除 Amazon SNS 主題

如果您想要刪除整個主題，您可以從 Amazon SNS 主控台執行此操作。

使用 SNS 主控台刪除 Amazon SNS 主題之前，您應該確保目錄不會向該主題傳送狀態訊息。

如果您使用 SNS 主控台刪除 Amazon SNS 主題，此變更不會立即反映在 Directory Services 主控台中。您只會在目錄下次發佈通知至已刪除主題時收到通知，在此情況下，您會在目錄的監控索引標籤上看到更新狀態，指出找不到主題。

因此，為了避免遺失重要的目錄狀態訊息，在刪除接收訊息的任何主題之前 AWS Directory Service，請將您的目錄與不同的 Amazon SNS 主題建立關聯。

如需如何刪除 Amazon SNS 主題的詳細資訊，請參閱刪除 Amazon SNS 主題和訂閱。

了解 AWS Managed Microsoft AD 目錄日誌

AWS Managed Microsoft AD 網域控制器執行個體的安全日誌會封存一年。您也可以設定 AWS Managed Microsoft AD 目錄，以近乎即時的方式將網域控制器日誌轉送至 Amazon CloudWatch Logs。如需詳細資訊，請參閱啟用 AWS Managed Microsoft AD 的 Amazon CloudWatch Logs 日誌轉送。

AWS 會記錄下列事件以確保合規。

監控類別	政策設定	稽核狀態
帳戶登入	稽核登入資料驗證	成功、失敗
	稽核其他帳戶登入事件	成功、失敗
	稽核 Kerberos 身分驗證服務	成功、失敗
帳戶管理	稽核電腦帳戶管理	成功、失敗
	稽核其他帳戶管理事件	成功、失敗
	稽核安全群組管理	成功、失敗
	稽核使用者帳戶管理	成功、失敗
詳細追蹤	稽核 DPAPI 活動	成功、失敗
	稽核 PNP 活動	成功
	稽核程序建立	成功、失敗
DS 存取	稽核目錄服務存取	成功、失敗
	稽核目錄服務變更	成功、失敗
登入/登出	稽核帳戶鎖定	成功、失敗
	稽核登出	成功
	稽核登入	成功、失敗

監控類別	政策設定	稽核狀態
	稽核其他登入/登出事件	成功、失敗
	稽核特殊登入	成功、失敗
物件存取	稽核其他物件存取事件	成功、失敗
	稽核抽取式儲存體	成功、失敗
	稽核集中存取政策執行	成功、失敗
政策變更	稽核政策變更	成功、失敗
	稽核身分驗證政策變更	成功、失敗
	稽核授權政策變更	成功、失敗
	稽核 MPSSVC 規則層級政策變更	成功
	稽核其他政策變更事件	失敗
權限使用	稽核敏感權限使用	成功、失敗
系統	稽核 IPsec 驅動程式	成功、失敗
	稽核其他系統事件	成功、失敗
	稽核安全狀態變更	成功、失敗
	稽核安全系統延伸	成功、失敗
	稽核系統完整性	成功、失敗

啟用 AWS Managed Microsoft AD 的 Amazon CloudWatch Logs 日誌轉送

您可以使用 AWS Directory Service 主控台或 APIs，將網域控制站安全事件日誌轉送至 AWS Managed Microsoft AD 的 Amazon CloudWatch Logs。這可讓目錄中的安全事件公開透明，協助滿足安全監控、稽核和日誌保留政策需求。

CloudWatch Logs 也可以將這些事件轉送至其他 AWS 帳戶、 AWS 服務或第三方應用程式。您可以更輕鬆地集中監控和設定提醒，以近乎即時的速度主動偵測和回應不尋常的活動。

啟用之後，即可使用 CloudWatch Logs 主控台，從您啟用服務時所指定的日誌群組擷取資料。此日誌群組包含您網域控制器的安全日誌。

如需日誌群組以及如何讀取它們的資料的詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的使用日誌群組和日誌串流兩節。

> **Note**
>
> 日誌轉送是 AWS Managed Microsoft AD 的區域功能。如果您使用的是多區域複寫，則必須在每個區域中分別套用下列程序。如需詳細資訊，請參閱全域與區域功能。
> 啟用後，日誌轉送功能將開始將日誌從網域控制站傳輸到指定的 CloudWatch 日誌群組。在啟用日誌轉送之前建立的任何日誌都不會轉移到 CloudWatch 日誌群組。

主題

- 使用 AWS Management Console 啟用 Amazon CloudWatch Logs 日誌轉送
- 使用 CLI 或 PowerShell 啟用 Amazon CloudWatch Logs 日誌轉送

使用 AWS Management Console 啟用 Amazon CloudWatch Logs 日誌轉送

您可以在 中為 AWS Managed Microsoft AD 啟用 Amazon CloudWatch Logs 日誌轉送 AWS Management Console。

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 選擇您要共用之 AWS Managed Microsoft AD 目錄的目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要啟用日誌轉發的區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
4. 在 Log forwarding (日誌轉發) 部分，選擇 Enable (啟用)。
5. 在啟用日誌轉發至 CloudWatch 對話方塊中，選擇下列其中一個選項：
   a. 在 CloudWatch 日誌群組名稱底下，選取建立新的 CloudWatch 日誌群組，指定您可以在 CloudWatch Logs 中參考的名稱。

b. 選取 Choose an existing CloudWatch log group (選擇現有 CloudWatch 日誌群組)，並在 Existing CloudWatch log groups (現有 CloudWatch 日誌群組) 中，從功能表選出一個日誌群組。

6. 檢閱價格資訊和連結，然後選擇 Enable (啟用)。

使用 CLI 或 PowerShell 啟用 Amazon CloudWatch Logs 日誌轉送

使用 `ds create-log-subscription` 指令之前，必須先建立 Amazon CloudWatch 日誌群組，然後建立 IAM 資源政策以授與該群組必要的許可。若要使用 CLI 或 PowerShell 啟用日誌轉送，請完成下列步驟。

步驟 1：在 CloudWatch Logs 中建立日誌群組

建立日誌群組以接收網域控制器的安全日誌。我們建議在名稱前面加上 `/aws/directoryservice/`，但這並非必要步驟。例如：

CLI Command

```
aws logs create-log-group --log-group-name '/aws/directoryservice/d-1111111111'
```

PowerShell Command

```
New-CWLLogGroup -LogGroupName '/aws/directoryservice/d-1111111111'
```

如需有關如何建立 CloudWatch 日誌群組的詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的在 CloudWatch Logs 中建立日誌群組。

步驟 2：在 IAM 中建立 CloudWatch Logs 資源政策

建立 CloudWatch Logs 資源政策，授予將日誌新增至您在步驟 1 中建立之新日誌群組 AWS Directory Service 的權限。您可以指定日誌群組的確切 ARN，以限制 對其他日誌群組 AWS Directory Service的存取，或使用萬用字元來包含所有日誌群組。下列範例政策使用 萬用字元方法，來識別將包含目錄所在`/aws/directoryservice/` AWS 帳戶以 開頭的所有日誌群組。

JSON

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ds.amazonaws.com"
            },
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1: 111122223333:log-group:/aws/
directoryservice/*"
        }
    ]
}
```

您必須在本機工作站上將此政策儲存為文字檔格式 (例如 DSPolicy.json)，以便之後從 CLI 加以執行。例如：

CLI Command

```
aws logs put-resource-policy --policy-name DSLogSubscription --policy-document
          file://DSPolicy.json
```

PowerShell Command

```
$PolicyDocument = Get-Content .\DSPolicy.json –Raw
```

```
Write-CWLResourcePolicy -PolicyName DSLogSubscription -PolicyDocument
 $PolicyDocument
```

步驟 3：建立 AWS Directory Service 日誌訂閱

在此最終步驟中，您可以藉由建立日誌訂閱，來啟用日誌轉發功能。例如：

CLI Command

```
aws ds create-log-subscription --directory-id 'd-1111111111' --log-group-name '/aws/
directoryservice/d-1111111111'
```

PowerShell Command

```
New-DSLogSubscription -DirectoryId 'd-1111111111' -LogGroupName '/aws/
directoryservice/d-1111111111'
```

使用 CloudWatch 監控 AWS Managed Microsoft AD 網域控制站的效能

AWS Directory Service 與 Amazon CloudWatch 整合，可協助您為 中的每個網域控制器提供重要的效能指標Active Directory。這意味著您可以監控域控制站效能計數器，例如 CPU 和記憶體使用率。您也可以設定警報，並啟動自動動作以回應高使用率時段。例如，您可以為域控制站設定 CPU 使用率高於 70% 警報，並建立 SNS 主題以在發生這種情況時獲得通知。您可以使用此 SNS 主題來啟動自動化，例如 AWS Lambda 函數，以增加 的網域控制站數量Active Directory。

如需監控域控制站的詳細資訊，請參閱 決定何時使用 CloudWatch 指標新增網域控制站。

Amazon CloudWatch 需支付相關費用。如需詳細資訊，請參閱 CloudWatch 帳單和成本。

> **Important**
>
> 搭配 CloudWatch 的網域控制站效能指標不適用於加拿大西部 （卡加利） 區域。
> 若要啟用 CloudWatch，請參閱 啟用 AWS Managed Microsoft AD 的 Amazon CloudWatch Logs 日誌轉送。

在 CloudWatch 中尋找網域控制站效能指標

在 Amazon CloudWatch 主控台中，指定服務的指標會先依服務的命名空間分組。您可以新增從屬於該命名空間的指標篩選條件。使用下列程序來尋找在 CloudWatch 中設定 AWS Managed Microsoft AD 網域控制站指標所需的正確命名空間和次級指標。

在 CloudWatch 主控台中尋找域控制站指標

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 指標。
3. 從指標清單中，選取 Directory Service 命名空間，然後從清單中選取 AWS Managed Microsoft AD 指標。

如需如何使用 CloudWatch 主控台設定網域控制器指標的指示，請參閱 安全部落格中的 AWS 如何根據使用率指標自動化 AWS Managed Microsoft AD 擴展。

決定何時使用 CloudWatch 指標新增網域控制站

在所有網域控制站之間進行負載平衡對於 的彈性和效能至關重要Active Directory。為了協助您最佳化 AWS Managed Microsoft AD 中域控制站的效能，我們建議您先監控 CloudWatch 中的重要指標以形成基準。在此過程中，您會分析Active Directory一段時間內的 ，以識別您的平均和尖峰Active Directory使用率。判斷基準後，您可以定期監控這些指標，以協助判斷何時將網域控制站新增至您的 Active Directory。

以下是需要定期監控的重要指標。如需 CloudWatch 中可用域控制站指標的完整清單，請參閱 AWS Managed Microsoft AD 效能計數器。

- 域控制站特定指標，例如：
  - 處理器
  - 記憶體
  - 邏輯磁碟
  - 網路介面
- AWS Managed Microsoft AD 目錄特定指標，例如：
  - LDAP 搜尋
  - 繫結
  - DNS 查詢
  - 目錄讀取
  - 目錄寫入

如需如何使用 CloudWatch 主控台設定網域控制器指標的指示，請參閱 安全部落格中的 AWS 如何根據使用率指標自動化 AWS Managed Microsoft AD 擴展。如需 CloudWatch 指標的一般資訊，請參閱《Amazon CloudWatch 使用者指南》中的使用 Amazon CloudWatch 指標一節。

如需網域控制器規劃的一般資訊，請參閱 Microsoft 網站上的Active Directory網域服務容量規劃。

AWS Managed Microsoft AD 效能計數器

下表列出 Amazon CloudWatch 中可用於追蹤 AWS Managed Microsoft AD 中網域控制站和目錄效能的所有效能計數器。

指標類別	指標名稱
資料庫 ==> 執行個體 (NTDSA)	資料庫快取命中率
	I/O 資料庫讀取平均延遲
	I/O 資料庫讀取/秒
	I/O 日誌寫入平均延遲
DirectoryServices (NTDS)	LDAP 繫結時間
	DRA 待定的複寫操作
	DRA 待定複寫同步
DNS	遞迴查詢/秒
	遞迴查詢失敗/秒
	接收的 TCP 查詢/秒
	接收的查詢總數/秒
	傳送的回應總數/秒
	接收的 UDP 查詢/秒
LogicalDisk	Avg. 磁碟佇列長度
	% 可用空間
記憶體	% 使用中的認可位元組
	長期平均備用快取生命週期 (s)
網路介面	傳送的位元組/秒
	接收的位元組/秒
	目前頻寬

指標類別	指標名稱
NTDS	ATQ 估計佇列延遲
	ATQ 請求延遲
	DS 目錄讀取/秒
	DS 目錄搜尋/秒
	DS 目錄寫入/秒
	LDAP 用戶端工作階段
	LDAP 搜尋/秒
	LDAP 成功繫結/秒
處理器	% 處理器時間
安全全系統範圍統計數字	Kerberos 身分驗證
	NTLM 身分驗證

停用 AWS Managed Microsoft AD 的 Amazon CloudWatch 日誌轉送

您可以在 中停用 AWS Managed Microsoft AD 的 CloudWatch Logs 日誌轉送 AWS Management Console。如需日誌轉送的詳細資訊，請參閱 the section called “使用 CloudWatch 監控您的目錄”。

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 選擇您要共用之 AWS Managed Microsoft AD 目錄的目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要停用日誌轉發的區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
4. 在 Log forwarding (日誌轉發) 部分，選擇 Disable (停用)。
5. 閱讀停用日誌轉送對話方塊中的資訊後，請選擇停用。

使用 Microsoft 事件檢視器監控 DNS 伺服器

您可以稽核 AWS Managed Microsoft AD DNS 事件，以便更輕鬆地識別和疑難排解 DNS 問題。例如，若 DNS 記錄遺失，您可以使用 DNS 稽核事件日誌來協助找出根本原因並解決問題。您也可以使用 DNS 稽核事件日誌來偵測並封鎖來自可疑 IP 地址的請求，進而提升安全性。

若要這麼做，您必須使用 Admin 帳戶登入，或者您登入的帳戶須為 AWS 委派的域名稱系統管理員群組的成員。如需此群組的詳細資訊，請參閱使用 AWS Managed Microsoft AD 建立的內容相關文章。

存取 AWS Managed Microsoft AD DNS 的事件檢視器

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在左側導覽窗格中選擇 (執行個體)。
3. 尋找已加入 AWS Managed Microsoft AD 目錄的 Amazon EC2 執行個體。選取執行個體，然後選取 Connect (連線)。
4. 連線至 Amazon EC2 執行個體後，開啟開始功能表並選取 Windows 系統管理工具資料夾。在系統管理工具資料夾中，選取事件檢視器。
5. 在事件檢視器視窗中，選擇 Action (動作)，然後選擇 Connect to Another Computer (連接到其他電腦)。
6. 選取另一部電腦，輸入其中一個 AWS Managed Microsoft AD DNS 伺服器名稱或 IP 地址，然後選擇確定。
7. 在左側窗格中，導覽到 Applications and Services Logs (應用程式與服務日誌) >Microsoft>Windows>DNS-Server (DNS 伺服器)，然後選取 Audit (稽核)。

從 AWS Managed Microsoft AD 存取 AWS 應用程式和服務

您可以授予 Managed Microsoft AD AWS 使用者的存取權，以存取 AWS 應用程式和服務。其中一些 AWS 應用程式和服務包括：

- Amazon Chime
- Amazon EC2
- QuickSight
- AWS Management Console
- Amazon WorkSpaces

您也可以搭配 AWS Managed Microsoft AD 使用存取 URLs 和單一登入。

從 AWS Managed Microsoft AD 存取 AWS 應用程式和服務的任務

- AWS Managed Microsoft AD 的應用程式相容性
- 啟用 AWS Managed Microsoft AD AWS 的應用程式和服務存取權
- 使用 AWS Managed Microsoft AD 登入資料啟用 AWS Management Console 存取
- 建立 AWS Managed Microsoft AD 的存取 URL
- 啟用 AWS Managed Microsoft AD 的單一登入

AWS Managed Microsoft AD 的應用程式相容性

AWS Directory Service for Microsoft Active Directory (AWS 受管 Microsoft AD) 與多個 AWS 服務和第三方應用程式相容。

以下是相容的 AWS 應用程式和服務清單：

- Amazon Chime
- Amazon Connect
- Amazon EC2
- QuickSight
- Amazon RDS
- WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS IAM Identity Center
- AWS License Manager
- AWS Management Console
- FSx for Windows File Server
- WorkSpaces

如需詳細資訊，請參閱啟用 AWS Managed Microsoft AD AWS 的應用程式和服務存取權。

由於使用 的自訂和商用off-the-shelf應用程式數量龐大Active Directory， AWS 不會也無法執行正式或廣泛的第三方應用程式與 AWS Directory Service for Microsoft Active Directory (AWS 受管 Microsoft

AD) 的相容性驗證。雖然 會與客戶 AWS 合作，嘗試克服他們可能遇到的任何潛在應用程式安裝挑戰，但我們無法保證任何應用程式目前或將繼續與 AWS Managed Microsoft AD 相容。

下列第三方應用程式與 AWS Managed Microsoft AD 相容：

- Active Directory以 為基礎的啟用 (ADBA)
- Active Directory Certificate Services (AD CS): Enterprise Certificate Authority
- Active Directory Federation Services (AD FS)
- Active Directory Users and Computers (ADUC)
- Application Server (.NET)
- Microsoft Entra （ 先前稱為 Azure Active Directory(Azure AD))
- Microsoft Entra Connect （ 先前稱為 Azure Active Directory Connect)
- 分散式檔案系統複寫 (DFSR)
- 分散式檔案系統命名空間 (DFSN)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server （ 包括 SQL Server Always On 可用性群組 ）
- Microsoft System Center Configuration Manager (SCCM) - 部署 SCCM 的使用者必須是 AWS 委派系統管理員群組的成員。
- Microsoft Windows and Windows Server OS
- Office 365

請注意，可能無法支援上述應用程式的一些設定。

相容性指南

雖然應用程式可能會有不相容的設定，應用程式部署設定通常可以克服不相容的問題。以下說明應用程式不相容最常見的原因。客戶可使用此資訊來深入了解理想應用程式的相容性特質，並找出可能的部署變更。

- 網域管理員或其他權限 - 某些應用程式要求您須將其安裝為網域管理員。由於 AWS 必須保留此許可層級的專屬控制權，才能將 Active Directory 做為受管服務提供，因此您無法擔任網域管理員來安裝此類應用程式。不過，您通常可以透過將特定、較少權限和 AWS 支援的許可委派給執行安裝的人員來安裝此類應用程式。如需應用程式要求之具體權限的詳細資訊，請詢問您的應用程式供應商。如需 AWS 允許您委派之許可的詳細資訊，請參閱 使用 AWS Managed Microsoft AD 建立的內容。

- 存取特殊權限Active Directory容器 – 在您的目錄中， AWS 受管 Microsoft AD 會提供組織單位 (OU)，您可以對其進行完整的管理控制。您沒有建立或寫入許可，而且對Active Directory樹狀目錄中高於 OU 的容器的讀取許可可能有限。建立或存取您沒有權限的容器的應用程式，可能無法運作。不過，此類應用程式通常能夠使用您在 OU 建立為替代品的容器。請洽詢您的應用程式供應商，以找到在 OU 建立並使用容器替代品的方法。如需 OU 的詳細資訊，請參閱 使用 AWS Managed Microsoft AD 建立的內容。
- 在安裝工作流程期間變更結構描述 – 有些Active Directory應用程式需要變更預設Active Directory結構描述，而且可能會在應用程式安裝工作流程中嘗試安裝這些變更。由於結構描述延伸項目的特權性質， 只會透過 AWS Directory Service 主控台、CLI 或 SDK 匯入輕量型目錄交換格式 (LDIF) 檔案，AWS 使之成為可能。這類應用程式通常隨附 LDIF 檔案，您可以透過 AWS Directory Service 結構描述更新程序套用到目錄。如需 LDIF 匯入程序運作方式的詳細資訊，請參閱教學課程：擴展 AWS Managed Microsoft AD 結構描述 相關文章。您可以採用某種方式安裝應用程式，以在安裝程序略過結構描述安裝。

已知的不相容應用程式

以下列出我們尚未找到與 AWS Managed Microsoft AD 搭配使用之組態的常見請求商用off-the-shelf應用程式。 會不時自行決定 AWS 更新此清單，以協助您避免不必要的工作。 AWS 提供此資訊，無需就目前或未來的相容性進行保證或聲明。

- Active Directory Certificate Services (AD CS): Certificate Enrollment Web Service
- Active Directory Certificate Services (AD CS): Certificate Enrollment Policy Web Service
- Microsoft Exchange Server
- Microsoft Skype for Business Server

啟用 AWS Managed Microsoft AD AWS 的應用程式和服務存取權

使用者可以授權 AWS Managed Microsoft AD 授予 AWS 應用程式和服務存取權，例如 Amazon WorkSpacesActive Directory。您可以啟用或停用下列 AWS 應用程式和服務，以使用 AWS Managed Microsoft AD。

AWS 應用程式/服務	詳細資訊...
Amazon Chime	如需詳細資訊，請參閱連線至 Active Directory。

AWS 應用程式/服務	詳細資訊...
Amazon Connect	如需詳細資訊，請參閱《Amazon Connect 管理指南》。
Amazon EC2	如需詳細資訊，請參閱將 Amazon EC2 執行個體加入 AWS Managed Microsoft AD 的方法。
Amazon FSx for Windows File Server	如需詳細資訊，請參閱搭配使用 Amazon FSx 與 AWS Directory Service for Microsoft Active Directory。
QuickSight	如需詳細資訊，請參閱搭配使用 Active Directory 與 QuickSight 企業版。
Amazon Relational Database Service	如需詳細資訊，請參閱下列內容： • 使用 MySQL 的 Kerberos 身分驗證 • 搭配 Amazon RDS for Oracle 使用 Kerberos 身分驗證 • 搭配 Amazon RDS for PostgreSQL 使用 Kerberos 身分驗證 • 使用 AWS Managed Microsoft AD 搭配 Amazon RDS for SQL Server
Amazon WorkDocs	如需詳細資訊，請參閱啟用 Amazon WorkDocs for AWS Managed Microsoft AD。
Amazon WorkMail	如需詳細資訊，請參閱建立組織。
Amazon WorkSpaces	您可以直接從 WorkSpaces 建立 Simple AD、AWS Managed Microsoft AD 或 AD Connector。只要在建立工作空間時啟動 Advanced Setup (進階設定) 即可。 如需詳細資訊，請參閱向 WorkSpaces 註冊現有 AWS Directory Service 目錄Personal。

AWS 應用程式/服務	詳細資訊...
AWS Client VPN	如需詳細資訊，請參閱 Active Directory Client VPN 中的身分驗證。
AWS IAM Identity Center	如需詳細資訊，請參閱連線至 Microsoft AD 目錄。
AWS License Manager	如需詳細資訊，請參閱 License Manager 中的管理使用者型訂閱。
AWS Management Console	如需詳細資訊，請參閱使用 AWS Managed Microsoft AD 登入資料啟用 AWS Management Console 存取。
AWS Private Certificate Authority	如需詳細資訊，請參閱 AWS Private CA Connector for Active Directory。
AWS Transfer Family	如需詳細資訊，請參閱設定 SFTP、FTP 或 FTP 伺服器端點。

一旦啟用，您就可以在要授權存取目錄之應用程式或服務的主控台中，管理您目錄的存取。

尋找 AWS 應用程式和服務

若要尋找 AWS 先前在 AWS Directory Service 主控台中描述的應用程式和服務，請執行下列步驟。

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。
4. 檢視 AWS 應用程式和服務區段下的清單。

如需如何使用 授權或取消授權 AWS 應用程式和服務的詳細資訊 AWS Directory Service，請參閱 使用 AWS 的應用程式和服務授權 AWS Directory Service。

使用 AWS Managed Microsoft AD 登入資料啟用 AWS Management Console 存取

AWS Directory Service 可讓您授予目錄成員對 的存取權 AWS Management Console。根據預設，您的目錄成員無法存取任何 AWS 資源。您可以將 IAM 角色指派給目錄成員，讓他們能夠存取各種 AWS 服務和資源。IAM 角色定義您的目錄成員可以存取的服務、資源和層級。

您的目錄必須具有存取 URL，才能授予主控台存取權給目錄成員。如需如何檢視目錄詳細資訊及取得您存取 URL 的詳細資訊，請參閱「檢視 AWS Managed Microsoft AD 目錄資訊」。如需如何建立存取 URL 的詳細資訊，請參閱「建立 AWS Managed Microsoft AD 的存取 URL」。

如需如何建立 IAM 角色並將之指派給您目錄成員的詳細資訊，請參閱「授予 AWS Managed Microsoft AD 使用者和群組存取 AWS 具有 IAM 角色的資源」。

主題

- 啟用 AWS Management Console 存取
- 停用 AWS Management Console 存取
- 設定 AWS Management Console 登入工作階段長度

相關 AWS 安全部落格文章

- 如何使用 AWS Management ConsoleAWS Managed Microsoft AD 和您的現場部署登入資料來存取

相關 AWS re:Post 文章

- 如何授予 AWS Management Console 現場部署Active Directory使用者的 存取權？

> **Note**
>
> 存取 AWS Management Console 是 AWS Managed Microsoft AD 的區域功能。如果您使用的是多區域複寫，則必須在每個區域中分別套用下列程序。如需詳細資訊，請參閱全域與區域功能。

啟用 AWS Management Console 存取

預設不會啟用任何目錄的主控台存取。若要啟用您目錄使用者和群組的主控台存取，請執行下列步驟：

啟用主控台存取

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果您有多個區域顯示在多區域複寫下，請選取您要啟用存取 的區域 AWS Management Console，然後選擇應用程式管理索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇應用程式管理索引標籤。
4. 在 AWS Management Console 區段下，選擇啟用。現在已啟用目錄的主控台存取。

> **Important**
>
> 您必須先將使用者新增至 IAM 角色，使用者才能使用您的存取 URL 登入主控台。如需將使用者指派給 IAM 角色的一般資訊，請參閱「將使用者或群組指派給現有的 IAM 角色」。指派 IAM 角色之後，使用者即可使用您的存取 URL 存取主控台。例如，如果您的目錄存取 URL 是 `example-corp.awsapps.com`，則存取主控台的 URL 是 `https://example-corp.awsapps.com/console/`。

停用 AWS Management Console 存取

若要停用 AWS Managed Microsoft AD 目錄使用者和群組的 AWS Management Console 存取，請執行下列步驟：

停用主控台存取

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果您有多個區域顯示在多區域複寫下，請選取您要停用存取 的區域 AWS Management Console，然後選擇應用程式管理索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇應用程式管理索引標籤。
4. 在 AWS Management Console 區段下，選擇停用。現在已停用目錄的主控台存取。

5. 如果已將任何 IAM 角色指派給目錄中的使用者或群組，則停用按鈕可能無法使用。在此情況下，您必須移除目錄的所有 IAM 角色指派，再繼續進行，包括您目錄中已刪除的使用者或群組指派，這些指派會顯示為已刪除的使用者或已刪除的群組。

   移除所有 IAM 角色指派之後，請重複上述步驟。

設定 AWS Management Console 登入工作階段長度

在預設情況下，使用者在成功登入 後有 1 小時的時間可以使用其工作階段， AWS Management Console 之後才會登出。在此之後，使用者必須重新登入，才能開始下一小時的工作階段，直到再次被登出。您可以使用下列程序，將每個工作階段的時間長度變更至最多 12 小時。

設定 AWS Management Console 登入工作階段長度

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要設定登入工作階段長度的區域，然後選擇應用程式管理索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇應用程式管理索引標籤。
4. 在 AWS 應用程式與服務區段下，選擇 AWS 管理主控台。
5. 在管理資源存取權 AWS 對話方塊中，選擇繼續。
6. 在 Assign users and groups to IAM roles (將使用者和群組指派給 IAM 角色) 頁面中，編輯 Set login session length (設定登入工作階段長度) 下的數值，然後選擇 Save (儲存)。

建立 AWS Managed Microsoft AD 的存取 URL

存取 URL 會與 AWS 應用程式和服務搭配使用，例如 Amazon WorkDocs，以連線到與您的目錄相關聯的登入頁面。您可以透過執行下列步驟，來建立目錄的存取 URL。

考量事項

- 此 URL 必須是全域唯一的。
- 使用多區域目錄時，只能從主要區域設定存取 URL。
- 為此目錄建立應用程式存取 URL 後即無法變更。建立存取 URL 之後，其他人便無法使用之。如果您刪除目錄，此存取 URL 也會被刪除，在此之後便可供其他帳戶使用。

建立存取 URL

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取主要區域，然後選擇應用程式管理索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇應用程式管理索引標籤。
4. 在存取 URL 區段中，如果尚未將存取 URL 指派給目錄，則會顯示建立存取 URL 按鈕。輸入目錄別名，然後選擇建立存取 URL。如果傳回 實體已經存在錯誤，代表指定的目錄別名已經配置。請選擇其他別名並重複此程序。

   存取 URL 以 *<alias>*.awsapps.com 格式顯示。根據預設，此 URL 會帶您前往 WorkDocs 的登入頁面。

啟用 AWS Managed Microsoft AD 的單一登入

AWS Directory Service 可讓您的使用者從加入目錄的電腦存取 WorkDocs，而不必另外輸入登入資料。

啟用單一登入之前，您需要採取額外的步驟，讓您使用者的 Web 瀏覽器支援單一登入。使用者可能需要修改其 Web 瀏覽器設定，才能啟用單一登入。

> **Note**
>
> 單一登入僅適用於加入 AWS Directory Service 目錄的電腦。它無法用於未加入目錄的電腦。

如果您的目錄是 AD Connector 目錄，且 AD Connector 服務帳戶沒有新增或移除其服務主要名稱屬性的權限，則對於以下的步驟 5 和 6，您有兩個選項：

1. 您可以繼續進行，且系統會提示您輸入具有此權限之目錄使用者的使用者名稱和密碼，以便在 AD Connector 服務帳戶上新增或移除服務主要名稱屬性。這些憑證只會用來啟用單一登入，服務不會存放此資料。 AD Connector 服務帳戶權限不會變更。
2. 您可以委派權限，以允許 AD Connector 服務帳戶新增或移除本身的服務主要名稱屬性，您可以從加入網域的電腦使用具有修改 AD Connector 服務帳戶權限的帳戶，以執行下列 PowerShell 命令。下列命令會讓 AD Connector 服務帳戶只能為本身新增和移除服務主要名稱屬性。

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

使用 WorkDocs 啟用或停用單一登入

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。
4. 在應用程式存取 URL 區段中，選擇啟用以啟用 WorkDocs 的單一登入。

   如果您看不到啟用按鈕，您可能需要先建立存取 URL，此選項才會顯示。如需如何建立存取 URL 的詳細資訊，請參閱「建立 AWS Managed Microsoft AD 的存取 URL」。
5. 在啟用此目錄的單一登入對話方塊中，選擇啟用。這會啟用目錄的單一登入。
6. 如果您稍後想要使用 WorkDocs 停用單一登入，請選擇停用，然後在停用此目錄的單一登入對話方塊中，再次選擇停用。

主題

- IE 和 Chrome 的單一登入

- Firefox 的單一登入

IE 和 Chrome 的單一登入

若要讓 Microsoft Internet Explorer (IE) 和 Google Chrome 瀏覽器支援單一登入，您必須在用戶端電腦上執行下列任務：

- 將您的存取 URL (例如 https://<##>.awsapps.com) 新增至允許單一登入的網站清單。
- 啟用動態指令碼處理 (JavaScript)。
- 允許自動登入。
- 啟用整合式身分驗證。

您或您的使用者可以手動執行這些任務，或者您可以使用群組原則設定來變更這些設定。

主題

- 手動更新 Windows 上的單一登入
- 手動更新 OS X 的單一登入
- 單一登入的群組政策設定

手動更新 Windows 上的單一登入

若要在 Windows 電腦上手動啟用單一登入，請在用戶端電腦上執行下列步驟。其中一些設定可能已正確設定。

在 Windows 上手動啟用 Internet Explorer 和 Chrome 的單一登入

1. 若要開啟網際網路內容對話方塊，請選擇開始選單，在搜尋方塊中輸入 `Internet Options`，然後選擇網際網路選項。
2. 執行下列步驟，將您的存取 URL 新增至允許單一登入的網站清單：
   a. 在網際網路內容對話方塊中，選取安全性標籤。
   b. 選取近端內部網路，然後選擇網站。
   c. 在近端內部網路對話方塊中，選擇進階。
   d. 將您的存取 URL 新增至網站清單，然後選擇關閉。
   e. 在近端內部網路對話方塊中，選擇確定。

3. 若要啟用動態指令碼處理，請執行下列步驟：

   a. 在網際網路內容對話方塊的安全性標籤中，選擇自訂等級。

   b. 在安全性設定 - 近端內部網路區域對話方塊中，向下捲動到指令碼處理，然後在 Active scripting 下選取啟用。

   c. 在安全性設定 - 近端內部網路區域對話方塊中，選擇確定。

4. 若要啟用自動登入，請執行下列步驟：

   a. 在網際網路內容對話方塊的安全性標籤中，選擇自訂等級。

   b. 在安全性設定 - 近端內部網路區域對話方塊中，向下捲動到使用者驗證，然後在登入下選取只在近端內部網路區域自動登入。

   c. 在安全性設定 - 近端內部網路區域對話方塊中，選擇確定。

   d. 在安全性設定 - 近端內部網路區域對話方塊中，選擇確定。

5. 若要啟用整合式身分驗證，請執行下列步驟：

   a. 在網際網路內容對話方塊中，選取進階標籤。

   b. 向下捲動到安全性，然後選取啟用整合式 Windows 驗證。

   c. 在網際網路內容對話方塊中，選擇確定。

6. 關閉並重新開啟您的瀏覽器，讓這些變更生效。

手動更新 OS X 的單一登入

若要在 OS X 上手動啟用 Chrome 的單一登入，請在用戶端電腦上執行下列步驟。您需要電腦的管理員權限，才能完成下列步驟。

在 OS X 上手動啟用 Chrome 的單一登入

1. 執行下列命令，將您的存取 URL 新增至 AuthServerAllowlist 政策：

   ```
   defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
   ```

2. 開啟 System Preferences，前往 Profiles 面板，然後刪除 `Chrome Kerberos Configuration` 描述檔。

3. 重新啟動 Chrome，然後在 Chrome 中開啟 chrome://policy 以確認具有此新的設定。

單一登入的群組政策設定

網域管理員可以實作群組原則設定，在加入網域的用戶端電腦上進行單一登入變更。

> **Note**
>
> 如果您使用 Chrome 政策在域中的電腦上管理 Chrome Web 瀏覽器，您必須將存取 URL 新增至 AuthServerAllowlist 政策。如需設定 Chrome 政策的詳細資訊，請前往 Policy Settings in Chrome。

使用群組原則設定啟用 Internet Explorer 和 Chrome 的單一登入

1. 執行下列步驟，建立新的群組原則物件：
   a. 開啟群組原則管理工具，導覽至您的網域，然後選取 Group Policy Objects (群組原則物件)。
   b. 從主選單選擇動作，然後選取新增。
   c. 在新增 GPO 對話方塊中，輸入群組政策物件的描述性名稱 (例如 `IAM Identity Center Policy`)，並將來源入門 GPO 保留設定為 (無)。按一下 OK (確定)。
2. 執行下列步驟，將存取 URL 新增至允許單一登入的網站清單：
   a. 在群組政策管理工具中，導覽至您的域並選取群組政策物件，開啟您 IAM Identity Center 政策的內容 (右鍵) 選單，然後選擇編輯。
   b. 在原則樹狀目錄中，導覽至使用者設定 > 喜好設定 > Windows 設定。
   c. 在 Windows 設定清單中，開啟登錄的內容 (右鍵) 選單，然後選擇新增登錄項目。
   d. 在新登錄內容對話方塊中，輸入下列設定並選擇確定：

      Action

      ```
      Update
      ```

      Hive

      ```
      HKEY_CURRENT_USER
      ```

      路徑

      ```
      Software\Microsoft\Windows\CurrentVersion\Internet Settings
      \ZoneMap\Domains\awsapps.com\<alias>
      ```

<##> 的值是衍生自您的存取 URL。如果您的存取 URL 是 https://examplecorp.awsapps.com，則別名是 examplecorp 且登錄機碼會是 Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp。

值名稱

https

值類型

REG_DWORD

值資料

1

3. 若要啟用動態指令碼處理，請執行下列步驟：

   a. 在群組政策管理工具中，導覽至您的域並選取群組政策物件，開啟您 IAM Identity Center 政策的內容 (右鍵) 選單，然後選擇編輯。

   b. 在原則樹狀目錄中，導覽至電腦設定 > 原則 > 系統管理範本 > Windows 元件 > Internet Explorer > 網際網路控制台 > 安全性畫面 > 內部網路區域。

   c. 在內部網路區域清單中，開啟允許動態指令碼處理的內容 (右鍵) 選單，然後選擇編輯。

   d. 在允許動態指令碼處理對話方塊中，輸入下列設定並選擇確定：

      - 選取已啟用選項按鈕。
      - 在選項下，將允許動態指令碼處理設定為啟用。

4. 若要啟用自動登入，請執行下列步驟：

   a. 在群組原則管理工具中，導覽至您的網域並選取群組原則物件，開啟您 SSO 原則的內容 (右鍵) 選單，然後選擇編輯。

   b. 在原則樹狀目錄中，導覽至電腦設定 > 原則 > 系統管理範本 > Windows 元件 > Internet Explorer > 網際網路控制台 > 安全性畫面 > 內部網路區域。

   c. 在內部網路區域清單中，開啟登入選項的內容 (右鍵) 選單，然後選擇編輯。

   d. 在登入選項對話方塊中，輸入下列設定並選擇確定：

      - 選取已啟用選項按鈕。
      - 在選項下，將登入選項設定為只在近端內部網路區域自動登入。

5. 若要啟用整合式身分驗證，請執行下列步驟：

   a. 在群組政策管理工具中，導覽至您的域並選取群組政策物件，開啟您 IAM Identity Center 政策的內容 (右鍵) 選單，然後選擇編輯。
   b. 在原則樹狀目錄中，導覽至使用者設定 > 喜好設定 > Windows 設定。
   c. 在 Windows 設定清單中，開啟登錄的內容 (右鍵) 選單，然後選擇新增登錄項目。
   d. 在新登錄內容對話方塊中，輸入下列設定並選擇確定：

      Action

      ```
      Update
      ```

      Hive

      ```
      HKEY_CURRENT_USER
      ```

      路徑

      ```
      Software\Microsoft\Windows\CurrentVersion\Internet Settings
      ```

      值名稱

      ```
      EnableNegotiate
      ```

      值類型

      ```
      REG_DWORD
      ```

      值資料

      ```
      1
      ```

6. 關閉仍然保持開啟狀態的群組原則管理編輯器視窗。
7. 執行下列步驟，將新的原則指派給您的網域：

   a. 在群組原則管理樹狀目錄中，開啟網域的內容 (右鍵) 選單，然後選擇連結到現有的 GPO。
   b. 在群組政策物件清單中，選取您的 IAM Identity Center 政策，然後選擇確定。

這些變更會在用戶端上的群組原則下次更新，或在使用者下次登入之後生效。

Firefox 的單一登入

若要讓 Mozilla 的 Firefox 瀏覽器支援單一登入，請將您的存取 URL (例如 https://<##>.awsapps.com) 新增至允許單一登入的網站清單。這可手動或透過指令碼自動完成。

主題

- 手動更新單一登入
- 自動更新單一登入

手動更新單一登入

若要在 Firefox 中將您的存取 URL 手動新增至允許的網站清單，請在用戶端電腦上執行下列步驟。

在 Firefox 中將您的存取 URL 手動新增至允許的網站清單

1. 開啟 Firefox，然後開啟 `about:config` 頁面。
2. 開啟 `network.negotiate-auth.trusted-uris` 偏好設定，然後將您的存取 URL 新增至網站清單。請使用逗號 (,) 來分隔多個項目。

自動更新單一登入

身為域管理員，您可以使用指令碼，將存取 URL 新增至網路上所有電腦的 Firefox `network.negotiate-auth.trusted-uris` 使用者偏好設定。如需詳細資訊，請前往 https://support.mozilla.org/zh-TW/questions/939037。

授予 AWS Managed Microsoft AD 使用者和群組存取 AWS 具有 IAM 角色的資源

AWS Directory Service 可讓您的 AWS Managed Microsoft AD 使用者和群組存取 AWS 服務和資源，例如存取 Amazon EC2 主控台。類似於授予 IAM 使用者管理目錄的存取權，如 中所述身分類型政策 (IAM 政策)，為了讓目錄中的使用者能夠存取其他 AWS 資源，例如 Amazon EC2，您必須將 IAM 角色和政策指派給這些使用者和群組。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色。

如需如何授予使用者存取權的詳細資訊 AWS Management Console，請參閱 使用 AWS Managed Microsoft AD 登入資料啟用 AWS Management Console 存取。

主題

- 建立新的 IAM 角色
- 編輯現有 IAM 角色的信任關係
- 將使用者或群組指派給現有的 IAM 角色
- 檢視指派給角色的使用者和群組

- 從 IAM 角色移除使用者或群組
- 搭配 使用 AWS 受管政策 AWS Directory Service

建立新的 IAM 角色

如果您需要建立新的 IAM 角色以搭配 使用 AWS Directory Service，則必須使用 IAM 主控台來建立角色。建立角色之後，您必須先設定與該角色的信任關係，才能在 AWS Directory Service 主控台中看到該角色。如需詳細資訊，請參閱編輯現有 IAM 角色的信任關係。

> **Note**
>
> 執行此任務的使用者必須具備執行下列 IAM 動作的許可。如需詳細資訊，請參閱身分類型政策 (IAM 政策)。
>
> - iam:PassRole
> - iam:GetRole
> - iam:CreateRole
> - iam：PutRolePolicy

在 IAM 主控台中建立新的角色

1. 在 IAM 主控台的導覽窗格中，選擇角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色 (AWS Management Console) 一節。
2. 選擇建立角色。
3. 在 Choose the service that will use this role (選擇將使用此角色的服務) 下，選擇 Directory Service (目錄服務)，然後選擇 Next (下一步)。
4. 選取您要套用到目錄使用者的政策 (例如 AmazonEC2FullAccess) 旁的核取方塊，然後選擇 Next (下一步)。
5. 如有必要，將標籤新增到該角色，然後選擇 Next (下一步)。
6. 提供 Role name (角色名稱) 和選用 Description (說明)，然後選擇 Create role (建立角色)。

範例：建立角色以啟用 AWS Management Console 存取

下列檢查清單提供您必須完成的任務範例，才能建立新的 IAM 角色，讓特定 AWS Managed Microsoft AD 使用者能夠存取 Amazon EC2 主控台。

1. 使用上述程序，以 IAM 主控台建立一個角色。當提示您輸入政策，請選擇 AmazonEC2FullAccess。
2. 使用編輯現有 IAM 角色的信任關係中的步驟來編輯您剛建立的角色，然後新增必要的信任關係資訊至政策文件。在下一個步驟中啟用對 AWS Management Console 的存取之後，需要此步驟才能立即顯示角色。
3. 依照使用 AWS Managed Microsoft AD 登入資料啟用 AWS Management Console 存取中的步驟來設定 AWS Management Console的一般存取。
4. 遵循將使用者或群組指派給現有的 IAM 角色中的步驟，將需要 EC2 資源完整存取權的使用者新增到新的角色。

編輯現有 IAM 角色的信任關係

您可以將現有的 IAM 角色指派給 AWS Directory Service 使用者和群組。不過，若要這樣做，角色必須與 建立信任關係 AWS Directory Service。當您使用 在 中使用 程序 AWS Directory Service 建立角色時建立新的 IAM 角色，會自動設定此信任關係。

> **Note**
>
> 您只需要為非 AWS Directory Service建立的 IAM 角色建立此信任關係。

建立現有 IAM 角色的信任關係 AWS Directory Service

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在 IAM 主控台導覽窗格的存取管理中，選擇角色。

   主控台會顯示您帳戶的角色。
3. 選擇您要修改之角色的名稱，然後在角色頁面上，選取信任關係索引標籤。
4. 選擇編輯信任政策。
5. 在政策文件，貼上以下內容，然後選擇更新政策。

   JSON

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

您也可以使用 AWS CLI更新此政策文件。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 update-trust 一節。

將使用者或群組指派給現有的 IAM 角色

您可以將現有的 IAM 角色指派給 AWS Managed Microsoft AD 使用者或群組。若要執行此作業，請確定您已完成下列操作。

先決條件

- 建立 AWS Managed Microsoft AD。
- 建立 IAM 使用者或建立 IAM 群組。
- 建立與 有信任關係的角色 AWS Directory Service。對於現有的 IAM 角色，您將需要編輯現有角色的信任關係。

> **Important**
>
> 不支援在目錄中巢狀群組中存取 AWS Managed Microsoft AD 使用者。父群組的成員可存取主控台，但子群組的成員則否。

將 AWS Managed Microsoft AD 使用者或群組指派給現有的 IAM 角色

1. 在 AWS Directory Service 主控台導覽窗格中的 Active Directory 下，選擇目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：

a. 如果多區域複寫下沒有顯示任何區域，請選擇應用程式管理索引標籤。

b. 如果多區域複寫下顯示多個區域，請選取要進行指派的區域，然後選擇應用程式管理索引標籤。如需詳細資訊，請參閱主要區域與其他區域。

4. 向下捲動至 AWS Management Console區段，選擇動作和啟用。
5. 在委派主控台存取區段下，選擇您要指派使用者之現有 IAM 角色的 IAM 角色名稱。
6. 在 Selected role (選取的角色) 頁面的 Manage users and groups for this role (管理此角色的使用者和群組) 下，選擇 Add (新增)。
7. 在將使用者和群組新增至角色頁面的選取 Active Directory 樹系 下，選擇包含需要存取 AWS Management Console之帳戶所在的 AWS Managed Microsoft AD 樹系 (此樹系) 或內部部署樹系 (信任樹系)。如需如何設定信任樹系的詳細資訊，請參閱「教學：在 AWS Managed Microsoft AD 和自我管理的 Active Directory 域之間建立信任關係」。
8. 在 Specify which users or groups to add (指定要新增的使用者或群組) 下，選取 Find by user (依使用者尋找) 或 Find by group (依群組尋找)，然後輸入使用者或群組的名稱。在可能的相符項目清單中，選擇您要新增的使用者或群組。
9. 選擇 Add (新增)，完成將使用者和群組指派給角色。

檢視指派給角色的使用者和群組

若要檢視指派給 IAM 角色的 AWS Managed Microsoft AD 使用者和群組，請執行下列步驟。

先決條件

- 建立 AWS Managed Microsoft AD。
- 建立 IAM 使用者或建立 IAM 群組。
- 建立與 有信任關係的角色 AWS Directory Service。對於現有的 IAM 角色，您將需要編輯現有角色的信任關係。
- 將您的使用者或群組指派給現有的 IAM 角色。

檢視指派給 IAM 角色的 AWS Managed Microsoft AD 使用者和群組

1. 在AWS Directory Service 主控台導覽窗格中的 下Active Directory，選擇目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：

a. 如果多區域複寫下顯示多個區域，請選取要檢視指派的區域，然後選擇應用程式管理索引標籤。如需詳細資訊，請參閱主要區域與其他區域。

b. 如果多區域複寫下沒有顯示任何區域，請選擇應用程式管理索引標籤。

4. 向下捲動至 AWS Management Console區段。狀態應為已啟用。如果沒有，請選擇動作並啟用。如需詳細資訊，請參閱使用 AWS Managed Microsoft AD 登入資料啟用 AWS Management Console 存取。

> **Note**
>
> 如果 AWS Management Console 停用 ，則不會看到任何群組或使用者。

5. 在委派主控台存取區段下，選取您要檢視之 IAM 角色的超連結。或者，您可以在 IAM 中選取檢視政策，以在 IAM 主控台中檢視 IAM 政策。

6. 在選取的角色頁面上，在此角色的管理使用者和群組區段下，您可以檢視指派給 IAM 角色的使用者和群組。

從 IAM 角色移除使用者或群組

若要從 IAM 角色移除 AWS Managed Microsoft AD 使用者或群組，請執行下列步驟。

從 IAM 角色移除使用者或群組

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。

2. 在 Directories (目錄) 頁面中，選擇目錄 ID。

3. 在目錄詳細資訊頁面上，執行下列其中一項：

a. 如果多區域複寫下顯示多個區域，請選取要移除指派的區域，然後選擇應用程式管理索引標籤。如需詳細資訊，請參閱主要區域與其他區域。

b. 如果多區域複寫下沒有顯示任何區域，請選擇應用程式管理索引標籤。

4. 在 AWS Management Console區段下，選擇您要從中移除使用者和群組的 IAM 角色。

5. 在 Selected role (選取的角色) 頁面的 Manage users and groups for this role (管理此角色的使用者和群組) 下，選取要從中移除角色的使用者或群組，然後選擇 Remove (移除) 該角色會隨即從指定的使用者和群組移除，但不會從您的帳戶移除。

> **Note**
>
> 如果您想要刪除角色，請參閱刪除角色或執行個體描述檔。

搭配 使用 AWS 受管政策 AWS Directory Service

AWS Directory Service 提供下列 AWS 受管政策，讓您的使用者和群組存取 AWS 服務和資源，例如存取 Amazon EC2 主控台。您必須先登入 AWS Management Console 才能檢視這些政策。

- 唯讀存取
- 進階使用者存取
- AWS Directory Service 完整存取
- AWS Directory Service 唯讀存取
- AWS Directory Service Data 完整存取
- AWS Directory Service Data 唯讀存取
- Amazon 雲端目錄完整存取
- Amazon 雲端目錄唯讀存取
- Amazon EC2 完整存取
- Amazon EC2 唯讀存取
- Amazon VPC 完整存取
- Amazon VPC 唯讀存取
- Amazon RDS 完整存取
- Amazon RDS 唯讀存取
- Amazon DynamoDB 完整存取
- Amazon DynamoDB 唯讀存取
- Amazon S3 完整存取
- Amazon S3 唯讀存取
- AWS CloudTrail 完整存取
- AWS CloudTrail 唯讀存取
- Amazon CloudWatch 完整存取

- Amazon CloudWatch 唯讀存取
- Amazon CloudWatch Logs 完整存取
- Amazon CloudWatch Logs 唯讀存取

如需如何建立自有政策的詳細資訊，請參閱《IAM 使用者指南》中的管理 AWS 資源的範例政策。

設定 AWS Managed Microsoft AD 的多區域複寫

多區域複寫可用於自動跨多個 複寫 AWS Managed Microsoft AD 目錄資料 AWS 區域。此複寫可以改善分散地理位置中使用者和應用程式的效能。 AWS 受管 Microsoft AD 使用原生Active Directory複寫，將目錄的資料安全地複寫到新區域。

只有 AWS Managed Microsoft AD 企業版支援多區域複寫。

您可以在可使用 AWS Managed Microsoft AD 的大多數區域中使用自動多區域複寫。

Important

選擇加入的區域無法使用多區域複寫。以下是選擇加入的區域：

- 非洲 (開普敦) af-south-1
- 亞太區域 (香港) ap-east-1
- 亞太區域 (海德拉巴) ap-south-2
- 亞太區域 (雅加達) ap-southeast-3
- 亞太區域 (墨爾本) ap–southeast–4
- 亞太區域 （ 泰國 ） ap-southeast-7
- 加拿大西部 （ 卡加利 ） ca-west-1
- 歐洲 (米蘭) eu-south-1
- 歐洲 (西班牙) eu–south–2
- 歐洲 (蘇黎世) eu–central–2
- 以色列 （ 特拉維夫 ） il-central-1
- 中東 (巴林) me-south-1
- 中東 (阿拉伯聯合大公國) me-central-1
- 墨西哥 （ 中部 ） mx-central-1

如需有關選擇加入區域以及如何啟用的詳細資訊，請參閱《AWS 帳戶管理 指南》中的指定您的帳戶可使用的 AWS 區域 一節。

多區域複寫的運作方式

使用多區域複寫功能， AWS 受管 Microsoft AD 可免除管理全域Active Directory基礎設施的繁重工作。設定後， AWS 會跨多個 複寫所有客戶目錄資料，包括使用者、群組、群組政策和結構描述 AWS 區域。

新增區域後，將自動發生以下操作，如圖所示：

- AWS Managed Microsoft AD 會在選取的 VPC 中建立兩個網域控制站，並將其部署到相同 AWS 帳戶中的新區域。目錄識別符 (`directory_id`) 在所有區域中保持不變。如果需要，您可以稍後新增更多域控制站。
- AWS Managed Microsoft AD 會設定主要區域與新區域之間的網路連線。
- AWS Managed Microsoft AD 會建立新的Active Directory網站，並提供與該區域相同的名稱，例如 us-east-1。您也可以稍後使用 Active Directory 站台及服務工具對其進行重新命名。
- AWS Managed Microsoft AD 會將所有 Active Directory 物件和組態複寫到新區域，包括使用者、群組、群組政策、Active Directory 信任、組織單位和 Active Directory 結構描述。設定 Active Directory 站台連結以使用變更通知。啟用站台之間的變更通知後，變更將以與在來源站台內傳播的頻率傳播到遠端站台，包括需要進行緊急複寫的變更。
- 如果這是您新增的第一個區域， AWS 受管 Microsoft AD 會讓所有功能多區域都知道。如需詳細資訊，請參閱全域與區域功能。

Active Directory 網站

多區域複寫支援多個Active Directory網站 （ 每個區域一個Active Directory網站 ）。新增區域時，會為其指定與相應區域相同的名稱，例如 us–east–1。您也可以稍後使用Active Directory網站和服務重新命名此項目。

AWS 服務

AWS Amazon RDS for SQL Server 和 Amazon FSx 等 服務會連線至 全域目錄的本機執行個體。這可讓您的使用者登入一次 中執行的Active Directory感知應用程式 AWS ，以及任何 AWS 區域中的

Amazon RDS for SQL Server 等 AWS 服務。若要這樣做，當您信任 AWS Managed Microsoft AD Active Directory時，使用者需要 AWS 來自 Managed Microsoft AD 或內部部署的登入資料。

您可以使用下列 AWS 服務搭配多區域複寫功能。

- Amazon EC2
- Amazon FSx for Windows File Server
- Amazon Relational Database Service for SQL Server
- Amazon RDS for Oracle
- Amazon RDS for MySQL
- Amazon RDS for PostgreSQL
- Amazon RDS for MariaDB
- Amazon Aurora for MySQL
- Amazon Aurora for PostgreSQL

容錯移轉

如果一個區域中的所有網域控制站都故障， AWS 受管 Microsoft AD 會復原網域控制站，並自動複寫目錄資料。同時，其他區域的域控制站保持正常運作。

多區域複寫的優點

在 AWS Managed Microsoft AD 中使用多區域複寫時， Active Directory感知應用程式會在本機使用 目錄以獲得高效能，並使用多區域功能來提供彈性。您可以使用多區域複寫搭配 Active Directory感知應用程式，例如 SharePoint 和 SQL Server Always On，以及 Amazon RDS for SQL Server 和 FSx for Windows File Server 等 AWS 服務。以下是多區域複寫的其他優勢。

- 它可讓您快速地全域部署單一 AWS Managed Microsoft AD 執行個體，並消除自我管理全球Active Directory基礎設施的繁重工作。
- 它可讓您在多個 AWS 區域中更輕鬆且更具成本效益地部署和管理 Windows 和 Linux 工作負載。自動化多區域複寫可讓您的全域 Active Directory感知應用程式中獲得最佳效能。在 Windows 或 Linux 執行個體中部署的所有應用程式都會在 區域本機使用 AWS Managed Microsoft AD，以便盡可能回應來自最接近區域的使用者請求。
- 它提供多區域彈性。 AWS 受管 Microsoft AD 部署在高可用性的 AWS 受管基礎設施中，可處理所有區域中基礎Active Directory基礎設施的自動化軟體更新、監控、復原和安全性。這使您可以專注於建立應用程式。

主題

- 全域與區域功能
- 主要區域與其他區域
- 新增 AWS Managed Microsoft AD 的複寫區域
- 刪除 AWS Managed Microsoft AD 的複寫區域

全域與區域功能

當您使用多區域複寫將 AWS 區域新增至目錄時， AWS Directory Service 會增強所有功能的範圍，使其成為區域感知。當您在 AWS Directory Service 主控台中選擇目錄的 ID 時，顯示的詳細資訊頁面會在各個索引標籤上列出這些功能。這表示所有功能都是根據您在主控台的多區域複寫區段中選取的區域啟用、設定和管理。對每個區域中的功能所做的變更會全域套用或按區域套用。

只有 AWS Managed Microsoft AD 企業版支援多區域複寫。

全域功能

選取 主要區域 時對全域功能所做的任何變更都會套用至所有區域。

您可以在目錄詳細資訊頁面上識別全域使用的功能，因為這些功能旁邊會顯示已套用至所有複寫的區域字樣。如果您在清單中選取的是其他區域不是主要區域，全域使用的功能旁邊會顯示已從主要區域繼承字樣。

區域功能

您對 其他區域 中的功能所做的任何變更將僅套用於相應區域。

您可以在目錄詳細資訊頁面上識別區域功能，因為這些功能旁邊不會顯示已套用至所有複寫的區域或已從主要區域繼承字樣。

主要區域與其他區域

使用多區域複寫時， AWS 受管 Microsoft AD 會使用下列兩種區域類型來區分全域或區域功能應如何套用至您的目錄。

主要區域

您首次建立目錄的初始區域稱為主要區域。您只能執行全域目錄層級操作，例如從主要區域建立Active Directory信任和更新 AD 結構描述。

主要區域始終會顯示為多區域複寫區段中清單頂部的第一個區域，並以「–主要」結尾。例如，美國東部 (維吉尼亞北部)– 主要。

您在選取主要區域全域功能時所做的任何變更都會套用至所有區域。

您只能在選取主要區域時新增區域。如需詳細資訊，請參閱新增 AWS Managed Microsoft AD 的複寫區域。

其他區域

您新增至目錄的任何區域稱為其他區域。

儘管某些功能可以針對所有區域進行全域管理，但其他功能則按區域單獨管理。若要管理其他區域 (非主要區域) 的功能，您必須先從目錄詳細資訊頁面上的多區域複寫區段的清單中選取其他區域。然後方可以管理相關功能。

選取其他區域時對 區域功能 所做的任何變更將僅套用於相應區域。

新增 AWS Managed Microsoft AD 的複寫區域

當您使用 設定 AWS Managed Microsoft AD 的多區域複寫功能新增區域時， AWS 受管 Microsoft AD 會在所選 AWS 區域、Amazon Virtual Private Cloud (VPC) 和子網路中建立兩個網域控制站。 AWS 受管 Microsoft AD 也會建立相關的安全群組，讓 Windows 工作負載能夠連線到新區域中的目錄。它還使用已部署目錄的相同 AWS 帳戶來建立這些資源。您透過選擇區域、指定 VPC 並提供新區域的組態來完成此操作。

多區域複寫僅支援 AWS Managed Microsoft AD 企業版。

先決條件

在繼續執行新增複寫區域的步驟之前，我們建議您先檢視下列事前準備事項。

- 確認您擁有必要的 AWS Identity and Access Management (IAM) 許可、Amazon VPC 設定，以及您要複寫目錄的新區域中的子網路設定。
- 如果您想要使用現有的現場部署 Active Directory 登入資料來存取和管理 中的 Active Directory 感知工作負載 AWS，則必須在 AWS Managed Microsoft AD 和您的現場部署 AD 基礎設施之間建立 Active Directory 信任。如需信任的詳細資訊，請參閱 將 AWS Managed Microsoft AD 連接至現有的 Active Directory 基礎設施。
- 如果您的現場部署 Active Directory 與您想要新增複寫區域之間存在現有的信任關係，則需要驗證您在想要複寫目錄的新區域中具有必要的 Amazon VPC 和子網路設定。

您也可以在 AWS Managed Microsoft AD 和內部部署 AD 基礎設施之間建立信任，以便使用現有的內部部署 Active Directory 憑證來管理 AD 感知工作負載。如需詳細資訊，請參閱將 AWS Managed Microsoft AD 連接至現有的 Active Directory 基礎設施。

新增區域

使用下列程序為您的 AWS Managed Microsoft AD 目錄新增複寫區域。

新增複寫區域

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上的多區域複寫下，從清單中選擇主要區域，然後選擇新增區域。

> **Note**
>
> 您只能在選取主要區域時新增區域。如需詳細資訊，請參閱主要區域。

4. 在新增區域頁面上的區域下，從清單中選擇要新增的區域。
5. 在 VPC 下，選擇要用於該區域的 VPC。

> **Note**
>
> 此 VPC 不得具有與此目錄在另一個區域中使用的 VPC 重疊的無類別域間路由 (CIDR)。

6. 在子網路 下，選擇要用於該區域的子網路。
7. 檢視定價下的資訊，然後選擇新增。
8. 當 AWS Managed Microsoft AD 完成網域控制站部署程序時，區域會顯示作用中狀態。現在您可以根據需要對此區域進行更新。

後續步驟

新增區域之後，您應該考慮進行以下後續步驟：

- 根據需要將其他的域控制站 (最多 20 個) 部署到新區域。新增區域時的域控制站數量預設為 2 個，這是實現容錯和高可用性目的所需的最小數目。如需詳細資訊，請參閱使用 新增或移除其他網域控制站 AWS Management Console。

> **Note**
>
> 當您將複寫的 AWS 區域 新增至 AWS Managed Microsoft AD 時，預設會建立兩個網域控制站，這是容錯能力和高可用性所需的網域控制站數目下限。

- 與每個區域的更多 AWS 帳戶共用您的目錄。目錄共用組態不會自動從主要區域複寫。如需詳細資訊，請參閱共用您的 AWS Managed Microsoft AD。

> **Note**
>
> 目錄共用組態不會在主要 中自動複寫 AWS 區域。

- 啟用日誌轉送，使用來自新區域的 Amazon CloudWatch Logs 擷取目錄的安全日誌。啟用日誌轉發時，您必須在複寫目錄的每個區域中提供日誌群組名稱。如需詳細資訊，請參閱啟用 AWS Managed Microsoft AD 的 Amazon CloudWatch Logs 日誌轉送。

> **Note**
>
> 啟用日誌轉送時，您必須在複寫目錄的每個 AWS 區域 中提供日誌群組的名稱。

- 為新區域啟用 Amazon Simple Notification Service (Amazon SNS) 監控，以追蹤每個區域的目錄運作狀況。如需詳細資訊，請參閱使用 Amazon Simple Notification Service 啟用 AWS Managed Microsoft AD 目錄狀態通知。

刪除 AWS Managed Microsoft AD 的複寫區域

使用下列程序來刪除 AWS Managed Microsoft AD 目錄的區域。在刪除區域之前，請確認相關區域不存在以下任一情況：

- 連接了授權的應用程式。
- 具有與之關聯的共用目錄。

刪除複寫區域

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 從導覽列中，新增區域選取器，然後選擇存放目錄的區域。

3. 在 Directories (目錄) 頁面中，選擇目錄 ID。
4. 在目錄詳細資訊頁面上的多區域複寫下，選擇刪除區域。
5. 在刪除區域對話方塊中，檢視訊息，然後輸入區域名稱進行確認。然後選擇 Delete (刪除)。

> **Note**
>
> 當區域正在被刪除時，您無法對其進行更新。

共用您的 AWS Managed Microsoft AD

AWS Managed Microsoft AD 與 緊密整合 AWS Organizations ，以允許跨多個 的無縫目錄共用 AWS 帳戶。您可以與同一組織內其他信任 AWS 帳戶 的 共用單一目錄，或與組織外 AWS 帳戶 的其他 共用該目錄。當您的 目前 AWS 帳戶 不是組織的成員時，您也可以共用您的目錄。

重要的目錄共享概念

如果您熟悉下列重要概念，將能充分利用目錄共用功能。

目錄擁有者帳戶

目錄擁有者是擁有共用目錄關係中原始目錄的 AWS 帳戶 擁有者。此帳戶中的管理員會指定與其共用其目錄的對象，以啟動目錄 AWS 帳戶 共用工作流程。目錄擁有者可以使用 Scale & Share (擴展和共享) 索引標籤，在 AWS Directory Service 主控台中的指定目錄中檢視與其共享目錄的人員。

目錄消費者帳戶

在共享目錄關係中，目錄消費者代表目錄擁有者與其共享目錄的 AWS 帳戶 。根據所用的共享方法，此帳戶中的管理員可能需要先接受目錄擁有者發出的邀請，才能開始使用共享的目錄。

目錄共享程序會在目錄消費者帳戶中建立共享目錄。這個共享目錄包含的中繼資料，能讓 EC2 執行個體無縫加入網域，並在目錄擁有者帳戶中找出發起的目錄。目錄消費者帳戶中的每個共享目錄，都有唯一的識別碼 Shared directory ID (共享目錄 ID)。

共享方法

AWS Managed Microsoft AD 提供下列兩種目錄共用方法：

- AWS Organizations – 運用這個方法，在組織中共享目錄將會更輕鬆，因為您可以瀏覽和驗證目錄消費者帳戶。若要使用此選項，您的組織必須先啟用所有功能，而且您的目錄必須在組織管理帳戶之中。此共用方法可簡化您的設定，因為它不需要目錄消費者帳戶接受您的目錄共用請求。在 主控台中，此方法稱為 AWS 帳戶 與組織內的 共用此目錄。
- 交握 – 此方法可在不使用 時啟用目錄共用 AWS Organizations。此交握方法在進行時會要求目錄消費者帳戶接受目錄共享請求。在主控台中，此方法稱為與其他 AWS 帳戶共用此目錄。

網路連線能力

網路連線是跨 使用目錄共用關係的先決條件 AWS 帳戶。 AWS 支援許多解決方案來連接 VPCs，其中一些包括 VPC 對等互連、Transit Gateway 和 VPN。若要開始使用，請參閱教學課程：共用 AWS Managed Microsoft AD 目錄以實現無縫 EC2 加入網域。

考量事項

以下是將目錄共用與 AWS Managed Microsoft AD 搭配使用時的一些考量：

定價

- AWS 會收取目錄共用的額外費用。使用共用 AWS Managed Microsoft AD AWS 帳戶 的 是收取共用費用的帳戶。若要進一步了解，請參閱 AWS Directory Service 網站上的 定價頁面。
- 目錄共用讓 AWS Managed Microsoft AD 在多個帳戶和 VPCs 中與 Amazon EC2 整合時更具成本效益。

區域可用性

- 提供 AWSAWS Managed Microsoft AD 的所有區域都提供目錄共用。
- AWS 在中國 （寧夏），此功能僅適用於使用 AWS Systems Manager(SSM) 無縫加入 Amazon EC2 執行個體時。

如需目錄共用以及如何跨 AWS 帳戶邊界擴展 AWS Managed Microsoft AD 目錄範圍的詳細資訊，請參閱下列主題。

主題

- 教學課程：共用 AWS Managed Microsoft AD 目錄以實現無縫 EC2 加入網域
- 取消共用您的目錄

教學課程：共用 AWS Managed Microsoft AD 目錄以實現無縫 EC2 加入網域

本教學課程說明如何與另一個（目錄消費者帳戶）共用 AWS Managed Microsoft AD 目錄 AWS 帳戶（目錄擁有者帳戶）。聯網先決條件完成後，您將在兩個 之間共用目錄 AWS 帳戶。然後，您將了解如何將 EC2 執行個體無縫加入目錄消費者帳戶中的網域。

我們建議您先檢閱目錄共享重要概念和使用案例，再開始處理這份教學課程的內容。如需詳細資訊，請參閱重要的目錄共享概念。

共用目錄的程序會因您是否與相同 AWS 組織中 AWS 帳戶 的另一個 或 AWS 組織外部的帳戶共用目錄而有所不同。如需共享運作方式的詳細資訊，請參閱共享方法。

此工作流程有四個基本步驟。

步驟 1：設定聯網環境

在目錄擁有者帳戶中，您會設定共享目錄程序的所有必要聯網先決條件。

步驟 2：共享您的目錄

在使用目錄擁有者管理員登入資料登入情況下，您會開啟 AWS Directory Service 主控台，並啟動共享目錄工作流程，而其會向目錄消費者帳戶發出邀請。

步驟 3：接受共用目錄邀請 - 選用

使用目錄消費者管理員登入資料登入時，您可以開啟 AWS Directory Service 主控台並接受目錄共用邀請。

步驟 4：測試將適用於 Windows Server 的 EC2 執行個體無縫加入域

最後，您會以目錄消費者管理員的身分，嘗試將 EC2 執行個體加入至網域，並且驗證其運作正常。

其他資源

- 使用案例：共享您的目錄以便跨 AWS 帳戶將 Amazon EC2 執行個體無縫加入域
- AWS 安全部落格文章：如何將 Amazon EC2 執行個體從多個帳戶和 VPCs 加入單一 AWS 受管 Microsoft AD 目錄

步驟 1：設定聯網環境

您需要建立 Amazon VPC 對等互連，才能與另一個（目錄消費者帳戶）共用 AWS Managed Microsoft AD 目錄 AWS 帳戶（目錄帳戶擁有者）。如需為共用 AWS Managed Microsoft AD 設定聯網環境的步驟，請參閱下列程序。

先決條件

在開始執行此教學課程中的步驟之前，您必須具備以下內容：

- 在同一區域中建立兩個新的 AWS 帳戶 以供測試之用。當您建立 時 AWS 帳戶，它會自動在每個帳戶中建立專用虛擬私有雲端 (VPC)。記下每個帳戶內的 VPC ID。後續操作將會用到這份資料。
- 建立 AWS Managed Microsoft AD。
- 建立 VPC 互連連線時，目錄帳戶擁有者和目錄消費者帳戶都需要必要的許可，才能建立和接受互連連線。如需詳細資訊，請參閱範例：建立 VPC 互連連線和範例：接受 VPC 互連連線。

> **Note**
>
> 雖然有許多方式可以連線到目錄擁有者和目錄消費者帳戶 VPC，但本教學將會使用 VPC 對等互連方法。其他額外的 VPC 連線能力選項，請參閱 網路連線能力。

在目錄擁有者和目錄消費者帳戶之間，設定 VPC 對等互連

您將建立的 VPC 對等連線，存在於目錄消費者和目錄擁有者 VPC 之間，依照以下步驟，設定 VPC 對等連線來與目錄消費者帳戶連線。使用此連線，您可以在兩個 VPC 之間使用私有 IP 地址來路由流量。

在目錄擁有者和目錄消費者帳戶之間，建立 VPC 對等連線

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。請務必以具有目錄擁有者帳戶中管理員登入資料的使用者身分登入，並具有建立 VPC 互連連線所需的許可。如需詳細資訊，請參閱先決條件。
2. 在導覽窗格中，選擇 Peering Connections (對等互連連線)。接著，選擇 Create Peering Connection (建立對等連線)。
3. 設定下列資訊：
   - 對等連線名稱標籤：提供可清楚定義與目錄消費者帳戶內 VPC 之間連線的名稱。
   - VPC (申請者)：選取目錄擁有者帳戶的 VPC ID。

- 在 Select another VPC to peer with (選取其他要對等連線的 VPC) 之下，確定 My account (我的帳戶) 及 This region (這個區域) 均已選取。
- VPC (接受者)：選取目錄消費者帳戶的 VPC ID。

4. 關閉 Create Peering Connection (建立對等連線)。在確認對話方塊中，選擇 OK (確定)。

代表目錄消費者帳戶接受對等請求

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。請務必以具有必要許可的使用者身分登入，以接受對等請求。如需詳細資訊，請參閱先決條件。
2. 在導覽窗格中，選擇 Peering Connections (對等互連連線)。
3. 選取正在等待的 VPC 對等連線。(其狀態為正在等待接受。) 選擇 Actions (動作)、Accept Request (接受請求)。
4. 在確認對話方塊中，選擇 Yes, Accept (是，接受)。在接下來的確認對話方塊中，選擇 Modify my route tables now (現在修改我的路由表)，直接前往路由表頁面。

現在您的 VPC 對等連線已處於作用中，您必須將項目新增至目錄擁有者帳戶中 VPC 的路由表。這樣可讓流量直接導向目錄消費者帳戶內的 VPC。

新增項目到目錄擁有者帳戶的 VPC 路由表中

1. 在 Amazon VPC 主控台的路由表區段中，選取目錄擁有者 VPC 的路由表。
2. 選擇路由索引標籤，選擇編輯路由，然後選擇新增路由。
3. 在 Destination (目的地) 欄位中，輸入目錄消費者 VPC 的 CIDR 區塊。
4. 在 Target (目標) 欄位中，為您之前在目錄擁有者帳戶中建立的對等連線，輸入 VPC 對等連線 ID (例如，**pcx-123456789abcde000**)。
5. 選擇儲存變更。

新增項目到目錄消費者帳戶的 VPC 路由表中

1. 在 Amazon VPC 主控台的路由表區段中，選取目錄消費者 VPC 的路由表。
2. 選擇路由索引標籤，選擇編輯路由，然後選擇新增路由。
3. 在 Destination (目的地) 欄位中，輸入目錄擁有者 VPC 的 CIDR 區塊。
4. 在 Target (目標) 欄位中，為您之前在目錄消費者帳戶中建立的對等連線，鍵入 VPC 對等連線 ID (例如，**pcx-123456789abcde001**)。

5. 選擇儲存變更。

將 Active Directory 通訊協定和連接埠新增至目錄取用者 VPCs 中安全群組的傳出規則。如需詳細資訊，請參閱 VPC 安全群組及 AWS Managed Microsoft AD 先決條件。

後續步驟

步驟 2：共享您的目錄

步驟 2：共享您的目錄

使用以下程序，從目錄擁有者帳戶中展開目錄共享工作流程。

> **Note**
>
> 目錄共用是 AWS Managed Microsoft AD 的區域功能。如果您使用的是多區域複寫，則必須在每個區域中分別套用下列程序。如需詳細資訊，請參閱全域與區域功能。

從目錄擁有者帳戶共享目錄

1. AWS Management Console 使用目錄擁有者帳戶中的管理員登入資料登入 ，然後開啟位於 https：//https://console.aws.amazon.com/directoryservicev2/ 的 AWS Directory Service 主控台。
2. 在導覽窗格中，選擇目錄。
3. 選擇您要共用之 AWS Managed Microsoft AD 目錄的目錄 ID。
4. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要共享目錄的區域，然後選擇擴展和共享索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇擴展和共享索引標籤。
5. 在 Shared directories (共享的目錄) 區段中，選擇 Actions (動作)，然後選擇 Create new shared directory (新建共享目錄)。
6. 在選擇要 AWS 帳戶 共用的頁面上，根據您的業務需求選擇下列其中一種共用方法：
   a. 與組織 AWS 帳戶 內部共用此目錄 – 使用此選項，您可以從顯示 AWS 組織 AWS 帳戶 內部所有 的清單中選取要 AWS 帳戶 共用目錄的 。您必須先啟用與 的受信任存取， AWS Directory Service 才能共用目錄。如需詳細資訊，請參閱如何啟用或停用信任的存取。

> **Note**
>
> 若要使用此選項，您的組織必須先啟用所有功能，而且您的目錄必須在組織管理帳戶之中。

i. AWS 帳戶 在組織中的 下，選取要與 AWS 帳戶 之共用目錄的 ，然後按一下新增。
ii. 檢閱定價詳細資訊，然後選擇 Share (共享)。
iii. 繼續執行本指南的步驟 4。由於所有 AWS 帳戶 都在同一個組織中，因此您不需要遵循步驟 3。

b. 與其他 共用此目錄 AWS 帳戶 - 使用此選項，您可以與 AWS 組織內外的帳戶共用目錄。當您的目錄不是 AWS 組織的成員，而且您想要與另一個組織共用時，您也可以使用此選項 AWS 帳戶。

i. 在 AWS 帳戶 ID 中，輸入您要共享目錄的所有 AWS 帳戶 ID，並接著按一下新增。
ii. 在傳送注意事項中，鍵入要給其他 AWS 帳戶之管理員的訊息。
iii. 檢閱定價詳細資訊，然後選擇 Share (共享)。
iv. 繼續進行步驟 3。

後續步驟

步驟 3：接受共用目錄邀請 - 選用

步驟 3：接受共用目錄邀請 - 選用

如果您在先前程序中選擇了與其他 AWS 帳戶共享此目錄 (交握方法) 選項，則您應該使用此程序來完成共享目錄工作流程。如果您選擇在組織 AWS 帳戶 內部與 共用此目錄選項，請略過此步驟並繼續步驟 4。

接受共享目錄邀請

1. AWS Management Console 使用目錄消費者帳戶中的管理員登入資料登入 ，然後開啟位於 https：//https://console.aws.amazon.com/directoryservicev2/ 的 AWS Directory Service 主控台。
2. 在導覽窗格中，選擇 Directories shared with me (與我共享目錄)。
3. 在 Shared directory ID (共享目錄 ID) 欄位中，選擇狀態 Pending acceptance (正在等待接受) 的目錄 ID。

4. 在 Shared directory details (共享目錄詳細資訊) 頁面上，選擇 Review (檢閱)。
5. 在 Pending shared directory invitation (等待共享目錄邀請) 對話方塊中，檢閱注意事項、目錄擁有者詳細資訊，以及關於定價的資訊。在您同意情況下，選擇 Accept (接受) 即可開始使用目錄。

後續步驟

步驟 4：測試將適用於 Windows Server 的 EC2 執行個體無縫加入域

步驟 4：測試將適用於 Windows Server 的 EC2 執行個體無縫加入域

您可以使用以下兩種方法來測試將 EC2 執行個體無縫加入域。

方法 1：使用 Amazon EC2 主控台測試加入域

在目錄消費者帳戶中執行這些步驟。

1. 登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/ec2/ 的 Amazon EC2 主控台。
2. 在導覽列中，選擇 AWS 區域 與現有目錄相同的 。
3. 在 EC2 儀表板的啟動執行個體區段中，選擇啟動執行個體。
4. 在啟動執行個體頁面上的名稱和標籤區段下，輸入您想要用於 Windows EC2 執行個體的名稱。
5. (選用) 針對新增標籤，新增一個或多個標籤鍵值對來組織、追蹤或控制對此 EC2 執行個體的存取。
6. 在應用程式和作業系統映像 (Amazon Machine Image) 區段中，選擇快速啟動窗格中的 Windows。您可以從 Amazon Machine Image (AMI)下拉式清單中變更 Windows Amazon Machine Image (AMI)。
7. 在執行個體類型區段中，從執行個體類型下拉式清單中選擇您要使用的執行個體類型。
8. 在金鑰對 (登入) 區段中，您可以選擇建立新金鑰對或從現有金鑰對中進行選擇。
    a. 若要建立新的金鑰對，請選擇建立新金鑰對。
    b. 輸入金鑰對的名稱，然後選取金鑰對類型和私有金鑰檔案格式的選項。
    c. 若要將私有金鑰儲存為可與 OpenSSH 搭配使用的格式，請選擇 .pem。若要將私有金鑰儲存為可與 PuTTY 搭配使用的格式，請選擇 .ppk。
    d. 選擇建立金鑰對。
    e. 您的瀏覽器會自動下載私有金鑰檔案。將私有金鑰檔案存放在安全的地方。

> **Important**
>
> 這是您儲存私有金鑰檔案的唯一機會。

9. 在啟動執行個體頁面上的網路設定區段下，選擇編輯。從 VPC – required 下拉式清單中選擇在其中建立目錄的 VPC。
10. 從子網路下拉式清單中選擇 VPC 中的公有子網路之一。您所選取的子網路必須將所有外部流量路由到網際網路閘道。如果沒有，則將無法從遠端連線到執行個體。

    如需有關連線至網際網路閘道的詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用網際網路閘道連線至網際網路一節。
11. 在自動指派公有 IP 下，選擇啟用。

    如需公有和私有 IP 定址的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 執行個體 IP 定址。 Amazon EC2
12. 對於防火牆 (安全群組)設定，您可以使用預設設定或根據需要進行變更。
13. 對於設定儲存設定，您可以使用預設設定或根據需要進行變更。
14. 選取進階詳細資訊區段，從域加入目錄下拉式清單中選取域。

> **Note**
>
> 選擇網域加入目錄後，您可能會看到：
>
> 如果 EC2 啟動精靈識別具有非預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
>
> - 如果您先前已編輯 SSM 文件，且預期屬性，請選擇關閉並繼續啟動 EC2 執行個體，而不進行任何變更。
> - 選取此處的刪除現有 SSM 文件連結，以刪除 SSM 文件。這將允許建立具有正確屬性的 SSM 文件。當您啟動 EC2 執行個體時，系統會自動建立 SSM 文件。

15. 對於 IAM 執行個體設定檔，您可以選取現有的 IAM 執行個體設定檔或建立新的設定檔。從 IAM 執行個體設定檔下拉式清單中選取具有 AWS AmazonSSMManagedInstanceCore 和 AmazonSSMDirectoryServiceAccess 受管政策的 IAM 執行個體設定檔。若要建立新的 IAM 設定檔連結，請選擇建立新的 IAM 設定檔連結，然後執行下列動作：

    1. 選擇建立角色。

2. 在選取信任的實體下，選取 AWS 服務。
3. 在 Use case (使用案例) 下，選擇 EC2。
4. 在新增許可下的政策清單中，選取 AmazonSSMManagedInstanceCore 和 AmazonSSMDirectoryServiceAccess 政策。在搜尋方塊中，輸入 **SSM** 以篩選政策。選擇下一步。

> **Note**
>
> AmazonSSMDirectoryServiceAccess 提供將執行個體加入 Active Directory受管 的許可 AWS Directory Service。AmazonSSMManagedInstanceCore 提供使用 AWS Systems Manager 服務所需的最低許可。有關建立具有這些許可的角色的更多資訊，以及有關可以指派給 IAM 角色的其他許可和政策的資訊，請參閱《AWS Systems Manager 使用者指南》中的為 Systems Manager 建立 IAM 執行個體設定檔一節。

5. 在命名、檢閱和建立頁面上，針對角色名稱輸入角色名稱。您將需要此角色名稱來連接到 EC2 執行個體。
6. (選用) 您可以在描述欄位中提供 IAM 執行個體設定檔的描述。
7. 選擇建立角色。
8. 返回啟動執行個體頁面，然後選擇 IAM 執行個體設定檔旁的重新整理圖示。剛剛建立的 IAM 執行個體設定檔應顯示在 IAM 執行個體設定檔下拉式清單中。選擇這個新的設定檔並將其餘設定保留為預設值。

16. 選擇啟動執行個體。

方法 2：使用 AWS Systems Manager測試加入域

在目錄消費者帳戶中執行這些步驟。若要完成此程序，您需要目錄擁有者帳戶的一些相關資訊，例如目錄 ID、目錄名稱和 DNS IP 地址。

先決條件

- 設定 AWS Systems Manager。
  - 如需有關 Systems Manager 的詳細資訊，請參閱AWS Systems Manager的一般設定。
- 您想要加入 AWS 受管 Microsoft Active Directory 網域的執行個體必須具有連接的 IAM 角色，其中包含 AmazonSSMManagedInstanceCore 和 AmazonSSMDirectoryServiceAccess 受管政策。

- 如需您可以連接至 Systems Manager IAM 執行個體設定檔的這些受管政策和其他政策的詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的建立 Systems Manager 的 IAM 執行個體設定檔。如需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。

如需使用 Systems Manager 將 EC2 執行個體加入 AWS 受管 Microsoft Active Directory 網域的詳細資訊，請參閱如何使用 AWS Systems Manager 將執行中的 EC2 Windows 執行個體加入我的 AWS Directory Service 網域？。

1. 在 開啟 AWS Systems Manager 主控台https://console.aws.amazon.com/systems-manager/。
2. 在導覽窗格中，於節點管理下方，選擇執行命令。
3. 選擇執行命令。
4. 在執行指令頁面上，搜尋 `AWS-JoinDirectoryServiceDomain`。顯示在搜尋結果時選擇 `AWS-JoinDirectoryServiceDomain` 選項。
5. 向下捲動到 Command parameters (命令參數) 區段。您必須提供下列參數給：

   > **Note**
   >
   > 您可以返回 AWS Directory Service 主控台，選取與我共用的目錄，然後選取您的目錄，以尋找目錄 ID、目錄名稱和 DNS IP 地址。目錄 ID 可以在共享目錄詳細資訊區段下找到。您可以在擁有者目錄詳細資訊區段下找到目錄名稱和 DNS IP 地址的值。

   - 針對目錄 ID，輸入 AWS Managed Microsoft Active Directory 的名稱。
   - 針對目錄名稱，輸入 AWS Managed Microsoft Active Directory 名稱 (適用於目錄擁有者帳戶)。
   - 針對 DNS IP 地址，在 AWS Managed Microsoft Active Directory （適用於目錄擁有者帳戶）中輸入 DNS 伺服器的 IP 地址。
6. 對於目標，選擇手動選擇執行個體，然後選取要加入域的執行個體。
7. 將表單其餘部分保留預設值，向下捲動頁面，然後選擇 Run (執行)。
8. 執行個體成功加入域後，指令狀態將從待定 變更為成功。您可以透過選取加入域的執行個體的執行個體 ID，然後選擇檢視輸出來檢視指令輸出。

完成上述任一步驟後，您現在應該可以加入您的 EC2 執行個體至網域。完成後，您可以使用遠端桌面通訊協定 (RDP) 用戶端搭配 AWS Managed Microsoft AD 使用者帳戶的登入資料來登入執行個體。

取消共用您的目錄

使用下列程序來取消共用 AWS Managed Microsoft AD 目錄。

取消目錄的共用

1. 在 AWS Directory Service 主控台導覽窗格中的 Active Directory 下，選取目錄。
2. 選擇您要取消共用之 AWS Managed Microsoft AD 目錄的目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取要取消共用目錄的區域，然後選擇擴展和共享索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇擴展和共享索引標籤。
4. 在 Shared directories (已共用目錄) 區段中，選取您要取消共用的已共用目錄，選擇 Actions (動作)，然後選擇 Unshare (取消共用)。
5. 在 Unshare directory (取消目錄的共用) 對話方塊中，選擇 Unshare (取消共用)。

其他資源

- 使用案例：共用您的目錄，將 amazon EC2 執行個體順暢地跨 AWS 帳戶加入網域
- AWS 安全部落格文章：如何將 Amazon EC2 執行個體從多個帳戶和 VPCs 加入單一 AWS Managed Microsoft AD 目錄
- 在多個帳戶之間將 Amazon RDS 資料庫執行個體加入單一共用域

將 Active Directory 使用者遷移至 AWS Managed Microsoft AD

您可以使用 Active Directory Migration Toolkit (ADMT) 搭配密碼匯出服務 (PES)，將使用者從自我管理遷移Active Directory至 AWS Managed Microsoft AD 目錄。這可讓您更輕鬆地遷移使用者的Active Directory物件和加密密碼。

如需詳細說明，請參閱 AWS 安全部落格上的如何使用 ADMT 將內部部署網域遷移至 AWS Managed Microsoft AD。

將 AWS Managed Microsoft AD 連接至現有的 Active Directory 基礎設施

本節說明如何設定 AWS Managed Microsoft AD 與現有Active Directory基礎設施之間的信任關係。

將 AWS Managed Microsoft AD 連接至現有 的任務Active Directory：

- 在 AWS Managed Microsoft AD 和自我管理 AD 之間建立信任關係
- 搭配 AWS Managed Microsoft AD 使用公有 IP 地址時新增 IP 路由
- 教學：在 AWS Managed Microsoft AD 和自我管理的 Active Directory 域之間建立信任關係
- 教學：在兩個 AWS Managed Microsoft AD 域之間建立信任關係

在 AWS Managed Microsoft AD 和自我管理 AD 之間建立信任關係

您可以在 AWS Directory Service for Microsoft Active Directory 和自我管理 （內部部署） 目錄之間，以及在 AWS 雲端的多個 AWS Managed Microsoft AD 目錄之間設定單向和雙向外部和樹系信任關係。 AWS 受管 Microsoft AD 支援這三種信任關係方向：傳入、傳出和雙向 （雙向）。

如需信任關係的詳細資訊，請參閱有關 AWS Managed Microsoft AD 信任的所有須知。

> **Note**
>
> 設定信任關係時，您必須確保您的自我管理目錄與 相容 AWS Directory Service。如需您責任的詳細資訊，請參閱我們的「共同的責任模型」。

AWS Managed Microsoft AD 同時支援外部和樹系信任。如需帶您演練如何建立樹系信任的示範案例，請參閱教學：在 AWS Managed Microsoft AD 和自我管理的 Active Directory 域之間建立信任關係。

Amazon Chime、Amazon Connect、QuickSight、 AWS IAM Identity Center、WorkDocs、Amazon WorkMail、Amazon WorkSpaces 和 等 AWS 企業應用程式需要雙向信任 AWS Management Console。 AWS 受管 Microsoft AD 必須能夠查詢自我管理 中的使用者和群組Active Directory。

您可以啟用選擇性身分驗證，以便只有 AWS 應用程式特定的服務帳戶可以查詢您的自我管理 Active Directory。如需詳細資訊，請參閱增強 AWS 應用程式與 AWS Managed Microsoft AD 整合的安全性。

Amazon EC2、Amazon RDS 和 Amazon FSx 將使用單向或雙向信任。

先決條件

建立信任只需要幾個步驟，但您必須先完成幾個必要步驟，才能設定信任。

> **Note**
>
> AWS Managed Microsoft AD 不支援與單一標籤網域的信任。

連線到 VPC

如果您要建立與自我管理目錄的信任關係，您必須先將自我管理網路連線到包含 AWS Managed Microsoft AD 的 Amazon VPC。自我管理網路和 AWS Managed Microsoft AD 網路的防火牆必須開啟Microsoft文件中 Windows Server 2008 和更新版本中列出的網路連接埠。

若要使用 NetBIOS 名稱而非完整網域名稱，搭配 Amazon WorkDocs 或 Amazon QuickSight 等 AWS 應用程式進行身分驗證，您必須允許連接埠 9389。如需 Active Directory 連接埠和通訊協定的詳細資訊，請參閱 Microsoft 文件中的 的服務概觀和網路連接埠需求Windows。

您至少需要這些連接埠，才可連線到您的目錄。您特定的組態可能需要開啟其他連接埠。

設定您的 VPC

包含 AWS Managed Microsoft AD 的 VPC 必須具有適當的傳出和傳入規則。

設定您的 VPC 輸出規則

1. 在 AWS Directory Service 主控台的目錄詳細資訊頁面上，記下您的 AWS Managed Microsoft AD 目錄 ID。
2. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
3. 選擇 Security Groups (安全群組)。
4. 搜尋您的 AWS Managed Microsoft AD 目錄 ID。在搜尋結果中，選取描述為「為目錄 ID 目錄控制站AWS 建立安全群組」的項目。

   > **Note**
   >
   > 選取的安全群組是您一開始建立目錄時自動建立的安全群組。

5. 前往該安全群組的 Outbound Rules (輸出規則) 標籤。依序選取 Edit (編輯) 和 Add another rule (新增其他規則)。針對新的規則，輸入下列值：

- Type (類型)：所有流量
- Protocol (協定)：全部
- 目標能決定可傳出您域控制站的流量及該流量可傳入您自我管理網路的目標。請指定單一 IP 地址，或是以 CIDR 表示法表示的 IP 地址範圍 (例如 203.0.113.5/32)。您也可以指定位在相同區域的另一個安全群組的名稱或 ID。如需詳細資訊，請參閱了解目錄 AWS 的安全群組組態和使用。

6. 選取 Save (儲存)。

啟用 Kerberos 預先身分驗證

您的使用者帳戶必須啟用 Kerberos 預先驗證。如需此設定的詳細資訊，請檢閱 Microsoft TechNet 上的 Preauthentication。

為您的自我管理域設定 DNS 條件式轉寄站

您必須在自我管理域上設定 DNS 條件式轉寄站。如需條件式轉寄站的詳細資訊，請參閱 Microsoft TechNet 上的 Assign a Conditional Forwarder for a Domain Name。

若要執行下列步驟，您必須具備自我管理域的下列 Windows Server 工具存取權：

- AD DS 及 AD LDS 工具
- DNS

在您的自我管理域上設定條件式轉寄站

1. 首先，您必須取得一些 Managed Microsoft AD AWS 的相關資訊。登入 AWS Management Console 並開啟 AWS Directory Service 主控台。
2. 在導覽窗格中，選取 Directories (目錄)。
3. 選擇 AWS Managed Microsoft AD 的目錄 ID。
4. 記下您目錄的完整網域名稱 (FQDN) 和 DNS 地址。
5. 現在，返回自我管理域控制站。開啟伺服器管理員。
6. 在工具選單上，選擇 DNS。
7. 在主控台樹狀目錄中，展開您要設定信任之網域的 DNS 伺服器。
8. 在主控台樹狀目錄中，選擇條件式轉寄站。

9. 在動作選單上，選擇新增條件式轉寄站。
10. 在 DNS 網域中，輸入您先前記下的 AWS Managed Microsoft AD 的完整網域名稱 (FQDN)。
11. 選擇主要伺服器的 IP 地址，然後輸入您稍早記下的 AWS Managed Microsoft AD 目錄的 DNS 地址。

    輸入 DNS 地址之後，您可能會收到「逾時」或「無法解析」錯誤。您通常可以忽略這些錯誤。
12. 選取 Store this conditional forwarder in Active Directory and replicate as follows: All DNS servers in this domain (在 Active Directory 中儲存此條件式轉寄站，並複寫如下：這個網域中的所有 DNS 伺服器)。選擇確定。

信任關係密碼

如果您想要建立與現有網域的信任關係，請使用 Windows Server 管理工具設定該網域上的信任關係。當您執行此作業時，請記下所使用的信任密碼。在 AWS Managed Microsoft AD 上設定信任關係時，您將需要使用此相同的密碼。如需詳細資訊，請參閱 Microsoft TechNet 上的 Managing Trusts。

您現在可以在 AWS Managed Microsoft AD 上建立信任關係。

NetBIOS 和域名稱

NetBIOS 和域名稱必須唯一且不能相同，才能建立信任關係。

建立、驗證或刪除信任關係

> **Note**
>
> 信任關係是 AWS Managed Microsoft AD 的全域功能。如果您使用 設定 AWS Managed Microsoft AD 的多區域複寫，則必須在 主要區域 中執行下列步驟。變更將自動套用至所有複寫區域。如需詳細資訊，請參閱全域與區域功能。

建立與 AWS Managed Microsoft AD 的信任關係

1. 開啟 AWS Directory Service 主控台。
2. 在目錄頁面上，選擇您的 AWS Managed Microsoft AD ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：

   - 如果多區域複寫下顯示多個區域，請選取主要區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。

- 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。

4. 在 Trust relationships (信任關係) 區段，選擇 Actions (動作)，然後選取 Add trust relationship (新增信任關係)。
5. 在 Add a trust relationship (新增信任關係) 頁面上提供所需的資訊，包括您信任類型、信任網域的完整網域名稱 (FQDN)、信任密碼和信任方向。
6. （選用）如果您想要僅允許授權使用者存取 AWS Managed Microsoft AD 目錄中的資源，您可以選擇選擇性身分驗證核取方塊。如需有關選擇性身分驗證的詳細資訊，請參閱 Microsoft TechNet 上的 Security Considerations for Trusts (信任的安全考量事項)。
7. 針對條件式轉寄站，輸入您自我管理 DNS 伺服器的 IP 地址。如果您先前已建立條件式轉寄站，您可以輸入自我管理域的 FQDN，而非 DNS 的 IP 地址。
8. (選用) 選擇新增另一個 IP 地址，然後輸入其他自我管理 DNS 伺服器的 IP 地址。您可以為每個適用的 DNS 伺服器地址 (共四個地址) 重複此步驟。
9. 選擇新增。
10. 如果您自我管理域的 DNS 伺服器或網路使用公有 (非 RFC 1918) IP 地址空間，請前往 IP 路由區段，選擇動作，然後選擇新增路由。使用 CIDR 格式輸入您 DNS 伺服器或自我管理網路的 IP 地址區塊，例如 203.0.113.0/24。如果您的 DNS 伺服器和自我管理網路都使用 RFC 1918 IP 地址空間，則不需要此步驟。

    > **Note**
    >
    > 使用公有 IP 地址空間時，請務必不要使用任何 AWS IP 地址範圍，因為這些範圍無法使用。

11. (選用) 我們建議您在 Add routes (新增路由) 頁面上時，同時選取 Add routes to the security group for this directory's VPC (將路由新增至此目錄 VPC 的安全群組)。這會設定安全群組，如上面的「設定您的 VPC」所詳述。這些安全規則會影響未公開的內部網路界面。如果這個選項無法使用，您會另外看到訊息，指出您已自訂安全群組。

您必須在這兩個網域上設定信任關係。這些關係必須是互補的。例如，如果您在一個網域上建立連出信任，則必須在另一個網域上建立連入信任。

如果您想要建立與現有網域的信任關係，請使用 Windows Server 管理工具設定該網域上的信任關係。

您可以在 AWS Managed Microsoft AD 和各種 Active Directory 網域之間建立多個信任。不過，每對一次只能存在一個信任關係。例如，如果您在「傳入方向」中有現有的單向信任，然後想要在「傳出方向」中設定另一個信任關係，您將需要刪除現有的信任關係，並建立新的「雙向」信任。

驗證連出信任關係

1. 開啟 AWS Directory Service 主控台。
2. 在目錄頁面上，選擇您的 AWS Managed Microsoft AD ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取主要區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
4. 在 Trust relationships (信任關係) 區段，選取您要驗證的信任，選擇 Actions (動作)，然後選取 Verify trust relationship (驗證信任關係)。

此程序只會驗證雙向信任的傳出方向。 AWS 不支援驗證傳入信任。如需如何驗證您自我管理 Active Directory 之連入或連出信任的詳細資訊，請參閱 Microsoft TechNet 上的 Verify a Trust 相關內容。

刪除現有的信任關係

1. 開啟 AWS Directory Service 主控台。
2. 在目錄頁面上，選擇您的 AWS Managed Microsoft AD ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取主要區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
4. 在 Trust relationships (信任關係) 區段，選取您要刪除的信任，選擇 Actions (動作)，然後選取 Delete trust relationship (刪除信任關係)。
5. 選擇刪除。

搭配 AWS Managed Microsoft AD 使用公有 IP 地址時新增 IP 路由

您可以使用適用於 Microsoft Active Directory 的 AWS Directory Service 來利用許多強大的Active Directory功能，包括與其他目錄建立信任。不過，如果其他目錄網路的 DNS 伺服器使用公有 (非 RFC 1918) IP 地址，則您必須在設定信任關係的過程中指定這些 IP 地址。如需執行此作業的說明，請參閱「在 AWS Managed Microsoft AD 和自我管理 AD 之間建立信任關係」。

同樣地，如果 VPC 使用公有 IP 範圍，則在將流量從 AWS Managed Microsoft AD 路由 AWS 到對等 AWS VPC 時，您也必須輸入 IP 地址資訊。

當您如「在 AWS Managed Microsoft AD 和自我管理 AD 之間建立信任關係」中所述新增 IP 地址時，您可以選取 Add routes to the security group for this directory's VPC (將路由新增至此目錄 VPC 的安全群組)。除非您之前已如下所示自訂安全群組來允許必要的流量，否則請務必選取此選項。如需詳細資訊，請參閱了解目錄 AWS 的安全群組組態和使用。

教學：在 AWS Managed Microsoft AD 和自我管理的 Active Directory 域之間建立信任關係

本教學課程會逐步解說設定 AWS Directory Service for Microsoft Active Directory 與自我管理 （內部部署） Microsoft 之間信任關係的所有必要步驟Active Directory。雖然建立信任只需要幾個步驟，但您必須先完成下列必要步驟。

主題

- 先決條件
- 步驟 1：準備您自我管理的 AD 域
- 步驟 2：準備您的 AWS Managed Microsoft AD
- 步驟 3：建立信任關係

另請參閱

在 AWS Managed Microsoft AD 和自我管理 AD 之間建立信任關係

先決條件

此教學假設您已具備下列項目：

> **Note**
>
> AWS Managed Microsoft AD 不支援對單一標籤網域的信任。

- 在 上建立的 AWS Managed Microsoft AD 目錄 AWS。如果您需要協助來執行此作業，請參閱「Managed AWS Microsoft AD 入門」。

- 執行 的 EC2 執行個體Windows已新增至該 AWS Managed Microsoft AD。如果您需要協助來執行此作業，請參閱「將 Amazon EC2 Windows 執行個體加入您的 AWS Managed Microsoft AD Active Directory」。

  > **Important**
  >
  > Managed AWS Microsoft AD 的管理員帳戶必須具有此執行個體的管理存取權。

- 該執行個體上安裝了下列Windows伺服器工具：
  - AD DS 及 AD LDS 工具
  - DNS

  如果您需要協助來執行此作業，請參閱「安裝 AWS Managed Microsoft AD 的 Active Directory 管理工具」。
- 自我管理 (內部部署) Microsoft Active Directory

  您必須具備此目錄的管理存取權。此目錄也必須提供上述相同的Windows伺服器工具。
- 自我管理網路與包含 AWS Managed Microsoft AD 的 VPC 之間的作用中連線。如果您需要協助來執行此作業，請參閱「Amazon Virtual Private Cloud 連線選項」。
- 已正確設定的本機安全政策。檢查 `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` 並確保其中包含至少下列三個具名管道：
  - netlogon
  - samr
  - lsarpc
- NetBIOS 和域名稱必須唯一且不能相同，才能建立信任關係

如需有關建立信任關係的先決條件的詳細資訊，請參閱 在 AWS Managed Microsoft AD 和自我管理 AD 之間建立信任關係。

教學組態

在本教學課程中，我們已建立 AWS Managed Microsoft AD 和自我管理網域。自我管理網路已連線至 AWS Managed Microsoft AD 的 VPC。以下是這兩個目錄的屬性：

AWS 在 上執行的受管 Microsoft AD AWS

- 網域名稱 (FQDN)：MyManagedAD.example.com
- NetBIOS 名稱：MyManagedAD
- DNS 地址：10.0.10.246、10.0.20.121
- VPC CIDR：10.0.0.0/16

AWS Managed Microsoft AD 位於 VPC ID：vpc-12345678。

自我管理或 AWS 受管 Microsoft AD 網域

- 網域名稱 (FQDN)：corp.example.com
- NetBIOS 名稱：CORP
- DNS 地址：172.16.10.153
- 自我管理 CIDR：172.16.0.0/16

後續步驟

步驟 1：準備您自我管理的 AD 域

步驟 1：準備您自我管理的 AD 域

首先，您必須在自我管理 (內部部署) 域上完成幾個必要步驟。

設定自我管理防火牆

您必須設定自我管理防火牆，以便將下列連接埠開放給包含 AWS Managed Microsoft AD 之 VPC 使用的所有子網路的 CIDRs。在本教學課程中，我們允許來自 10.0.0.0/16 (AWS 受管 Microsoft AD 的 VPC 的 CIDR 區塊) 的傳入和傳出流量位於下列連接埠：

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 身分驗證
- TCP/UDP 389 - 輕量型目錄存取通訊協定 (LDAP)
- TCP 445 - 伺服器訊息區塊 (SMB)
- TCP 9389 - Active Directory Web Services (ADWS) (選用 - 如果您想要使用 NetBIOS 名稱而非完整網域名稱來驗證 Amazon WorkDocs 或 Amazon QuickSight 等 AWS 應用程式，則需要開啟此連接埠。)

> **Note**
>
> 不再支援 SMBv1。
> 您至少需要這些連接埠，才可將 VPC 連線到自我管理目錄。您特定的組態可能需要開啟其他連接埠。

確定已啟用 Kerberos 預先驗證

這兩個目錄中的使用者帳戶必須已啟用 Kerberos 預先驗證。這是預設值，但請檢查隨機使用者的屬性以確定沒有任何變更。

檢視使用者的 Kerberos 設定

1. 在自我管理的域控制站上，開啟「伺服器管理員」。
2. 在 Tools (工具) 選單上，選擇 Active Directory Users and Computers (Active Directory 使用者和電腦)。
3. 選擇 Users (使用者) 資料夾，開啟內容功能表 (按一下滑鼠右鍵)。選擇適當窗格中所列的任何隨機使用者帳戶。選擇 Properties (屬性)。
4. 選擇 Account (帳戶) 標籤。在帳戶選項清單中，向下捲動並確定 未核取不需要 Kerberos 預先驗證。

為您的自我管理域設定 DNS 條件式轉寄站

您必須在每個網域上設定 DNS 條件式轉寄站。在自我管理網域上執行此操作之前，您會先取得一些 AWS Managed Microsoft AD 的相關資訊。

在您的自我管理域上設定條件式轉寄站

1. 登入 AWS Management Console 並開啟 AWS Directory Service 主控台。
2. 在導覽窗格中，選取 Directories (目錄)。
3. 選擇 AWS Managed Microsoft AD 的目錄 ID。
4. 在 Details (詳細資訊) 頁面，記錄目錄中的 Directory name (目錄名稱) 以及 DNS address (DNS 地址) 的數值。
5. 現在，返回自我管理域控制站。開啟伺服器管理員。
6. 在工具選單上，選擇 DNS。

7. 在主控台樹狀目錄中，展開您要設定信任之網域的 DNS 伺服器。我們的伺服器是 WIN-5V70CN7VJ0.corp.example.com。
8. 在主控台樹狀目錄中，選擇條件式轉寄站。
9. 在動作選單上，選擇新增條件式轉寄站。
10. 在 DNS 網域中，輸入您先前記下的 AWS Managed Microsoft AD 的完整網域名稱 (FQDN)。在此範例中，FQDN 是 MyManagedAD.example.com。
11. 選擇主要伺服器的 IP 地址，然後輸入您稍早記下的 AWS Managed Microsoft AD 目錄的 DNS 地址。在此範例中為 10.0.10.246、10.0.20.121

    輸入 DNS 地址之後，您可能會收到「逾時」或「無法解析」錯誤。您通常可以忽略這些錯誤。

12. 選取在 Active Directory 中儲存此條件式轉寄站，並複寫如下。
13. 選取這個網域中的所有 DNS 伺服器，然後選擇確定。

後續步驟

步驟 2：準備您的 AWS Managed Microsoft AD

步驟 2：準備您的 AWS Managed Microsoft AD

現在，讓我們讓您的 AWS Managed Microsoft AD 準備好建立信任關係。下列許多步驟幾乎都與您剛剛在自我管理域方面完成的步驟相同。不過，這次您正在使用 AWS Managed Microsoft AD。

設定您的 VPC 子網路和安全群組

您必須允許從自我管理網路到包含 AWS Managed Microsoft AD 的 VPC 的流量。若要這樣做，您需要確保與用來部署 AWS Managed Microsoft AD 的子網路相關聯的 ACLs 和網域控制站上設定的安全群組規則，都允許必要的流量支援信任。

連接埠要求取決於您網域控制器所使用的 Windows Server 以及使用信任的服務或應用程式。在此教學課程中，您需開啟以下連接埠：

傳入

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 身分驗證
- UDP 123 - NTP
- TCP 135 - RPC

- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB
- TCP/UDP 464 - Kerberos 身分驗證
- TCP 636 - LDAPS (透過 TLS/SSL 的 LDAP)
- TCP 3268-3269 - 通用類別
- TCP/UDP 49152-65535 - RPC 暫時性連接埠

> **Note**
>
> 不再支援 SMBv1。

傳出

- ALL

> **Note**
>
> 您至少需要這些連接埠，才可連線 VPC 和自我管理目錄。您特定的組態可能需要開啟其他連接埠。

設定 AWS Managed Microsoft AD 網域控制器傳出和傳入規則

1. 返回 AWS Directory Service 主控台。在目錄清單中，記下 AWS Managed Microsoft AD 目錄的目錄 ID。
2. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
3. 在導覽窗格中，選擇 Security Groups (安全群組)。
4. 使用搜尋方塊來搜尋 AWS Managed Microsoft AD 目錄 ID。在搜尋結果中，選取描述為 的安全群組**`AWS created security group for yourdirectoryID directory controllers`**。
5. 前往該安全群組的 Outbound Rules (傳出規則) 標籤。選擇編輯規則，然後選擇新增規則。針對新的規則，輸入下列值：
   - Type (類型)：所有流量

- Protocol (協定)：全部
- Destination (目標) 能決定可傳出您網域控制器的流量及該流量傳入的目標。請指定單一 IP 地址，或是以 CIDR 表示法表示的 IP 地址範圍 (例如 203.0.113.5/32)。您也可以指定位在相同區域的另一個安全群組的名稱或 ID。如需詳細資訊，請參閱了解目錄 AWS 的安全群組組態和使用。

6. 選取儲存規則。

確定已啟用 Kerberos 預先驗證

現在，您想要確認 AWS Managed Microsoft AD 中的使用者也已啟用 Kerberos 預先驗證。這與您在自我管理目錄方面完成的程序相同。這是預設值，但請檢查以確定沒有任何變更。

檢視使用者的 Kerberos 設定

1. 使用AWS Managed Microsoft AD Administrator 帳戶和群組許可網域的 或已委派管理網域中使用者許可的帳戶，登入屬於 AWS Managed Microsoft AD 目錄成員的執行個體。
2. 如果尚未安裝，請安裝 Active Directory 使用者和電腦工具及 DNS 工具。若要了解如何安裝這些工具，請參閱安裝 AWS Managed Microsoft AD 的 Active Directory 管理工具。
3. 開啟伺服器管理員。在 Tools (工具) 選單上，選擇 Active Directory Users and Computers (Active Directory 使用者和電腦)。
4. 選擇您網域中的 Users (使用者) 資料夾。請注意，這是在您的 NetBIOS 名稱下的 Users (使用者) 資料夾，而不是在完全合格的網域名稱 (FQDN) 下的 Users (使用者) 資料夾。

5. 使用者清單中，請按一下滑鼠右鍵，選擇 Properties (屬性)。
6. 選擇 Account (帳戶) 標籤。在 Account options (帳戶選項) 清單中，確認 Do not require Kerberos preauthentication (不需要 Kerberos 預先驗證) 未核取。

後續步驟

步驟 3：建立信任關係

步驟 3：建立信任關係

既然準備工作已完成，最後步驟便要建立信任。首先，您在自我管理網域上建立信任，最後在 AWS Managed Microsoft AD 上建立信任。如果您在信任建立程序期間發生任何問題，請參閱「信任建立狀態原因」以取得協助。

在您的自我管理 Active Directory 設定信任

在此教學課程中，您會設定雙向樹系信任。但是如果您建立單向樹系信任，請注意您每個網域的信任方向都必須互相配合。例如，如果您在自我管理網域上建立單向傳出信任，則需要在 AWS Managed Microsoft AD 上建立單向傳入信任。

> **Note**
>
> AWS Managed Microsoft AD 也支援外部信任。但在此教學課程中，您將建立一個雙向樹系信任。

在自我管理 Active Directory 中設定信任

1. 開啟 Server Manager (伺服器管理員)，然後在 Tools (工具) 選單上，選擇 Active Directory Domains and Trusts (Active Directory 網域和信任)。
2. 開啟您網域的內容 (按一下滑鼠右鍵) 選單，然後選擇 Properties (屬性)。
3. 選擇 Trusts (信任) 標籤，再選擇 New trust (新增信任)。輸入 AWS Managed Microsoft AD 的名稱，然後選擇下一步。
4. 選擇 Forest trust (森林信任)。選擇 Next (下一步)。
5. 選擇 Two-way (雙向)。選擇 Next (下一步)。
6. 選擇 This domain only (僅限此網域)。選擇 Next (下一步)。
7. 選擇 Forest-wide authentication (全森林身分驗證)。選擇 Next (下一步)。
8. 輸入 Trust password (信任密碼)。請務必記住此密碼，因為在設定 AWS Managed Microsoft AD 的信任時，您需要此密碼。
9. 在下一個對話方塊中，確認您的設定，然後選擇 Next (下一步)。確認信任已成功建立，並再次選擇 Next (下一步)。
10. 選擇 No, do not confirm the outgoing trust (否，不要確認傳出信任)。選擇 Next (下一步)。
11. 選擇 No, do not confirm the incoming trust (否，不要確認傳入信任)。選擇 Next (下一步)。

在 AWS Managed Microsoft AD 目錄中設定信任

最後，您可以設定與 AWS Managed Microsoft AD 目錄的樹系信任關係。由於您在自我管理網域上建立雙向樹系信任，因此您也可以使用 AWS Managed Microsoft AD 目錄建立雙向信任。

> **Note**
>
> 信任關係是 AWS Managed Microsoft AD 的全域功能。如果您使用 設定 AWS Managed Microsoft AD 的多區域複寫，則必須在 主要區域 中執行下列步驟。變更將自動套用至所有複寫區域。如需詳細資訊，請參閱全域與區域功能。

在 AWS Managed Microsoft AD 目錄中設定信任

1. 返回 AWS Directory Service 主控台。
2. 在目錄頁面上，選擇您的 AWS Managed Microsoft AD ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取主要區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
4. 在 Trust relationships (信任關係) 區段，選擇 Actions (動作)，然後選取 Add trust relationship (新增信任關係)。
5. 在新增信任關係頁面上，指定信任類型。在此例中，我們選擇林信任。鍵入自我管理域的 FQDN (在本教學中為 **`corp.example.com`**)。輸入您在建立自我管理域之信任時使用的同一組信任密碼。指定方向。在此例中，我們選擇雙向。
6. 在條件式轉寄站欄位中，輸入您自我管理 DNS 伺服器的 IP 地址。在此範例中，請輸入 172.16.10.153。
7. (選用) 選擇新增另一個 IP 地址，然後輸入您自我管理 DNS 伺服器的第二個 IP 地址。您最多總共可以指定四個 DNS 伺服器。
8. 選擇新增。

恭喜您。您現在在自我管理網域 (corp.example.com) 與 AWS Managed Microsoft AD (MyManagedAD.example.com). 這兩個網域之間只可設定一項關係。例如，如果您想要將信任方向變更為單向，您需要先刪除這項現有關係，再建立新的關係。

如需詳細資訊，包括驗證或刪除信任的相關說明，請參閱 在 AWS Managed Microsoft AD 和自我管理 AD 之間建立信任關係。

教學：在兩個 AWS Managed Microsoft AD 域之間建立信任關係

本教學課程會逐步解說設定兩個 AWS Directory Service for Microsoft Active Directory 網域之間的信任關係所需的所有步驟。

主題

- 步驟 1：準備您的 AWS Managed Microsoft AD
- 步驟 2：建立與其他 AWS Managed Microsoft AD 網域的信任關係

另請參閱

在 AWS Managed Microsoft AD 和自我管理 AD 之間建立信任關係

步驟 1：準備您的 AWS Managed Microsoft AD

在本節中，您會讓 AWS Managed Microsoft AD 準備好與另一個 AWS Managed Microsoft AD 建立信任關係。下列許多步驟幾乎都與您在 教學：在 AWS Managed Microsoft AD 和自我管理的 Active Directory 域之間建立信任關係 中完成的步驟相同。不過，這次您要將 AWS Managed Microsoft AD 環境設定為彼此搭配使用。

設定您的 VPC 子網路和安全群組

您必須允許流量從一個 AWS Managed Microsoft AD 網路流向包含其他 AWS Managed Microsoft AD 的 VPC。若要這樣做，您需要確保與用來部署 AWS Managed Microsoft AD 的子網路相關聯的 ACLs 和網域控制站上設定的安全群組規則，都允許必要的流量支援信任。

連接埠要求取決於您網域控制器所使用的 Windows Server 以及使用信任的服務或應用程式。在此教學課程中，您需開啟以下連接埠：

傳入

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 身分驗證
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB

> **Note**
>
> 不再支援 SMBv1。

- TCP/UDP 464 - Kerberos 身分驗證
- TCP 636 - LDAPS (透過 TLS/SSL 的 LDAP)
- TCP 3268-3269 - 通用類別
- TCP/UDP 1024-65535 - RPC 暫時性連接埠

傳出

- ALL

> **Note**
>
> 這些是能夠從兩個 AWS Managed Microsoft AD 連線至相應的不同 VPC 所需的最少連接埠。您特定的組態可能需要開啟其他連接埠。如需詳細資訊，請參閱 Microsoft 網站上的如何設定 Active Directory 域及信任的防火牆一文。

設定 AWS Managed Microsoft AD 網域控制器傳出規則

> **Note**
>
> 對每個目錄重複下面的步驟 1-6。

1. 前往 AWS Directory Service 主控台。在目錄清單中，記下 AWS Managed Microsoft AD 目錄的目錄 ID。
2. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
3. 在導覽窗格中，選擇 Security Groups (安全群組)。
4. 使用搜尋方塊來搜尋 AWS Managed Microsoft AD 目錄 ID。在搜尋結果中，選取描述為 的項目**`AWS created security group for yourdirectoryID directory controllers`**。

5. 前往該安全群組的 Outbound Rules (傳出規則) 標籤。選擇 Edit (編輯) 和 Add another rule (新增其他規則)。針對新的規則，輸入下列值：
   - Type (類型)：所有流量
   - Protocol (協定)：全部
   - Destination (目標) 能決定可傳出您網域控制器的流量及該流量傳入的目標。請指定單一 IP 地址，或是以 CIDR 表示法表示的 IP 地址範圍 (例如 203.0.113.5/32)。您也可以指定位在相同區域的另一個安全群組的名稱或 ID。如需詳細資訊，請參閱了解目錄 AWS 的安全群組組態和使用。
6. 選取 Save (儲存)。

確定已啟用 Kerberos 預先驗證

現在，您想要確認 AWS Managed Microsoft AD 中的使用者也已啟用 Kerberos 預先驗證。這與您在內部部署目錄方面完成的程序相同。這是預設值，但請檢查以確定沒有任何變更。

檢視使用者的 Kerberos 設定

1. 使用AWS Managed Microsoft AD Administrator 帳戶和群組許可網域的 或已委派管理網域中使用者許可的帳戶，登入屬於 AWS Managed Microsoft AD 目錄成員的執行個體。
2. 如果尚未安裝，請安裝 Active Directory 使用者和電腦工具及 DNS 工具。若要了解如何安裝這些工具，請參閱安裝 AWS Managed Microsoft AD 的 Active Directory 管理工具。
3. 開啟伺服器管理員。在 Tools (工具) 選單上，選擇 Active Directory Users and Computers (Active Directory 使用者和電腦)。
4. 選擇您網域中的 Users (使用者) 資料夾。請注意，這是在您的 NetBIOS 名稱下的 Users (使用者) 資料夾，而不是在完全合格的網域名稱 (FQDN) 下的 Users (使用者) 資料夾。
5. 使用者清單中，請按一下滑鼠右鍵，選擇 Properties (屬性)。
6. 選擇 Account (帳戶) 標籤。在 Account options (帳戶選項) 清單中，確認 Do not require Kerberos preauthentication (不需要 Kerberos 預先驗證) 未核取。

後續步驟

步驟 2：建立與其他 AWS Managed Microsoft AD 網域的信任關係

步驟 2：建立與其他 AWS Managed Microsoft AD 網域的信任關係

現在準備工作已完成，最終步驟是在兩個 AWS Managed Microsoft AD 網域之間建立信任。如果您在信任建立程序期間發生任何問題，請參閱「信任建立狀態原因」以取得協助。

在第一個 AWS Managed Microsoft AD 網域中設定信任

在此教學課程中，您會設定雙向樹系信任。但是如果您建立單向樹系信任，請注意您每個網域的信任方向都必須互相配合。例如，如果您在此第一個網域上建立單向傳出信任，則需要在第二個 AWS Managed Microsoft AD 網域上建立單向傳入信任。

> **Note**
>
> AWS Managed Microsoft AD 也支援外部信任。但在此教學課程中，您將建立一個雙向樹系信任。

在第一個 AWS Managed Microsoft AD 網域中設定信任

1. 開啟 AWS Directory Service 主控台。
2. 在目錄頁面上，選擇您的第一個 AWS Managed Microsoft AD ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取主要區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
4. 在 Trust relationships (信任關係) 區段，選擇 Actions (動作)，然後選取 Add trust relationship (新增信任關係)。
5. 在新增信任關係頁面上，輸入第二個 AWS Managed Microsoft AD 網域的 FQDN。請務必記住此密碼，因為在設定第二個 AWS Managed Microsoft AD 的信任時，您需要此密碼。指定方向。在此例中，我們選擇雙向。
6. 在條件式轉送器欄位中，輸入第二個 AWS Managed Microsoft AD DNS 伺服器的 IP 地址。
7. （選用）選擇新增另一個 IP 地址，並輸入第二個 AWS Managed Microsoft AD DNS 伺服器的第二個 IP 地址。您最多總共可以指定四個 DNS 伺服器。
8. 選擇新增。該信任將在此時失敗，這是正常的，因為在我們建立另一方的信任之前這一信任關係並不會成立。

在第二個 AWS Managed Microsoft AD 網域中設定信任

現在，您可以設定與第二個 AWS Managed Microsoft AD 目錄的樹系信任關係。由於您在第一個 AWS Managed Microsoft AD 網域上建立雙向森林信任，因此您也可以使用此 AWS Managed Microsoft AD 網域建立雙向信任。

在第二個 AWS Managed Microsoft AD 網域中設定信任

1. 返回 AWS Directory Service 主控台。
2. 在目錄頁面上，選擇您的第二個 AWS Managed Microsoft AD ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取主要區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
4. 在 Trust relationships (信任關係) 區段，選擇 Actions (動作)，然後選取 Add trust relationship (新增信任關係)。
5. 在新增信任關係頁面上，輸入第一個 AWS Managed Microsoft AD 網域的 FQDN。輸入您在建立內部部署域之信任時使用的同一組信任密碼。指定方向。在此例中，我們選擇雙向。
6. 在條件式轉寄站欄位中，輸入第一個 AWS Managed Microsoft AD DNS 伺服器的 IP 地址。
7. （選用）選擇新增另一個 IP 地址，並輸入第一個 AWS Managed Microsoft AD DNS 伺服器的第二個 IP 地址。您最多總共可以指定四個 DNS 伺服器。
8. 選擇新增。該信任應該很快就會得到驗證。
9. 現在，返回您在第一個域中建立的信任並再次確認信任關係。

恭喜您。您現在在兩個 AWS Managed Microsoft AD 網域之間具有信任關係。這兩個網域之間只可設定一項關係。例如，如果您想要將信任方向變更為單向，您需要先刪除這項現有關係，再建立新的關係。

擴展您的 AWS Managed Microsoft AD 結構描述

AWS Managed Microsoft AD 使用結構描述來組織和強制執行目錄資料的儲存方式。將定義新增至結構描述的程序稱為「延伸結構描述」。結構描述延伸可讓您使用有效的 LDAP 資料交換格式 (LDIF) 檔案來修改 AWS Managed Microsoft AD 目錄的結構描述。如需 AD 結構描述及如何擴展您結構描述的詳細資訊，請參閱下列主題。

何時擴展 AWS Managed Microsoft AD 結構描述

您可以透過新增物件類別和屬性來擴展 AWS Managed Microsoft AD 結構描述。例如，如果您的應用程式需要變更結構描述才能支援單一登入功能，您就可以執行此操作。

您也可以使用結構描述延伸，對於仰賴特定 Active Directory 物件類別和屬性的應用程式提供支援。如果您需要將相依於 AWS Managed Microsoft AD 的企業應用程式遷移至 AWS 雲端，這會特別有用。

每個新增至現有 Active Directory 結構描述的屬性或類別都必須定義唯一的 ID。如此一來，當公司新增結構描述延伸時，就可以確保這些延伸是唯一的，而且不會與其他延伸相衝突。這些 IDs 稱為 AD 物件識別符 (OIDs)，並存放在 AWS Managed Microsoft AD 中。

若要開始使用，請參閱教學課程：擴展 AWS Managed Microsoft AD 結構描述。

相關主題

- 擴展您的 AWS Managed Microsoft AD 結構描述
- 結構描述元素

主題

- 教學課程：擴展 AWS Managed Microsoft AD 結構描述

教學課程：擴展 AWS Managed Microsoft AD 結構描述

在本教學課程中，您將了解如何透過新增符合您特定需求的唯一屬性和類別 AWS ，擴展 AWS Directory Service for Microsoft Active Directory 目錄的結構描述。 AWS 受管 Microsoft AD 結構描述延伸只能使用有效的 LDIF （輕量型目錄交換格式） 指令碼檔案來上傳和套用。

屬性 (attributeSchema) 定義資料庫中的欄位，而類別 (classSchema) 定義資料庫中的表格。例如，Active Directory 中所有的使用者物件都由結構描述類別使用者所定義，而使用者的個別內容，例如電子郵件地址或電話號碼，則分別由屬性定義。

如果您想要新增新的屬性，例如鞋碼，您可以定義類型為整數的新屬性。您也可以定義下限和上限，像是 1 到 20。一旦建立鞋碼 attributeSchema 物件，您就要更改使用者classSchema 物件來包含該屬性。屬性可以連結到多個類別。例如，鞋碼也可以新增到聯絡人類別。如需 Active Directory 結構描述的詳細資訊，請參閱「何時擴展 AWS Managed Microsoft AD 結構描述」。

此工作流程有三個基本步驟。

步驟 1：建立您的 LDIF 檔案

首先，您要建立 LDIF 檔案以及定義屬性應該新增到的新屬性和任何類別。您會在工作流程的下一個階段中使用這個檔案。

步驟 2：匯入您的 LDIF 檔案

在此步驟中，您可以使用 AWS Directory Service 主控台將 LDIF 檔案匯入 Microsoft Active Directory 環境。

步驟 3：驗證結構描述延伸是否成功

最後，身為管理員，您要使用 EC2 執行個體驗證新的延伸會出現在 Active Directory 結構描述內嵌中。

步驟 1：建立您的 LDIF 檔案

LDIF 檔案是標準的純文字資料互換格式，代表 LDAP (輕量型目錄存取協定) 目錄內容和更新請求。LDIF 會將目錄內容傳輸為一個記錄集，每個物件 (或項目) 一筆記錄。它也代表記錄集的更新請求，例如新增、修改、刪除和重新命名，每個更新請求一筆記錄。

透過在 AWS Managed Microsoft AD 目錄上執行`ldifde.exe`應用程式，匯入結構描述變更 AWS Directory Service 的 LDIF 檔案。因此，您會發現了解 LDIF 指令碼語法很有幫助。如需詳細資訊，請參閱 LDIF 指令碼。

很多第三方 LDIF 工具可以擷取、清理和更新您的結構描述更新。無論您使用哪種工具，請務必了解您 LDIF 檔案中使用的所有識別符都必須是唯一的。

我們強烈建議您先行檢閱下列概念和秘訣，再建立您的 LDIF 檔案。

- 結構描述元素 - 了解結構描述元素，例如屬性、類別、物件 ID 和連結的屬性。如需詳細資訊，請參閱結構描述元素。

- 項目序列 - 請確定您 LDIF 檔案中的項目順序是遵循 Directory Information Tree (DIT) 從上到下的配置順序。LDIF 檔案排序的一般規則如下：

  - 不同的項目間隔一行。
  - 子項目列在父項目之後。
  - 請確定結構描述中有屬性或物件類別等項目。如果它們不存在，您必須先將它們新增至結構描述才能使用。例如，您必須先建立屬性，才能將屬性指派給類別。

- DN 的格式 - 針對 LDIF 檔案中的每條新指示，在指示的第一行定義辨別名稱 (DN)。DN 可識別 Active Directory 物件樹狀目錄中的 Active Directory 物件，且必須包含目錄的網域元件。例如，此教學中的目錄網域元件是 `DC=example,DC=com`。

  DN 必須包含 Active Directory 物件的通用名稱 (CN)。第一個 CN 項目代表屬性或類別名稱。若要延伸 Active Directory 結構描述，請使用 `CN=Schema,CN=Configuration`。請記住，您無法修改 Active Directory 物件內容。一般 DN 格式如下。

  ```
  dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
  ```

  在此教學中，新鞋碼屬性的 DN 如下：

  ```
  dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
  ```

- 警告 - 擴展您的結構描述之前，請先檢閱以下的警告。
  - 擴展您的 Active Directory 結構描述之前，請務必檢閱有關此操作影響的 Microsoft 警告。如需詳細資訊，請參閱 What You Must Know Before Extending the Schema。
  - 您無法刪除結構描述屬性或類別。因此，如果您發生錯誤且不想從備份還原，您只能停用物件。如需詳細資訊，請參閱 Disabling Existing Classes and Attributes。
  - 不支援變更 defaultSecurityDescriptor。

若要進一步了解如何建構 LDIF 檔案，並查看可用於測試 AWS Managed Microsoft AD 結構描述延伸的範例 LDIF 檔案，請參閱 AWS 安全部落格上的如何擴展 AWS Managed Microsoft AD Directory 結構描述一文。

後續步驟

步驟 2：匯入您的 LDIF 檔案

步驟 2：匯入您的 LDIF 檔案

您可以從 AWS Directory Service 主控台匯入 LDIF 檔案或使用 API 來擴展結構描述。如需如何使用結構描述延伸 API 執行此操作的詳細資訊，請參閱《AWS Directory Service API 參考》。 AWS 目前不支援 Microsoft Exchange 等外部應用程式來直接執行結構描述更新。

> **Important**
>
> 當您更新 AWS Managed Microsoft AD 目錄結構描述時，此操作無法還原。換句話說，當您建立新的類別或屬性時，Active Directory 不允許您將其移除。不過，您可以停用它。

如果您必須刪除結構描述的變更，您可以選擇從之前的快照還原目錄。還原快照會讓結構描述和目錄資料都退回到先前的點，而不僅只是結構描述。請注意，快照的支援存留期上限為 180 天。如需詳細資訊，請參閱 Microsoft 網站上的 Useful shelf life of a system-state backup of Active Directory。

在更新程序開始之前， AWS 受管 Microsoft AD 會拍攝快照來保留目錄的目前狀態。

Note

結構描述延伸是 AWS Managed Microsoft AD 的全域功能。如果您使用 設定 AWS Managed Microsoft AD 的多區域複寫，則必須在 主要區域 中執行下列步驟。變更將自動套用至所有複寫區域。如需詳細資訊，請參閱全域與區域功能。

匯入您的 LDIF 檔案

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取主要區域，然後選擇維護索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇維護索引標籤。
4. 在 Schema extensions (結構描述延伸) 區段，選擇 Actions (動作)，然後選擇 Upload and update schema (上傳及更新結構描述)。
5. 在對話方塊中，按一下 Browse (瀏覽)，選取有效的 LDIF 檔案，輸入描述，然後選擇 Update Schema (更新結構描述)。

Important

擴展結構描述是一項重要的操作。若未先在開發或測試環境中使用您的應用程式進行測試，請勿在生產環境中套用任何結構描述更新。

LDIF 檔案的套用方式

上傳 LDIF 檔案之後， AWS 受管 Microsoft AD 會採取步驟來保護您的目錄免於發生錯誤，因為它會依下列順序套用變更。

1. 驗證 LDIF 檔案。由於 LDIF 指令碼可以操作網域中的任何物件，因此 AWS 受管 Microsoft AD 會在您上傳後立即執行檢查，以協助確保匯入操作不會失敗。這些檢查包括確保下列項目：
   - 要更新的物件只保留在結構描述容器中
   - DC (網域控制站) 部分符合 LDIF 指令碼執行所在的網域名稱
2. 建立您的目錄快照。您可以使用快照來還原您的目錄，以免您的應用程式在更新結構描述之後發生任何問題。
3. 將變更套用至單一 DC。 AWS 受管 Microsoft AD 會隔離其中一個 DCs，並將 LDIF 檔案中的更新套用至隔離的 DC。然後，它會選取其中一個 DCs 做為主要結構描述，從目錄複寫中移除該 DC，並使用 套用您的 LDIF 檔案`Ldifde.exe`。
4. 複寫適用於所有 DCs。 AWS 受管 Microsoft AD 會將隔離的 DC 重新新增至複寫，以完成更新。在一切都發生後，您的目錄仍不中斷，繼續向您的應用程式提供 Active Directory 服務。

下一步驟

步驟 3：驗證結構描述延伸是否成功

步驟 3：驗證結構描述延伸是否成功

完成匯入流程後，請務必驗證結構描述更新是否套用到您的目錄。這在您遷移或更新任何依賴結構描述更新的應用程式之前，尤其重要。您可以使用各種不同的 LDAP 工具，或撰寫發出適當 LDAP 命令的測試工具來執行此作業。

此程序使用 Active Directory 結構描述內嵌及/或 PowerShell 驗證是否套用結構描述更新。您必須從加入 AWS Managed Microsoft AD 的網域電腦執行這些工具。這可以是能夠存取您虛擬私有雲端 (VPC) 或透過虛擬私有網路 (VPN) 連線，在您內部部署網路中執行的 Windows 伺服器。您也可以在 Amazon EC2 Windows 執行個體上執行這些工具 (請參閱如何使用無縫加入域啟動新的 EC2 執行個體)。

使用 Active Directory 結構描述內嵌進行驗證

1. 使用 TechNet 網站的指示來安裝 Active Directory 結構描述內嵌。
2. 開啟 Microsoft Management Console (MMC) 以及擴展您目錄的 AD 結構描述樹狀目錄。
3. 導覽 Classes (類別) 和 Attributes (屬性) 資料夾，直到您找到之前所做的結構描述變更。

使用 PowerShell 進行驗證

1. 開啟 PowerShell 視窗。
2. 使用以下 `Get-ADObject` cmdlet 來驗證結構描述變更。例如：

```
get-adobject -Identity 'CN=Shoe-
Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
```

選用步驟

將值新增至新屬性 - 選用

將值新增至新屬性 - 選用

當您建立新的屬性，並想要將新值新增至 AWS Managed Microsoft AD 目錄中的屬性時，請使用此選用步驟。

在屬性中新增值

1. 開啟PowerShell命令列公用程式，並使用下列命令設定新屬性。在這個範例中，我們會將新的 EC2InstanceID 值新增到特定電腦的屬性中。

```
PS C:\> set-adcomputer -Identity computer name -add @{example-
EC2InstanceID = 'EC2 instance ID'}
```

2. 您可以執行以下命令，驗證 EC2InstanceID 值是否已新增到電腦物件：

```
PS C:\> get-adcomputer -Identity computer name –Property example-
EC2InstanceID
```

相關資源

下列資源連結位於 Microsoft 網站並提供相關資訊。

- Extending the Schema (Windows)
- Active Directory Schema (Windows)
- Active Directory Schema
- Windows 系統管理：擴充 Active Directory 架構

- Restrictions on Schema Extension (Windows)
- Ldifde

將 Amazon EC2 執行個體加入 AWS Managed Microsoft AD 的方法

您可以在執行個體啟動時，將 Amazon EC2 執行個體無縫加入您的Active Directory網域。如需詳細資訊，請參閱將 Amazon EC2 Windows 執行個體加入您的 AWS Managed Microsoft AD Active Directory。您也可以啟動 EC2 執行個體，並透過AWS Systems Manager 自動化直接從 AWS Directory Service 主控台加入 Active Directory網域。

如果您需要手動將 EC2 執行個體加入Active Directory網域，您必須在適當的區域和安全群組或子網路中啟動執行個體，然後將執行個體加入網域。

若要從遠端連線到這些執行個體，您必須具備從來源網路連線到執行個體的 IP 連線能力。在大多數情況下，這需要將網際網路閘道連接到您的 VPC，而且執行個體必須具備公有 IP 地址。

主題

- 在 AWS Managed Microsoft AD 中啟動目錄管理執行個體 Active Directory
- 將 Amazon EC2 Windows 執行個體加入您的 AWS Managed Microsoft AD Active Directory
- 將 Amazon EC2 Linux 執行個體加入您的 AWS Managed Microsoft AD Active Directory
- 將 Amazon EC2 Mac 執行個體加入您的 AWS Managed Microsoft AD Active Directory
- 委派 AWS Managed Microsoft AD 的目錄聯結權限
- 建立或變更 AWS Managed Microsoft AD 的 DHCP 選項集

在 AWS Managed Microsoft AD 中啟動目錄管理執行個體 Active Directory

此程序 AWS Management Console 會使用 AWS Systems Manager 自動化來管理您的目錄，在 中啟動 Amazon EC2 目錄管理Windows執行個體。您也可以直接在 AWS Systems Manager 自動化主控台中執行自動化 AWS-CreateDSManagementInstance 來完成此操作。

如需詳細資訊，請參閱下列連結：

- 使用 簡化Active Directory網域加入 AWS Systems Manager
- 如何使用 AWS Systems Manager 將執行中的 EC2 Windows執行個體加入我的 AWS Directory Service 網域？

先決條件

完成本教學課程需要下列先決條件：

- 您將需要設定 AWS Systems Manager。如需詳細資訊，請參閱設定 AWS Systems Manager。
- 您需要一個允許 Systems Manager 和 AWS Managed Microsoft AD 的 IAM 執行個體描述檔角色。
  - 如需 Systems Manager 的詳細資訊，請參閱設定 Systems Manager 所需的執行個體許可。
  - IAM 執行個體角色需要下列 AWS 受管政策，以便您的 EC2 目錄管理Windows執行個體可以加入您的 AWS Managed Microsoft AD 網域：
    - **AmazonSSMManagedInstanceCore**
    - **AmazonSSMDirectoryServiceAccess**
- 連線至 AWS Managed Microsoft AD 的 VPC 需要允許存取公 AWS Directory Service 有端點。如需詳細資訊，請參閱建立 AWS Managed Microsoft AD 的先決條件。
- 您必須在帳戶中啟用下列許可，才能從主控台啟動目錄管理 EC2 執行個體：
  - `ds:DescribeDirectories`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateTags`
  - `ec2:DeleteSecurityGroup`
  - `ec2:DescribeInstances`
  - `ec2:DescribeInstanceStatus`
  - `ec2:DescribeKeyPairs`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeVpcs`
  - `ec2:RunInstances`
  - `ec2:TerminateInstances`
  - `iam:AddRoleToInstanceProfile`
  - `iam:AttachRolePolicy`
  - `iam:CreateInstanceProfile`
  - `iam:CreateRole`
  - `iam:DeleteInstanceProfile`
  - `iam:DeleteRole`

- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:ListInstanceProfiles
- iam:ListInstanceProfilesForRole
- iam:PassRole
- iam:RemoveRoleFromInstanceProfile
- iam:TagInstanceProfile
- iam:TagRole
- ssm:CreateDocument
- ssm:DeleteDocument
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetParameters
- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:ListDocuments
- ssm:SendCommand
- ssm:StartAutomationExecution
- ssm:GetDocument

在 中啟動目錄管理 EC2 執行個體 AWS Management Console

1. 登入 AWS Directory Service 主控台。
2. 在 Active Directory 下，選擇目錄。
3. 選擇您要啟動目錄管理 EC2 執行個體之目錄的目錄 ID。
4. 在目錄頁面的右上角，選擇動作。
5. 在動作下拉式清單中，選擇啟動目錄管理 EC2 執行個體。
6. 在啟動目錄管理 EC2 執行個體頁面上的輸入參數下，填入欄位。

a. （選用）您可以為執行個體提供金鑰對。從金鑰對名稱 - 選用下拉式清單中，選取金鑰對。

b. （選用）選擇檢視 AWS CLI 命令，以查看您在 中用來 AWS CLI 執行此自動化的範例。

7. 選擇提交。

8. 您將返回目錄頁面。螢幕頂部會顯示綠色閃爍列，表示您已成功開始啟動。

檢視目錄管理 EC2 執行個體

如果您尚未為目錄啟動任何 EC2 執行個體，則目錄管理 EC2 執行個體下會顯示連字號 (-)。

1. 在 Active Directory 下，選擇目錄，然後選取要檢視的目錄。

2. 在目錄詳細資訊中的目錄管理 EC2 執行個體下，選擇要檢視的一個或所有執行個體。

3. 選擇執行個體後，您將被帶到 EC2 連線至執行個體頁面，以遠端連線至執行個體桌面。

將 Amazon EC2 Windows 執行個體加入您的 AWS Managed Microsoft AD Active Directory

您可以啟動 Amazon EC2 Windows執行個體並將其加入 AWS Managed Microsoft AD。或者，您可以手動將現有的 EC2 Windows執行個體加入 AWS Managed Microsoft AD。

Seamlessly join EC2 Windows instance

此程序會將 Amazon EC2 Windows執行個體無縫加入您的 AWS Managed Microsoft AD。如果您需要跨多個 執行無縫網域聯結 AWS 帳戶，請參閱 教學課程：共用 AWS Managed Microsoft AD 目錄以實現無縫 EC2 加入網域。如需 Amazon EC2 的詳細資訊，請參閱什麼是 Amazon EC2？。

先決條件

若要無縫加入 EC2 執行個體的網域，您將需要完成下列操作：

- 擁有 AWS Managed Microsoft AD。如需詳細資訊，請參閱 建立 AWS Managed Microsoft AD。
- 您需要下列 IAM 許可才能無縫加入 EC2 Windows執行個體：
  - 具有下列 IAM 許可的 IAM 執行個體設定檔：
    - `AmazonSSMManagedInstanceCore`
    - `AmazonSSMDirectoryServiceAccess`
  - 將 EC2 加入 AWS Managed Microsoft AD 的使用者無縫網域需要下列 IAM 許可：

- AWS Directory Service 許可：
  - "ds:DescribeDirectories"
  - "ds:CreateComputer"
- Amazon VPC 許可：
  - "ec2:DescribeVpcs"
  - "ec2:DescribeSubnets"
  - "ec2:DescribeNetworkInterfaces"
  - "ec2:CreateNetworkInterface"
  - "ec2:AttachNetworkInterface"
- EC2 許可：
  - "ec2:DescribeInstances"
  - "ec2:DescribeImages"
  - "ec2:DescribeInstanceTypes"
  - "ec2:RunInstances"
  - "ec2:CreateTags"
- AWS Systems Manager 許可：
  - "ssm:DescribeInstanceInformation"
  - "ssm:SendCommand"
  - "ssm:GetCommandInvocation"
  - "ssm:CreateBatchAssociation"

建立 AWS Managed Microsoft AD 時，會使用傳入和傳出規則建立安全群組。若要進一步了解這些規則和連接埠，請參閱 使用 AWS Managed Microsoft AD 建立的內容。若要無縫加入 EC2 Windows執行個體的網域，您要啟動執行個體的 VPC 應允許 AWS Managed Microsoft AD 安全群組傳入和傳出規則中允許的相同連接埠。

- 根據您的網路安全和防火牆設定，您可能需要允許額外的傳出流量。此流量適用於 HTTPS （連接埠 443) 到下列端點：

端點	角色
ec2messages. *region*.amazonaws.com	使用 Session Manager 服務建立和刪除工作階段通道。如需詳細資訊，請參閱 AWS Systems Manager 端點和配額。
ssm.*region*.amazonaws.com	的端點 AWS Systems Manager Session Manager。如需詳細資訊，請參閱 AWS Systems Manager 端點和配額。
ssmmessages. *region*.amazonaws.com	使用 Session Manager 服務建立和刪除工作階段通道。如需詳細資訊，請參閱 AWS Systems Manager 端點和配額。
ds.*region*.amazonaws.com	的端點 AWS Directory Service。如需詳細資訊，請參閱的區域可用性 AWS Directory Service。

- 我們建議您使用 DNS 伺服器來解析 AWS Managed Microsoft AD 網域名稱。若要這樣做，您可以建立 DHCP 選項集。如需詳細資訊，請參閱建立或變更 AWS Managed Microsoft AD 的 DHCP 選項集。
  - 如果您選擇不建立 DHCP 選項集，則您的 DNS 伺服器將是靜態的，並由 AWS Managed Microsoft AD 設定為 。

無縫加入 Amazon EC2 Windows執行個體

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/ec2/：// 開啟 Amazon EC2 主控台。
2. 在導覽列中，選擇 AWS 區域 與現有目錄相同的 。
3. 在 EC2 儀表板的啟動執行個體區段中，選擇啟動執行個體。
4. 在啟動執行個體頁面上的名稱和標籤區段下，輸入您想要用於 Windows EC2 執行個體的名稱。
5. (選用) 針對新增標籤，新增一個或多個標籤鍵值對來組織、追蹤或控制對此 EC2 執行個體的存取。

6. 在應用程式和作業系統映像 (Amazon Machine Image) 區段中，選擇快速啟動窗格中的 Windows。您可以從 Amazon Machine Image (AMI)下拉式清單中變更 Windows Amazon Machine Image (AMI)。
7. 在執行個體類型區段中，從執行個體類型下拉式清單中選擇您要使用的執行個體類型。
8. 在金鑰對 (登入) 區段中，您可以選擇建立新金鑰對或從現有金鑰對中進行選擇。

   a. 若要建立新的金鑰對，請選擇建立新金鑰對。

   b. 輸入金鑰對的名稱，然後選取金鑰對類型和私有金鑰檔案格式的選項。

   c. 若要將私有金鑰儲存為可與 OpenSSH 搭配使用的格式，請選擇 .pem。若要將私有金鑰儲存為可與 PuTTY 搭配使用的格式，請選擇 .ppk。

   d. 選擇建立金鑰對。

   e. 您的瀏覽器會自動下載私有金鑰檔案。將私有金鑰檔案存放在安全的地方。

   > **Important**
   >
   > 這是您儲存私有金鑰檔案的唯一機會。

9. 在啟動執行個體頁面上的網路設定區段下，選擇編輯。從 VPC – required 下拉式清單中選擇在其中建立目錄的 VPC。
10. 從子網路下拉式清單中選擇 VPC 中的公有子網路之一。您所選取的子網路必須將所有外部流量路由到網際網路閘道。如果沒有，則將無法從遠端連線到執行個體。

    如需有關連線至網際網路閘道的詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用網際網路閘道連線至網際網路一節。
11. 在自動指派公有 IP 下，選擇啟用。

    如需公有和私有 IP 定址的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 執行個體 IP 定址。 Amazon EC2
12. 對於防火牆 (安全群組)設定，您可以使用預設設定或根據需要進行變更。
13. 對於設定儲存設定，您可以使用預設設定或根據需要進行變更。
14. 選取進階詳細資訊區段，從域加入目錄下拉式清單中選取域。

    > **Note**
    >
    > 選擇網域加入目錄後，您可能會看到：

如果 EC2 啟動精靈識別具有非預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：

- 如果您先前已編輯 SSM 文件，且預期屬性，請選擇關閉並繼續啟動 EC2 執行個體，而不進行任何變更。
- 選取此處的刪除現有 SSM 文件連結，以刪除 SSM 文件。這將允許建立具有正確屬性的 SSM 文件。當您啟動 EC2 執行個體時，系統會自動建立 SSM 文件。

15. 對於 IAM 執行個體設定檔，您可以選取現有的 IAM 執行個體設定檔或建立新的設定檔。從 IAM 執行個體設定檔下拉式清單中選取具有 AmazonSSMManagedInstanceCore 和 AmazonSSMDirectoryServiceAccess AWS 受管政策的 IAM 執行個體設定檔。若要建立新的 IAM 設定檔，請選擇建立新的 IAM 設定檔連結，然後執行下列動作：

    1. 選擇建立角色。
    2. 在選取信任的實體下，選取 AWS 服務。
    3. 在 Use case (使用案例) 下，選擇 EC2。
    4. 在新增許可下的政策清單中，選取 AmazonSSMManagedInstanceCore 和 AmazonSSMDirectoryServiceAccess 政策。在搜尋方塊中，輸入 **SSM** 以篩選政策。選擇下一步。

    > **Note**
    >
    > AmazonSSMDirectoryServiceAccess 提供將執行個體加入 Active Directory受管的許可 AWS Directory Service。AmazonSSMManagedInstanceCore 提供使用 AWS Systems Manager 服務所需的最低許可。有關建立具有這些許可的角色的更多資訊，以及有關可以指派給 IAM 角色的其他許可和政策的資訊，請參閱《AWS Systems Manager 使用者指南》中的為 Systems Manager 建立 IAM 執行個體設定檔一節。

    5. 在命名、檢閱和建立頁面上，針對角色名稱輸入角色名稱。您將需要此角色名稱來連接到 EC2 執行個體。
    6. (選用) 您可以在描述欄位中提供 IAM 執行個體設定檔的描述。
    7. 選擇建立角色。
    8. 返回啟動執行個體頁面，然後選擇 IAM 執行個體設定檔旁的重新整理圖示。剛剛建立的 IAM 執行個體設定檔應顯示在 IAM 執行個體設定檔下拉式清單中。選擇這個新的設定檔並將其餘設定保留為預設值。

16. 選擇啟動執行個體。

Manually join EC2 Windows instance

若要手動將現有的 Amazon EC2 Windows執行個體加入 AWS Managed Microsoft ADActive Directory，必須使用 中指定的參數啟動執行個體將 Amazon EC2 Windows 執行個體加入您的 AWS Managed Microsoft AD Active Directory。

您需要 AWS Managed Microsoft AD DNS 伺服器的 IP 地址。此資訊可在目錄服務 > 目錄 > 目錄的目錄 ID 連結 > 目錄詳細資料和網路與安全部分下找到。

將 Windows 執行個體加入 AWS Managed Microsoft AD Active Directory

1. 使用任何遠端桌面協定用戶端連線到執行個體。
2. 在執行個體上開啟 TCP/IPv4 屬性內容對話方塊。
   a. 開啟 Network Connections (網路連線)。

      Tip

      您可以在執行個體上，透過從命令提示執行下列命令，來直接開啟 Network Connections (網路連線)。

      ```
      %SystemRoot%\system32\control.exe ncpa.cpl
      ```

   b. 開啟任何已啟用網路連線的內容 (右鍵) 選單，然後選擇 Properties (內容)。
   c. 在連線內容對話方塊中，開啟 (按兩下) Internet Protocol Version 4 (網際網路協定第 4 版)。
3. 選取使用以下 DNS 伺服器地址，將偏好的 DNS 伺服器和備用 DNS 伺服器地址變更為 AWS Managed Microsoft AD 提供的 DNS 伺服器的 IP 地址，然後選擇確定。
4. 開啟執行個體的 System Properties (系統內容) 對話方塊，選取 Computer Name (電腦名稱) 標籤，然後選擇 Change (變更)。

> **Tip**
>
> 您可以在執行個體上，透過從命令提示執行下列命令，來直接開啟 System Properties (系統內容對話方塊)。
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. 在成員欄位中，選取網域，輸入 AWS Managed Microsoft AD Active Directory 的完整名稱，然後選擇確定。
6. 當系統提示您輸入網域管理員的名稱和密碼時，請輸入具有網域加入權限的帳戶使用者名稱和密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

> **Note**
>
> 您可以輸入網域的完整名稱或 NetBIOS 名稱，後面接著反斜線 (\)，然後輸入使用者名稱。使用者名稱為 Admin。例如 **`corp.example.com\admin`** 或 **`corp\admin`**。

7. 收到歡迎您加入網域的訊息之後，請重新啟動執行個體，讓變更生效。

現在您的執行個體已加入 AWS Managed Microsoft AD Active Directory 網域，您可以遠端登入該執行個體，並安裝公用程式來管理目錄，例如新增使用者和群組。Active Directory 管理工具可用來建立使用者和群組。如需詳細資訊，請參閱安裝 AWS Managed Microsoft AD 的 Active Directory 管理工具。

> **Note**
>
> 您也可以使用 Amazon Route 53 來處理 DNS 查詢，而不是手動變更 Amazon EC2 執行個體上的 DNS 地址。如需詳細資訊，請參閱將 Directory Service 的 DNS 解析與 整合 Amazon Route 53 Resolver，以及將傳出 DNS 查詢轉送至您的網路。

將 Amazon EC2 Linux 執行個體加入您的 AWS Managed Microsoft AD Active Directory

您可以在 中啟動 EC2 Linux 執行個體並將其加入 AWS Managed Microsoft AD AWS Management Console。您也可以手動將 EC2 Linux 執行個體加入 AWS Managed Microsoft AD。您也可以使用 Winbind 等工具，讓網域將 EC2 Linux 執行個體加入 AWS Managed Microsoft AD。

系統支援下列 Linux 執行個體分佈和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 位元 x86)
- Red Hat Enterprise Linux 8 (HVM) (64 位元 x86)
- Ubuntu Server 18.04 LTS 及 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Ubuntu 14 和 Red Hat Enterprise Linux 7 和 8 之前的分佈不支援無縫網域聯結功能。

加入 EC2 Linux 執行個體的網域方式：

- 將 Amazon EC2 Linux 執行個體無縫加入 AWS Managed Microsoft AD Active Directory
- 將 Amazon EC2 Linux 執行個體無縫加入共用的 AWS Managed Microsoft AD
- 手動將 Amazon EC2 Linux 執行個體加入 AWS Managed Microsoft AD Active Directory
- 使用 Winbind 手動將 Amazon EC2 Linux 執行個體加入 AWS Managed Microsoft AD Active Directory

將 Amazon EC2 Linux 執行個體無縫加入 AWS Managed Microsoft AD Active Directory

此程序會將 Amazon EC2 Linux 執行個體無縫加入您的 AWS Managed Microsoft AD Active Directory。若要完成此程序，您需要建立可能會產生額外費用的 AWS Secrets Manager 秘密。如需詳細資訊，請參閱AWS Secrets Manager 定價。

如果您需要跨多個 AWS 帳戶執行無縫網域聯結，您可以選擇啟用目錄共用。

系統支援下列 Linux 執行個體分佈和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 位元 x86)
- Red Hat Enterprise Linux 8 (HVM) (64 位元 x86)
- Ubuntu Server 18.04 LTS 及 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Ubuntu 14 和 Red Hat Enterprise Linux 7 和 8 之前的分佈不支援無縫網域聯結功能。

如需將 Linux 執行個體無縫加入 AWS Managed Microsoft AD Active Directory 的程序示範，請參閱下列 YouTube 影片。

Amazon EC2 for Linux 無縫 AD 域加入示範

先決條件

您必須先完成這些區段中的程序，才能設定 EC2 Linux 執行個體的無縫網域聯結。

無縫網域聯結的網路先決條件

若要無縫加入 EC2 Linux 執行個體的網域，您需要完成下列操作：

- 您需要下列 IAM 許可才能無縫加入 EC2 Linux 執行個體：
  - 擁有 AWS Managed Microsoft AD。如需詳細資訊，請參閱 建立 AWS Managed Microsoft AD。
  - 您需要下列 IAM 許可才能無縫加入 EC2 Windows執行個體：
    - 具有下列 IAM 許可的 IAM 執行個體設定檔：
      - `AmazonSSMManagedInstanceCore`
      - `AmazonSSMDirectoryServiceAccess`
    - 將 EC2 加入 AWS Managed Microsoft AD 的使用者無縫網域需要下列 IAM 許可：
      - AWS Directory Service 許可：
        - `"ds:DescribeDirectories"`

        - "ds:CreateComputer"
    - Amazon VPC 許可：
        - "ec2:DescribeVpcs"
        - "ec2:DescribeSubnets"
        - "ec2:DescribeNetworkInterfaces"
        - "ec2:CreateNetworkInterface"
        - "ec2:AttachNetworkInterface"
    - EC2 許可：
        - "ec2:DescribeInstances"
        - "ec2:DescribeImages"
        - "ec2:DescribeInstanceTypes"
        - "ec2:RunInstances"
        - "ec2:CreateTags"
    - AWS Systems Manager 許可：
        - "ssm:DescribeInstanceInformation"
        - "ssm:SendCommand"
        - "ssm:GetCommandInvocation"
        - "ssm:CreateBatchAssociation"
- 建立 AWS Managed Microsoft AD 時，會使用傳入和傳出規則建立安全群組。若要進一步了解這些規則和連接埠，請參閱 使用 AWS Managed Microsoft AD 建立的內容。若要無縫加入 EC2 Linux 執行個體的網域，您要啟動執行個體的 VPC 應允許 AWS Managed Microsoft AD 安全群組傳入和傳出規則中允許的相同連接埠。
    - 根據您的網路安全和防火牆設定，您可能需要允許額外的傳出流量。此流量適用於 HTTPS （連接埠 443) 到下列端點：

端點	角色
ec2messages. *region*.amazonaws.com	使用 Session Manager 服務建立和刪除工作階段通道。如需詳細資訊，請參閱 AWS Systems Manager 端點和配額。

端點	角色
ssm.*region*.amazonaws.com	的端點 AWS Systems Manager Session Manager。如需詳細資訊，請參閱 AWS Systems Manager 端點和配額。
ssmmessages. *region*.amazonaws.com	使用 Session Manager 服務建立和刪除工作階段通道。如需詳細資訊，請參閱 AWS Systems Manager 端點和配額。
ds.*region*.amazonaws.com	的端點 AWS Directory Service。如需詳細資訊，請參閱的區域可用性 AWS Directory Service。
secretsmanager. *region*.amazonaws.com	的端點 AWS Secrets Manager。如需詳細資訊，請參閱 AWS Secrets Manager 端點和配額。

- 我們建議您使用 DNS 伺服器來解析 AWS Managed Microsoft AD 網域名稱。若要這樣做，您可以建立 DHCP 選項集。如需詳細資訊，請參閱建立或變更 AWS Managed Microsoft AD 的 DHCP 選項集。
  - 如果您選擇不建立 DHCP 選項集，則您的 DNS 伺服器將是靜態的，並由 AWS Managed Microsoft AD 設定為 。

選取無縫域加入服務帳戶

您可以將 Linux 電腦無縫加入 AWS Managed Microsoft AD Active Directory網域。為此，您必須使用一個具有建立電腦帳戶許可的使用者帳戶，才能將機器加入域。儘管 AWS 委派管理員或其他群組的成員可能有足夠的權限將電腦加入域，但我們不建議這樣做。我們建議您使用具有將電腦加入域所需的最低權限的服務帳戶，這才是最佳做法。

若要委派具有所需最低權限的帳戶將電腦加入域，您可以執行下列 PowerShell 命令。您必須從已加入域並安裝了 安裝 AWS Managed Microsoft AD 的 Active Directory 管理工具 的 Windows 電腦執行這些命令。此外，您必須使用有權修改電腦 OU 或容器許可的帳戶。PowerShell 命令會設定許可，允許服務帳戶在網域的預設電腦容器中建立電腦物件。

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
```

```
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
 'schemaNamingContext'
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
 -Filter { lDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
 in the Computers container.
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
 'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

如果您偏好使用圖形使用者介面 (GUI)，您可以使用 委派權限給您的服務帳戶 中所述的手動流程。

建立儲存域服務帳戶的機密

您可以使用 AWS Secrets Manager 來存放網域服務帳戶。如需詳細資訊，請參閱建立 AWS Secrets Manager 秘密。

> **Note**
>
> Secrets Manager 需支付相關費用。如需詳細資訊，請參閱AWS Secrets Manager 《 使用者指南》中的 定價。

建立機密並儲存域服務帳戶資訊

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/secretsmanager/ 開啟 AWS Secrets Manager 主控台。
2. 選擇 Store a new secret (存放新機密)。
3. 在 Store a new secret (儲存新機密) 頁面中，執行下列動作：

a. 在秘密類型下，選擇其他類型的秘密。

b. 在鍵/值對下，執行下列動作：

i. 在第一個方塊中，輸入 **awsSeamlessDomainUsername**。在相同資料列的下一個方塊中，輸入服務帳戶的使用者名稱。例如，如果您之前使用的是 PowerShell 命令，則服務帳戶名稱將為 **awsSeamlessDomain**。

> **Note**
>
> 您必須輸入完全正確的 **awsSeamlessDomainUsername**。確認頭尾沒有任何空格。否則域加入將會失敗。

ii. 選擇新增列。

iii. 在新的一列的第一個方塊中，輸入 **awsSeamlessDomainPassword**。在同一列的下一個方塊中，輸入服務帳戶的密碼。

> **Note**
>
> 您必須輸入完全正確的 **awsSeamlessDomainPassword**。確認頭尾沒有任何空格。否則域加入將會失敗。

iv. 在加密金鑰下，保留預設值 `aws/secretsmanager`。 選擇此選項時， AWS Secrets Manager 一律會加密秘密。您也可以選擇您建立的金鑰。

v. 選擇下一步。

4. 在秘密名稱下，使用下列格式輸入包含目錄 ID 的秘密名稱，將 *d-xxxxxxxxx* 取代為您的目錄 ID：

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

這在應用程式中將用於擷取機密。

> **Note**
>
> 您必須輸入完全正確的 **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join**，但需要將 *d-xxxxxxxxxx* 替換為目錄 ID。確認頭尾沒有任何空格。否則域加入將會失敗。

5. 將其他所有設定保留為預設值，然後選擇下一步。
6. 針對設定自動輪換，選擇停用自動輪換，然後選擇下一步。

   您可以在存放後開啟此秘密的輪換。
7. 檢查設定，然後選擇儲存以儲存變更。Secrets Manager 主控台會傳回帳戶中的秘密清單，清單中包含現在的新秘密。
8. 從清單中選擇您新建立的機密名稱，並記下 Secret ARN 值。您會在下一節中用到它。

開啟網域服務帳戶秘密的輪換

我們建議您定期輪換秘密，以改善您的安全狀態。

開啟網域服務帳戶秘密的輪換

- 遵循AWS Secrets Manager 《 使用者指南》中設定 AWS Secrets Manager 秘密的自動輪換中的指示。

  對於步驟 5，請使用AWS Secrets Manager 《 使用者指南》中的輪換範本 Microsoft Active Directory 登入資料。

  如需協助，請參閱AWS Secrets Manager 《 使用者指南》中的疑難排解 AWS Secrets Manager 輪換。

建立必要的 IAM 政策和角色

透過下列步驟建立自訂政策，以允許對 Secrets Manager 無縫域加入機密 (您先前建立的) 進行唯讀存取，以及建立新的 LinuxEC2DomainJoin IAM 角色。

建立 Secrets Manager IAM 讀取政策

您需要使用 IAM 主控台建立一個政策，授予對 Secrets Manager 機密的唯讀存取權。

建立 Secrets Manager IAM 讀取政策

1. 以具有建立 IAM 政策許可的使用者 AWS Management Console 身分登入 。前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，存取管理，選擇政策。
3. 選擇建立政策。
4. 選擇 JSON 標籤並從下列 JSON 政策文件複製文字。然後將其貼到 JSON 文字方塊中。

> **Note**
>
> 請務必將區域和資源 ARN 取代為您先前建立之秘密的實際區域和 ARN。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. 完成時，選擇 Next (下一步)。政策驗證程式會回報任何語法錯誤。如需詳細資訊，請參閱驗證 IAM 政策。
6. 在檢閱政策頁面上，輸入政策的名稱，例如 **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**。檢閱摘要區段來查看您的政策所授予的許可。然後選擇建立政策來儲存變更。新的政策會出現在受管政策清單中，並且已準備好連接至身分。

> **Note**
>
> 我們建議您為每個機密建立一個政策。這樣做可以確保執行個體只能存取適當的機密，並在執行個體受到入侵時將影響降至最低。

建立 LinuxEC2DomainJoin 角色

您可以使用 IAM 主控台建立將用於域加入 Linux EC2 執行個體的角色。

建立 LinuxEC2DomainJoin 角色

1. 以具有建立 IAM 政策許可的使用者 AWS Management Console 身分登入 。前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格的存取管理下，選擇角色。
3. 在內容窗格中，選擇建立角色。
4. 在 Select type of trusted entity (選擇可信任執行個體類型) 下，選擇 AWS service (服務)。
5. 在使用案例中，選擇 EC2，然後選擇下一步。

6. 對於篩選政策，請執行下列操作：

   a. 輸入 **AmazonSSMManagedInstanceCore**。然後選取清單中相應項目的核取方塊。

   b. 輸入 **AmazonSSMDirectoryServiceAccess**。然後選取清單中相應項目的核取方塊。

   c. 輸入 **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read** 或您在上一個程序中建立的 IAM 政策名稱。然後選取清單中相應項目的核取方塊。

   d. 新增上述三個政策後，選取建立角色。

   > **Note**
   >
   > AmazonSSMDirectoryServiceAccess 提供將執行個體加入 Active Directory受管 的許可 AWS Directory Service。AmazonSSMManagedInstanceCore 提供使用 AWS Systems Manager 服務所需的最低許可。有關建立具有這些許可的角色的更多資訊，以及有關可以指派給 IAM 角色的其他許可和政策的資訊，請參閱《AWS Systems Manager 使用者指南》中的為 Systems Manager 建立 IAM 執行個體設定檔一節。

7. 在角色名稱欄位中輸入新角色的名稱，例如 **LinuxEC2DomainJoin**或您偏好的另一個名稱。

8. (選用) 針對 Role description (角色描述)，輸入描述。
9. （選用）選擇步驟 3：新增標籤以新增標籤下的新增標籤。標籤鍵值對用於組織、追蹤或控制此角色的存取。
10. 選擇建立角色。

無縫加入您的 Linux 執行個體

無縫加入您的 Linux 執行個體

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/ec2/ ：// 開啟 Amazon EC2 主控台。
2. 從導覽列的區域選擇器中，選擇 AWS 區域 與現有目錄相同的 。
3. 在 EC2 儀表板的啟動執行個體區段中，選擇啟動執行個體。
4. 在啟動執行個體頁面的名稱和標籤區段下，輸入您要用於 Linux EC2 執行個體的名稱。
5. （選用）選擇新增其他標籤以新增一或多個標籤鍵值對，以組織、追蹤或控制此 EC2 執行個體的存取。
6. 在應用程式和作業系統映像 (Amazon Machine Image) 區段中，選擇您要啟動的 Linux AMI。

> **Note**
>
> 使用的 AMI 必須具有 AWS Systems Manager (SSM Agent) 2.3.1644.0 版或更新版本。若要透過從 AMI 啟動執行個體來檢查 AMI 中已安裝的 SSM 代理程式版本，請參閱取得目前安裝的 SSM 代理程式版本。如需升級 SSM 代理程式，請參閱在適用於 Linux 的 EC2 執行個體上安裝和設定 SSM 代理程式。
>
> 將 Linux 執行個體加入Active Directory網域時，SSM 會使用 `aws:domainJoin` 外掛程式。外掛程式會將 Linux 執行個體的主機名稱變更為 EC2AMAZ-*XXXXXXX* 格式。如需 的詳細資訊`aws:domainJoin`，請參閱AWS Systems Manager 《 使用者指南》中的AWS Systems Manager 命令文件外掛程式參考。

7. 在執行個體類型區段中，從執行個體類型下拉式清單中選擇您要使用的執行個體類型。
8. 在金鑰對 (登入) 區段中，您可以選擇建立新金鑰對或從現有金鑰對中進行選擇。若要建立新的金鑰對，請選擇建立新金鑰對。輸入金鑰對的名稱，然後選取金鑰對類型和私有金鑰檔案格式的選項。若要將私有金鑰儲存為可與 OpenSSH 搭配使用的格式，請選擇 .pem。若要將私有金鑰儲存為可與 PuTTY 搭配使用的格式，請選擇 .ppk。選擇建立金鑰對。您的瀏覽器會自動下載私有金鑰檔案。將私有金鑰檔案存放在安全的地方。

> **Important**
>
> 這是您儲存私有金鑰檔案的唯一機會。

9. 在啟動執行個體頁面上的網路設定區段下，選擇編輯。從 VPC – required 下拉式清單中選擇在其中建立目錄的 VPC。
10. 從子網路下拉式清單中選擇 VPC 中的公有子網路之一。您所選取的子網路必須將所有外部流量路由到網際網路閘道。如果沒有，則將無法從遠端連線到執行個體。

    如需有關連線至網際網路閘道的詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用網際網路閘道連線至網際網路一節。
11. 在自動指派公有 IP 下，選擇啟用。

    如需公有和私有 IP 定址的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 執行個體 IP 定址。 Amazon EC2
12. 對於防火牆 (安全群組)設定，您可以使用預設設定或根據需要進行變更。
13. 對於設定儲存設定，您可以使用預設設定或根據需要進行變更。
14. 選取進階詳細資訊區段，從域加入目錄下拉式清單中選取域。

> **Note**
>
> 選擇網域加入目錄後，您可能會看到：
>
> 如果 EC2 啟動精靈識別具有非預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
>
> - 如果您先前已編輯 SSM 文件，且預期屬性，請選擇關閉並繼續啟動 EC2 執行個體，而不進行任何變更。
> - 選取此處的刪除現有 SSM 文件連結，以刪除 SSM 文件。這將允許建立具有正確屬性的 SSM 文件。當您啟動 EC2 執行個體時，系統會自動建立 SSM 文件。

15. 針對 IAM 執行個體描述檔，選擇您先前在先決條件區段 步驟 2：建立 LinuxEC2DomainJoin 角色中建立的 IAM 角色。
16. 選擇啟動執行個體。

> **Note**
>
> 如果您使用 SUSE Linux 執行無縫域加入，則需要重新啟動才能進行身分驗證。若要從 Linux 終端重新啟動 SUSE，請鍵入 sudo reboot。

將 Amazon EC2 Linux 執行個體無縫加入共用的 AWS Managed Microsoft AD

在此程序中，您將順暢地將 Amazon EC2 Linux 執行個體加入共用的 AWS Managed Microsoft AD。若要這樣做，您將在想要啟動 EC2 Linux AWS Secrets Manager 執行個體的帳戶中的 EC2 執行個體角色中建立 IAM 讀取政策。這將在此程序`Account 2`中稱為 。此執行個體將使用從另一個帳戶共用的 AWS Managed Microsoft AD，稱為 `Account 1`。

先決條件

您必須先完成下列動作，才能將 Amazon EC2 Linux 執行個體無縫加入共用的 AWS Managed Microsoft AD：

- 教學課程中的步驟 1 到 3。 教學課程：共用 AWS Managed Microsoft AD 目錄以實現無縫 EC2 加入網域本教學課程會逐步引導您設定網路和共用 AWS Managed Microsoft AD。
- 中所述的程序將 Amazon EC2 Linux 執行個體無縫加入 AWS Managed Microsoft AD Active Directory。

步驟 1. 在帳戶 2 中建立 LinuxEC2DomainJoin 角色

在此步驟中，您將使用 IAM 主控台來建立 IAM 角色，用於在登入 時加入 EC2 Linux 執行個體的網域`Account 2`。

建立 LinuxEC2DomainJoin 角色

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在左側導覽窗格的存取管理下，選擇角色。
3. 在 Roles (角色) 頁面上，選擇 Create role (建立角色)。
4. 在 Select type of trusted entity (選擇可信任執行個體類型) 下，選擇 AWS service (服務)。
5. 在使用案例下，選擇 EC2，然後選擇下一步
6. 對於篩選政策，請執行下列操作：

    a. 輸入 `AmazonSSMManagedInstanceCore`。然後選取清單中該項目的核取方塊。

b. 輸入 AmazonSSMDirectoryServiceAccess。然後選取清單中該項目的核取方塊。

c. 新增這些政策之後，請選取建立角色。

> **Note**
>
> AmazonSSMDirectoryServiceAccess 提供將執行個體加入 Active Directory受管 的許可 AWS Directory Service。 AmazonSSMManagedInstanceCore提供使用所需的最低許可 AWS Systems Manager。如需使用這些許可建立角色的詳細資訊，以及您可以指派給 IAM 角色的其他許可和政策的相關資訊，請參閱AWS Systems Manager 《 使用者指南》中的設定 Systems Manager 所需的執行個體許可。

7. 在角色名稱欄位中輸入新角色的名稱，例如 LinuxEC2DomainJoin或您偏好的另一個名稱。
8. （選用）針對角色描述，輸入描述。
9. （選用）選擇步驟 3：新增標籤以新增標籤下的新增標籤。標籤鍵值對用於組織、追蹤或控制此角色的存取。
10. 選擇建立角色。

步驟 2. 建立跨帳戶資源存取權以共用 AWS Secrets Manager 秘密

下一節是無縫加入 EC2 Linux 執行個體與共用 AWS Managed Microsoft AD 所需的其他需求。這些要求包括建立資源政策，並將其連接到適當的 服務和資源。

若要允許帳戶中的使用者存取另一個帳戶中的 AWS Secrets Manager 秘密，您必須在資源政策和身分政策中允許存取。這種類型的存取稱為跨帳戶資源存取。

這種存取類型不同於將存取權授予與 Secrets Manager 秘密相同帳戶中的身分。您還必須允許身分使用秘密加密所用的 AWS Key Management Service(KMS) 金鑰。此許可是必要的，因為您無法使用 AWS 受管金鑰 (aws/secretsmanager) 進行跨帳戶存取。反之，您會使用您建立的 KMS 金鑰來加密秘密，然後將金鑰政策連接至該金鑰。若要變更秘密的加密金鑰，請參閱修改 AWS Secrets Manager 秘密。

> **Note**
>
> 根據您使用的秘密 AWS Secrets Manager，會產生相關費用。如需目前完整定價清單，請參閱 AWS Secrets Manager 定價。您可以使用 Secrets Manager 建立 AWS 受管金鑰 aws/secretsmanager的 免費加密秘密。如果您建立自己的 KMS 金鑰來加密秘密， 會以目前的

AWS KMS 費率向您 AWS 收費。如需詳細資訊，請參閱AWS Key Management Service 定價。

下列步驟可讓您建立資源政策，讓使用者將 EC2 Linux 執行個體無縫加入共用的 AWS Managed Microsoft AD。

將資源政策連接至帳戶 1 中的秘密

1. 前往以下位置開啟機密管理員控制台：https://console.aws.amazon.com/secretsmanager/。
2. 從秘密清單中，選擇您在 期間建立的秘密先決條件。
3. 在秘密的詳細資訊頁面的概觀索引標籤下，向下捲動至資源許可。
4. 選取編輯許可。
   - 在政策欄位中，輸入下列政策。下列政策允許 中的 LinuxEC2DomainJoin Account 2存取 中的秘密Account 1。將 ARN 值取代為您在步驟 1 中建立的 Account 2LinuxEC2DomainJoin角色的 ARN 值。若要使用此政策，請參閱將許可政策連接至 AWS Secrets Manager 秘密。

     JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/LinuxEC2DomainJoin"
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*"
    }
  ]
}
```

將陳述式新增至帳戶 1 中 KMS 金鑰的金鑰政策

1. 前往以下位置開啟機密管理員控制台：https://console.aws.amazon.com/secretsmanager/。
2. 在左側導覽窗格中，選取客戶受管金鑰。
3. 在客戶受管金鑰頁面上，選取您建立的金鑰。
4. 在金鑰詳細資訊頁面上，導覽至金鑰政策，然後選取編輯。
5. 下列金鑰政策陳述式允許 ApplicationRole 中的 Account 2使用 中的 KMS 金鑰Account 1來解密 中的秘密Account 1。若要使用此陳述式，請將其新增至 KMS 金鑰的金鑰政策。如需詳細資訊，請參閱變更金鑰政策。

```
{
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::Account2:role/ApplicationRole"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

為帳戶 2 中的身分建立身分政策

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在左側導覽窗格的存取管理下，選取政策。
3. 選取 Create Policy (建立政策)。在政策編輯器中選擇 JSON。
4. 下列政策允許 ApplicationRole中的 Account 2存取秘密，Account 1並使用 中的加密金鑰解密秘密值Account 1。您可以在 Secret ARN 下秘密詳細資訊頁面的 Secrets Manager 主控台中找到秘密的 ARN。或者，您可以呼叫 describe-secret 來識別秘密的 ARN。將資源 ARN 取代為秘密 ARN 和 的資源 ARNAccount 1。若要使用此政策，請參閱將許可政策連接至 AWS Secrets Manager 秘密。

   JSON

```
{
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:secretName-AbCdEf"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:Describekey"
      ],
      "Resource": "arn:aws:kms:us-
east-1:111122223333:key/Your_Encryption_Key"
    }
  ]
```

5. 選取下一步，然後選取儲存變更。
6. 尋找並選取您在 Account 2中建立的角色Attach a resource policy to the secret in Account 1。
7. 在新增許可下，選取連接政策。
8. 在搜尋列中，尋找您在 中建立的政策Add a statement to the key policy for the KMS key in Account 1，然後選取將政策新增至角色的方塊。然後選取新增許可。

步驟 3。無縫加入您的 Linux 執行個體

您現在可以使用下列程序，將 EC2 Linux 執行個體無縫加入共用的 AWS Managed Microsoft AD。

無縫加入您的 Linux 執行個體

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/ec2/ ：// 開啟 Amazon EC2 主控台。
2. 從導覽列的區域選擇器中，選擇 AWS 區域 與現有目錄相同的 。
3. 在 EC2 儀表板的啟動執行個體區段中，選擇啟動執行個體。
4. 在啟動執行個體頁面的名稱和標籤區段下，輸入您要用於 Linux EC2 執行個體的名稱。

5. （選用）選擇新增其他標籤以新增一或多個標籤鍵值對，以組織、追蹤或控制此 EC2 執行個體的存取。
6. 在應用程式和作業系統映像 (Amazon Machine Image) 區段中，選擇您要啟動的 Linux AMI。

> **Note**
>
> 使用的 AMI 必須具有 AWS Systems Manager (SSM Agent) 2.3.1644.0 版或更新版本。若要透過從 AMI 啟動執行個體來檢查 AMI 中已安裝的 SSM 代理程式版本，請參閱取得目前安裝的 SSM 代理程式版本。如需升級 SSM 代理程式，請參閱在適用於 Linux 的 EC2 執行個體上安裝和設定 SSM 代理程式。
> SSM 在將 Linux 執行個體加入Active Directory網域時使用 `aws:domainJoin` 外掛程式。外掛程式會將 Linux 執行個體的主機名稱變更為 EC2AMAZ-*XXXXXXX* 格式。如需 的詳細資訊`aws:domainJoin`，請參閱AWS Systems Manager 《 使用者指南》中的AWS Systems Manager 命令文件外掛程式參考。

7. 在執行個體類型區段中，從執行個體類型下拉式清單中選擇您要使用的執行個體類型。
8. 在金鑰對 (登入) 區段中，您可以選擇建立新金鑰對或從現有金鑰對中進行選擇。若要建立新的金鑰對，請選擇建立新金鑰對。輸入金鑰對的名稱，然後選取金鑰對類型和私有金鑰檔案格式的選項。若要將私有金鑰儲存為可與 OpenSSH 搭配使用的格式，請選擇 .pem。若要將私有金鑰儲存為可與 PuTTY 搭配使用的格式，請選擇 .ppk。選擇建立金鑰對。您的瀏覽器會自動下載私有金鑰檔案。將私有金鑰檔案存放在安全的地方。

> **Important**
>
> 這是您儲存私有金鑰檔案的唯一機會。

9. 在啟動執行個體頁面上的網路設定區段下，選擇編輯。從 VPC – required 下拉式清單中選擇在其中建立目錄的 VPC。
10. 從子網路下拉式清單中選擇 VPC 中的公有子網路之一。您所選取的子網路必須將所有外部流量路由到網際網路閘道。如果沒有，則將無法從遠端連線到執行個體。

    如需有關連線至網際網路閘道的詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用網際網路閘道連線至網際網路一節。
11. 在自動指派公有 IP 下，選擇啟用。

    如需公有和私有 IP 定址的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 執行個體 IP 定址。 Amazon EC2

12. 對於防火牆 (安全群組)設定，您可以使用預設設定或根據需要進行變更。
13. 對於設定儲存設定，您可以使用預設設定或根據需要進行變更。
14. 選取進階詳細資訊區段，從域加入目錄下拉式清單中選取域。

> **Note**
>
> 選擇網域加入目錄後，您可能會看到：
>
> 如果 EC2 啟動精靈識別具有非預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
>
> - 如果您先前已編輯 SSM 文件，且預期屬性，請選擇關閉並繼續啟動 EC2 執行個體，而不進行任何變更。
> - 選取此處的刪除現有 SSM 文件連結，以刪除 SSM 文件。這將允許建立具有正確屬性的 SSM 文件。當您啟動 EC2 執行個體時，系統會自動建立 SSM 文件。

15. 針對 IAM 執行個體描述檔，選擇您先前在先決條件區段步驟 2：建立 LinuxEC2DomainJoin 角色中建立的 IAM 角色。
16. 選擇啟動執行個體。

> **Note**
>
> 如果您使用 SUSE Linux 執行無縫域加入，則需要重新啟動才能進行身分驗證。若要從 Linux 終端重新啟動 SUSE，請鍵入 sudo reboot。

手動將 Amazon EC2 Linux 執行個體加入 AWS Managed Microsoft AD Active Directory

除了 Amazon EC2 Windows執行個體之外，您也可以將特定 Amazon EC2 Linux 執行個體加入 AWS Managed Microsoft ADActive Directory。系統支援下列 Linux 執行個體分佈和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 位元 x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64 位元 x86)
- Ubuntu Server 18.04 LTS 及 Ubuntu Server 16.04 LTS

- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> 其他 Linux 分佈和版本也許能正常運作，但尚未經過測試。

將 Linux 執行個體加入 AWS Managed Microsoft AD

在將 Amazon Linux、CentOS、Red Hat 或 Ubuntu 執行個體加入目錄之前，必須先依照 無縫加入您的 Linux 執行個體 中的指定啟動執行個體。

> **Important**
>
> 以下某些程序若未正確執行，可能會導致您的執行個體無法連線或無法使用。因此，我們強烈建議您在執行這些程序之前，對您的執行個體進行備份或擷取快照。

將 Linux 執行個體加入您的目錄

使用以下其中一個標籤，依照您的特定 Linux 執行個體的步驟：

Amazon Linux

1. 使用任何 SSH 用戶端連線到執行個體。
2. 設定 Linux 執行個體以使用 AWS Directory Service所提供 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動進行設定，請參閱 AWS 知識中心的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，了解為特定 Linux 分佈和版本設定持久性 DNS 伺服器的方式。
3. 請確定您的 Amazon Linux - 64 位元執行個體處於最新狀態。

   ```
   sudo yum -y update
   ```

4. 在您的 Linux 執行個體上安裝所需的 Amazon Linux 套件。

> **Note**
>
> 系統可能已安裝其中一些套裝服務。
> 在安裝套件時，可能會出現好幾個跳出式設定畫面。您通常可以將這些畫面中的欄位留白。

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> 如需協助確定您所使用的 Amazon Linux 版本，請參閱 《Amazon EC2 Linux 執行個體使用者指南》中的識別 Amazon Linux 映像。

5. 使用下列命令將執行個體加入目錄。

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

example.com 域中具備域加入權限的帳戶。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
...
 * Successfully enrolled machine in realm
```

6. 設定 SSH 服務以允許密碼身分驗證。

   a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. 將 PasswordAuthentication 設定設為 yes。

```
PasswordAuthentication yes
```

c. 重新啟動 SSH 服務。

```
sudo systemctl restart sshd.service
```

或使用：

```
sudo service sshd restart
```

7. 執行個體重新啟動後，請透過任何 SSH AWS 用戶端與其連線，並執行下列步驟，將委派管理員群組新增至 sudoers 清單：

a. 使用下列命令開啟 `sudoers` 檔案：

```
sudo visudo
```

b. 在 `sudoers` 檔案的底部加入下列程式碼，然後儲存檔案。

```
## Add the "AWS Delegated Administrators" group from the example.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(上述範例使用 "\<space>" 來建立 Linux 空白字元。)

CentOS

1. 使用任何 SSH 用戶端連線到執行個體。
2. 設定 Linux 執行個體以使用 AWS Directory Service所提供 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動進行設定，請參閱 AWS 知識中心的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，了解為特定 Linux 分佈和版本設定持久性 DNS 伺服器的方式。
3. 請確定您的 CentOS 7 執行個體處於最新狀態。

```
sudo yum -y update
```

4. 在您的 CentOS 7 執行個體上安裝必要的套裝服務。

> **Note**
>
> 系統可能已安裝其中一些套裝服務。
> 在安裝套件時，可能會出現好幾個跳出式設定畫面。您通常可以將這些畫面中的欄位留白。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 使用下列命令將執行個體加入目錄。

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

example.com 域中具備域加入權限的帳戶。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
...
 * Successfully enrolled machine in realm
```

6. 設定 SSH 服務以允許密碼身分驗證。

   a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. 將 PasswordAuthentication 設定設為 yes。

   ```
   PasswordAuthentication yes
   ```

   c. 重新啟動 SSH 服務。

   ```
   sudo systemctl restart sshd.service
   ```

   或使用：

```
sudo service sshd restart
```

7. 執行個體重新啟動後，請透過任何 SSH AWS 用戶端與其連線，並執行下列步驟，將委派管理員群組新增至 sudoers 清單：

   a. 使用下列命令開啟 sudoers 檔案：

   ```
   sudo visudo
   ```

   b. 在 sudoers 檔案的底部加入下列程式碼，然後儲存檔案。

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (上述範例使用 "\<space>" 來建立 Linux 空白字元。)

Red Hat

1. 使用任何 SSH 用戶端連線到執行個體。
2. 設定 Linux 執行個體以使用 AWS Directory Service所提供 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動進行設定，請參閱 AWS 知識中心的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，了解為特定 Linux 分佈和版本設定持久性 DNS 伺服器的方式。
3. 確定 Red Hat 64 位元執行個體是最新版本。

   ```
   sudo yum -y update
   ```

4. 在您的 Linux 執行個體上，安裝必要的 Red Hat 套件。

   > **Note**
   >
   > 系統可能已安裝其中一些套裝服務。
   > 在安裝套件時，可能會出現好幾個跳出式設定畫面。您通常可以將這些畫面中的欄位留白。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 使用下列命令將執行個體加入目錄。

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

在 *example.com* 域中帳戶的 sAMAccountName 具備域加入權限。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
...
 * Successfully enrolled machine in realm
```

6. 設定 SSH 服務以允許密碼身分驗證。
   a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

```
sudo vi /etc/ssh/sshd_config
```

   b. 將 PasswordAuthentication 設定設為 yes。

```
PasswordAuthentication yes
```

   c. 重新啟動 SSH 服務。

```
sudo systemctl restart sshd.service
```

   或使用：

```
sudo service sshd restart
```

7. 執行個體重新啟動後，請透過任何 SSH AWS 用戶端與其連線，並執行下列步驟，將委派管理員群組新增至 sudoers 清單：
   a. 使用下列命令開啟 sudoers 檔案：

```
sudo visudo
```

b. 在 sudoers 檔案的底部加入下列程式碼，然後儲存檔案。

```
## Add the "AWS Delegated Administrators" group from the example.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(上述範例使用 "\<space>" 來建立 Linux 空白字元。)

SUSE

1. 使用任何 SSH 用戶端連線到執行個體。
2. 設定 Linux 執行個體，讓其得以使用 AWS Directory Service所提供之 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動設定，請參閱 AWS 知識中心中的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，以取得為特定 Linux 發行版本設定持久性 DNS 伺服器的指引。
3. 請確定您的 SUSE Linux 15 執行個體處於最新狀態。
   a. 連接套件儲存庫。

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

   b. 更新 SUSE。

```
sudo zypper update -y
```

4. 在您的 Linux 執行個體上安裝所需的 SUSE Linux 15 套件。

> **Note**
>
> 系統可能已安裝其中一些套裝服務。
> 在安裝套件時，可能會出現好幾個跳出式設定畫面。您通常可以將這些畫面中的欄位留白。

```
sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-
client
```

5. 使用下列命令將執行個體加入目錄。

```
sudo realm join -U join_account example.com --verbose
```

join_account

在 *example.com* 網域的 sAMAccountName 具備網域加入權限。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
…
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

請注意，以下兩者都是預期會發生的傳回項目。

```
! Couldn't authenticate with keytab while discovering which salt to use:
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. 手動啟用 PAM 中的 SSSD。

```
sudo pam-config --add --sss
```

7. 編輯 nsswitch.conf 以在 nsswitch.conf 中啟用 SSSD

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss
group:  compat sss
shadow: compat sss
```

8. 將以下資料行新增到 /etc/pam.d/common-session ，以便在初始登入時自動建立主目錄

```
sudo vi /etc/pam.d/common-session
```

```
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

9. 重新啟動執行個體以完成加入網域的程序。

```
sudo reboot
```

10.使用任何 SSH 用戶端重新連線至執行個體，以確認域加入已成功完成並完成其他步驟。

a. 確認執行個體已在網域上註冊

```
sudo realm list
```

```
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: adcli
  required-package: samba-client
  login-formats: %U@example.com
  login-policy: allow-realm-logins
```

b. 驗證 SSSD 精靈的狀態

```
systemctl status sssd
```

```
sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor
 preset: disabled)
   Active: active (running) since Wed 2020-04-15 16:22:32 UTC; 3min 49s ago
 Main PID: 479 (sssd)
    Tasks: 4
   CGroup: /system.slice/sssd.service
           ##479 /usr/sbin/sssd -i --logger=files
```

```
            ##505 /usr/lib/sssd/sssd_be --domain example.com --uid 0 --gid 0 --
logger=files
            ##548 /usr/lib/sssd/sssd_nss --uid 0 --gid 0 --logger=files
            ##549 /usr/lib/sssd/sssd_pam --uid 0 --gid 0 --logger=files
```

11.允許使用者透過 SSH 和主控台存取

```
sudo realm permit join_account@example.com
```

允許透過 SSH 和主控台存取網域群組

```
sudo realm permit -g 'AWS Delegated Administrators'
```

或者允許所有使用者存取

```
sudo realm permit --all
```

12設定 SSH 服務以允許密碼身分驗證。

a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

```
sudo vi /etc/ssh/sshd_config
```

b. 將 PasswordAuthentication 設定設為 yes。

```
PasswordAuthentication yes
```

c. 重新啟動 SSH 服務。

```
sudo systemctl restart sshd.service
```

或使用：

```
sudo service sshd restart
```

13.13. 執行個體重新啟動後，請透過任何 SSH AWS 用戶端與其連線，並執行下列步驟，將委派管理員群組新增至 sudoers 清單：

a. 使用下列命令開啟 sudoers 檔案：

```
sudo visudo
```

b. 在 sudoers 檔案的底部加入下列程式碼，然後儲存檔案。

```
## Add the "Domain Admins" group from the awsad.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
```

Ubuntu

1. 使用任何 SSH 用戶端連線到執行個體。
2. 設定 Linux 執行個體以使用 AWS Directory Service所提供 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動進行設定，請參閱 AWS 知識中心的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，了解為特定 Linux 分佈和版本設定持久性 DNS 伺服器的方式。
3. 確定 Ubuntu 64 位元執行個體是最新版本。

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. 在您的 Linux 執行個體上，安裝必要的 Ubuntu 套件。

> **Note**
>
> 系統可能已安裝其中一些套裝服務。
> 在安裝套件時，可能會出現好幾個跳出式設定畫面。您通常可以將這些畫面中的欄位留白。

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. 停用反向 DNS 解析，並將預設領域設定為網域的 FQDN。Ubuntu 執行個體在 DNS 中必須能夠反向解析，領域才能使用。否則，您必須依照下列步驟，停用在 /etc/krb5.conf 中的反向 DNS：

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
```

```
rdns = false
```

6. 使用下列命令將執行個體加入目錄。

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

在 *example.com* 域中帳戶的 sAMAccountName 具備域加入權限。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
...
 * Successfully enrolled machine in realm
```

7. 設定 SSH 服務以允許密碼身分驗證。

a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

```
sudo vi /etc/ssh/sshd_config
```

b. 將 PasswordAuthentication 設定設為 yes。

```
PasswordAuthentication yes
```

c. 重新啟動 SSH 服務。

```
sudo systemctl restart sshd.service
```

或使用：

```
sudo service sshd restart
```

8. 執行個體重新啟動後，請透過任何 SSH AWS 用戶端與其連線，並執行下列步驟，將委派管理員群組新增至 sudoers 清單：

a. 使用下列命令開啟 sudoers 檔案：

```
sudo visudo
```

b. 在 sudoers 檔案的底部加入下列程式碼，然後儲存檔案。

```
## Add the "AWS Delegated Administrators" group from the example.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(上述範例使用 "\<space>" 來建立 Linux 空白字元。)

限制帳戶登入存取

由於在 Active Directory 中定義了所有帳戶，因此目錄中的所有使用者預設可登入該執行個體。您可以在 sssd.conf 中使用 ad_access_filter 只允許特定使用者登入執行個體。例如：

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

表示唯有使用者是特定群組的成員時，才可以存取執行個體。

cn

應該具備存取權的群組通用名稱。在此範例中，群組名稱為 *admins*。

ou

這代表上述群組所在的組織單位。在此範例中，OU 為 *Testou*。

dc

這代表網域的網域元件。在此範例中為 *example*。

dc

這代表額外的網域元件。在此範例中為 *com*。

您必須將 ad_access_filter 手動新增至 /etc/sssd/sssd.conf。

在文字編輯器中開啟 /etc/sssd/sssd.conf 檔案。

```
sudo vi /etc/sssd/sssd.conf
```

執行此動作後，您的 sssd.conf 可能如下所示：

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

您需要重新啟動 sssd 服務，才能使設定生效：

```
sudo systemctl restart sssd.service
```

或者，您可以使用：

```
sudo service sssd restart
```

由於在 Active Directory 中定義了所有帳戶，因此目錄中的所有使用者預設可登入該執行個體。您可以在 sssd.conf 中使用 ad_access_filter 只允許特定使用者登入執行個體。

例如：

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

表示唯有使用者是特定群組的成員時，才可以存取執行個體。

cn

應該具備存取權的群組通用名稱。在此範例中，群組名稱為 *admins*。

ou

這代表上述群組所在的組織單位。在此範例中，OU 為 *Testou*。

dc

這代表網域的網域元件。在此範例中為 *example*。

dc

這代表額外的網域元件。在此範例中為 *com*。

您必須將 ad_access_filter 手動新增至 /etc/sssd/sssd.conf。

1. 在文字編輯器中開啟 /etc/sssd/sssd.conf 檔案。

```
sudo vi /etc/sssd/sssd.conf
```

2. 執行此動作後，您的 sssd.conf 可能如下所示：

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

3. 您需要重新啟動 sssd 服務，才能使設定生效：

```
sudo systemctl restart sssd.service
```

或者，您可以使用：

```
sudo service sssd restart
```

ID 映射

ID 映射可以透過兩種方法執行，以維護 UNIX/Linux 使用者識別符 (UID) 和群組識別符 (GID) 以及 Windows 和Active Directory安全識別符 (SID) 身分之間的統一體驗。這些方法是：

1. 集中
2. 分散式

> **Note**
>
> 中的集中式使用者身分映射Active Directory需要可攜式作業系統界面或 POSIX。

集中式使用者身分映射

Active Directory 或其他輕量型目錄存取通訊協定 (LDAP) 服務為 Linux 使用者提供 UID 和 GID。在 中 Active Directory，如果已設定 POSIX 延伸，這些識別符會存放在使用者的屬性中：

- UID - Linux 使用者名稱 （ 字串 ）
- UID 號碼 - Linux 使用者 ID 號碼 （ 整數 ）
- GID 號碼 - Linux 群組 ID 號碼 （ 整數 ）

若要將 Linux 執行個體設定為使用來自 的 UID 和 GIDActive Directory，`ldap_id_mapping = False`請在 sssd.conf 檔案中設定 。在設定此值之前，請確認您已將 UID、UID 號碼和 GID 號碼新增至 中的使用者和群組Active Directory。

分散式使用者身分映射

如果 Active Directory沒有 POSIX 擴充功能，或者如果您選擇不集中管理身分映射，Linux 可以計算 UID 和 GID 值。Linux 使用使用者的唯一安全識別符 (SID) 來維持一致性。

若要設定分散式使用者 ID 映射，`ldap_id_mapping = True`請在 sssd.conf 檔案中設定 。

常見問題

如果您設定 `ldap_id_mapping = False`，有時啟動 SSSD 服務將會失敗。此失敗的原因是因為不支援變更 UIDs。當您從 ID 映射變更為 POSIX 屬性，或從 POSIX 屬性變更為 ID 映射時，我們建議您刪除 SSSD 快取。如需 ID 映射和 ldap_id_mapping 參數的進一步詳細資訊，請參閱 Linux 命令列中的 sssd-ldap(8) man 頁面。

連線至 Linux 執行個體

當使用者使用 SSH 用戶端連線到執行個體時，系統會提示其輸入使用者名稱。如果使用者想輸入使用者名稱，可以善用 `username@example.com` 或 `EXAMPLE\username` 格式。視您使用的 Linux 發行版本而定，回應會如下所示：

Amazon Linux、Red Hat Enterprise Linux 及 CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
```

```
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

使用 Winbind 手動將 Amazon EC2 Linux 執行個體加入 AWS Managed Microsoft AD Active Directory

您可以使用 Winbind 服務，將 Amazon EC2 Linux 執行個體手動加入 AWS Managed Microsoft AD Active Directory 網域。這可讓您現有的內部部署 Active Directory 使用者在存取加入 AWS Managed Microsoft AD Active Directory 的 Linux 執行個體時，使用其 Active Directory 登入資料。系統支援下列 Linux 執行個體分佈和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 位元 x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64 位元 x86)
- Ubuntu Server 18.04 LTS 及 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> 其他 Linux 分佈和版本也許能正常運作，但尚未經過測試。

將 Linux 執行個體加入 AWS Managed Microsoft AD Active Directory

> **Important**
>
> 以下某些程序若未正確執行，可能會導致您的執行個體無法連線或無法使用。因此，我們強烈建議您在執行這些程序之前，對您的執行個體進行備份或擷取快照。

將 Linux 執行個體加入您的目錄

使用以下其中一個標籤，依照您的特定 Linux 執行個體的步驟：

Amazon Linux/CENTOS/REDHAT

1. 使用任何 SSH 用戶端連線到執行個體。
2. 設定 Linux 執行個體，讓其得以使用 AWS Directory Service所提供之 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動設定，請參閱 AWS 知識中心中的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，以取得為特定 Linux 發行版本設定持久性 DNS 伺服器的指引。
3. 請確定您的 Linux 執行個體處於最新狀態。

```
sudo yum -y update
```

4. 在您的 Linux 執行個體上安裝必要的 Samba / Winbind 套裝服務。

```
sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-
clients
```

5. 備份主 smb.conf 檔案，以便在發生任何故障時可以恢復：

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. 在文字編輯器中開啟原始組態檔案 [/etc/samba/smb.conf] 。

```
sudo vim /etc/samba/smb.conf
```

填寫您的 Active Directory 網域環境資訊，如以下範例所示：

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
```

```
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. 在文字編輯器中開啟 [/etc/hosts] 檔案。

```
sudo vim /etc/hosts
```

新增 Linux 執行個體私有 IP 地址，如下所示：

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> 如果您未在 /etc/hosts 檔案中指定 IP 地址，則在將執行個體加入域時可能會收到下列 DNS 錯誤：
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> 此錯誤表示加入成功，但 [net ads] 命令無法在 DNS 中登錄 DNS 記錄。

8. 使用 net 公用程式將 Linux 執行個體加入 Active Directory。

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

example.com 域中具備域加入權限的帳戶。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. 修改 PAM 組態檔案，使用以下命令新增 winbind 身分驗證所需的項目：

```
sudo authconfig --enablewinbind --enablewinbindauth  --enablemkhomedir   --update
```

10透過編輯 /etc/ssh/sshd_config 檔案，設定 SSH 服務以允許密碼身分驗證。

a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

```
sudo vi /etc/ssh/sshd_config
```

b. 將 PasswordAuthentication 設定設為 yes。

```
PasswordAuthentication yes
```

c. 重新啟動 SSH 服務。

```
sudo systemctl restart sshd.service
```

或使用：

```
sudo service sshd restart
```

11重新啟動執行個體之後，請執行下列步驟，以使用任何 SSH 用戶端連線到該執行個體，並將域使用者或群組的根權限新增至 sudoers 清單：

a. 使用下列命令開啟 sudoers 檔案：

```
sudo visudo
```

b. 從信任或受信任域中新增所需群組或使用者，如下所示，然後儲存。

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(上述範例使用 "\<space>" 來建立 Linux 空白字元。)

SUSE

1. 使用任何 SSH 用戶端連線到執行個體。

2. 設定 Linux 執行個體，讓其得以使用 AWS Directory Service所提供之 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動設定，請參閱 AWS 知識中心中的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，以取得為特定 Linux 發行版本設定持久性 DNS 伺服器的指引。
3. 請確定您的 SUSE Linux 15 執行個體處於最新狀態。

   a. 連接套件儲存庫。

   ```
   sudo SUSEConnect -p PackageHub/15.1/x86_64
   ```

   b. 更新 SUSE。

   ```
   sudo zypper update -y
   ```

4. 在您的 Linux 執行個體上安裝必要的 Samba / Winbind 套裝服務。

   ```
   sudo zypper in -y samba samba-winbind
   ```

5. 備份主 smb.conf 檔案，以便在發生任何故障時可以恢復：

   ```
   sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
   ```

6. 在文字編輯器中開啟原始組態檔案 [/etc/samba/smb.conf] 。

   ```
   sudo vim /etc/samba/smb.conf
   ```

   填寫 Active Directory 域環境訊息，如下例所示：

   ```
   [global]
    workgroup = example
    security = ads
    realm = example.com
    idmap config * : rangesize = 1000000
    idmap config * : range = 1000000-19999999
    idmap config * : backend = autorid
    winbind enum users = no
    winbind enum groups = no
    template homedir = /home/%U@%D
    template shell = /bin/bash
    winbind use default domain = false
   ```

7. 在文字編輯器中開啟 [/etc/hosts] 檔案。

```
sudo vim /etc/hosts
```

新增 Linux 執行個體私有 IP 地址，如下所示：

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> 如果您未在 /etc/hosts 檔案中指定 IP 地址，則在將執行個體加入域時可能會收到下列 DNS 錯誤：
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> 此錯誤表示加入成功，但 [net ads] 命令無法在 DNS 中登錄 DNS 記錄。

8. 使用下列命令將 Linux 執行個體加入目錄。

```
sudo net ads join -U join_account@example.com
```

join_account

在 *example.com* 網域的 sAMAccountName 具備網域加入權限。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. 修改 PAM 組態檔案，使用以下命令新增 Winbind 身分驗證所需的項目：

```
sudo pam-config --add --winbind --mkhomedir
```

10.在文字編輯器中開啟名稱服務交換器組態檔案 [/etc/nsswitch.conf]。

```
vim /etc/nsswitch.conf
```

新增 Winbind 指令，如下所示。

```
passwd: files winbind
shadow: files winbind
group:  files winbind
```

11透過編輯 /etc/ssh/sshd_config 檔案，設定 SSH 服務以允許密碼身分驗證。

a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

```
sudo vim /etc/ssh/sshd_config
```

b. 將 PasswordAuthentication 設定設為 yes。

```
PasswordAuthentication yes
```

c. 重新啟動 SSH 服務。

```
sudo systemctl restart sshd.service
```

或使用：

```
sudo service sshd restart
```

12重新啟動執行個體之後，請執行下列步驟，以使用任何 SSH 用戶端連線到該執行個體，並將域使用者或群組的根權限新增至 sudoers 清單：

a. 使用下列命令開啟 sudoers 檔案：

```
sudo visudo
```

b. 從信任或受信任域中新增所需群組或使用者，如下所示，然後儲存。

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
```

```
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(上述範例使用 "\<space>" 來建立 Linux 空白字元。)

Ubuntu

1. 使用任何 SSH 用戶端連線到執行個體。
2. 設定 Linux 執行個體，讓其得以使用 AWS Directory Service所提供之 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動設定，請參閱 AWS 知識中心中的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，以取得為特定 Linux 發行版本設定持久性 DNS 伺服器的指引。
3. 請確定您的 Linux 執行個體處於最新狀態。

   ```
   sudo apt-get -y upgrade
   ```

4. 在您的 Linux 執行個體上安裝必要的 Samba / Winbind 套裝服務。

   ```
   sudo apt -y install samba winbind libnss-winbind libpam-winbind
   ```

5. 備份主 `smb.conf` 檔案，以便在發生任何故障時可以恢復。

   ```
   sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
   ```

6. 在文字編輯器中開啟原始組態檔案 [`/etc/samba/smb.conf`] 。

   ```
   sudo vim /etc/samba/smb.conf
   ```

   填寫 Active Directory 域環境訊息，如下例所示：

   ```
   [global]
    workgroup = example
    security = ads
    realm = example.com
    idmap config * : rangesize = 1000000
    idmap config * : range = 1000000-19999999
    idmap config * : backend = autorid
    winbind enum users = no
    winbind enum groups = no
   ```

```
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. 在文字編輯器中開啟 [/etc/hosts] 檔案。

```
sudo vim /etc/hosts
```

新增 Linux 執行個體私有 IP 地址，如下所示：

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> 如果您未在 /etc/hosts 檔案中指定 IP 地址，則在將執行個體加入域時可能會收到下列 DNS 錯誤：
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> 此錯誤表示加入成功，但 [net ads] 命令無法在 DNS 中登錄 DNS 記錄。

8. 使用 net 公用程式將 Linux 執行個體加入 Active Directory。

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

example.com 域中具備域加入權限的帳戶。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. 修改 PAM 組態檔案，使用以下命令新增 Winbind 身分驗證所需的項目：

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

10.在文字編輯器中開啟名稱服務交換器組態檔案 [/etc/nsswitch.conf]。

```
vim /etc/nsswitch.conf
```

新增 Winbind 指令，如下所示。

```
passwd: compat winbind
group:  compat winbind
shadow: compat winbind
```

11.透過編輯 /etc/ssh/sshd_config 檔案，設定 SSH 服務以允許密碼身分驗證。

a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

```
sudo vim /etc/ssh/sshd_config
```

b. 將 PasswordAuthentication 設定設為 yes。

```
PasswordAuthentication yes
```

c. 重新啟動 SSH 服務。

```
sudo systemctl restart sshd.service
```

或使用：

```
sudo service sshd restart
```

12.重新啟動執行個體之後，請執行下列步驟，以使用任何 SSH 用戶端連線到該執行個體，並將域使用者或群組的根權限新增至 sudoers 清單：

a. 使用下列命令開啟 sudoers 檔案：

```
sudo visudo
```

b. 從信任或受信任域中新增所需群組或使用者，如下所示，然後儲存。

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
```

```
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(上述範例使用 "\<space>" 來建立 Linux 空白字元。)

連線至 Linux 執行個體

當使用者使用 SSH 用戶端連線到執行個體時，系統會提示其輸入使用者名稱。如果使用者想輸入使用者名稱，可以善用 username@example.com 或 EXAMPLE\username 格式。視您使用的 Linux 發行版本而定，回應會如下所示：

Amazon Linux、Red Hat Enterprise Linux 及 CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020
```

```
System load:  0.01              Processes:           102
Usage of /:   18.6% of 7.69GB   Users logged in:     2
Memory usage: 16%               IP address for eth0: 10.24.34.1
Swap usage:   0%
```

將 Amazon EC2 Mac 執行個體加入您的 AWS Managed Microsoft AD Active Directory

此程序會將 Amazon EC2 Mac 執行個體手動加入您的 AWS Managed Microsoft AD Active Directory。

先決條件

- Amazon EC2 Mac 執行個體需要 Amazon EC2 專用主機。您必須配置專用主機，並在主機上啟動執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的啟動 Mac 執行個體。
- 建議您為 AWS Managed Microsoft AD Active Directory 建立 DHCP 選項集。這將允許 Amazon VPC 中的任何執行個體指向指定的網域和 DNS 伺服器，以解析其網域名稱。如需詳細資訊，請參閱建立或變更 AWS Managed Microsoft AD 的 DHCP 選項集。

> **Note**
>
> 專用主機定價會因您選擇的付款選項而有所不同。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的定價和帳單。

手動加入 Mac 執行個體

1. 使用下列 SSH 命令連線至 Mac 執行個體。如需連線至 Mac 執行個體的詳細資訊，請參閱連線至 Mac 執行個體。

   ```
   ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
   ```

2. 連線至 Mac 執行個體後，請使用下列命令建立 *ec2-user* 帳戶的密碼：

   ```
   sudo passwd ec2-user
   ```

3. 在命令列出現提示時，請提供 *ec2-user* 帳戶的密碼。您可以依照 Amazon EC2 使用者指南中的更新作業系統和軟體中的程序來更新作業系統和軟體。

4. 使用下列 *dsconfigad* 命令，將您的 Mac 執行個體加入 AWS Managed Microsoft AD Active Directory 網域。請務必將網域名稱、電腦名稱和組織單位取代為您的 AWS Managed Microsoft AD Active Directory 網域資訊。如需詳細資訊，請參閱 Apple 網站上的在 Mac 上的 Directory Utility 中設定網域存取。

   > **Warning**
   >
   > 電腦名稱不應包含連字號。Hyphens 可能會阻止 繫結至 AWS Managed Microsoft AD Active Directory。

   ```
   sudo dsconfigad -add domainName -computer computerName -username Username -
   ou "Your-AWS-Delegated-Organizational-Unit"
   ```

   下列範例是將名為 的 Mac 執行個體上的管理使用者加入**myec2mac01example.com**網域時，命令應該看起來的樣子：

   ```
   sudo dsconfigad -add example.com -computer myec2mac01 -username admin -
   ou "OU=Computers,OU=Example,DC=Example,DC=com"
   ```

5. 使用下列命令，將AWS 委派管理員新增至 Mac 執行個體上的管理使用者：

   ```
   sudo dsconfigad -group "EXAMPLE\aws delegated administrators
   ```

6. 使用下列命令來確認 AWS Managed Microsoft AD Active Directory 網域已成功加入：

   ```
   dsconfigad -show
   ```

您已成功將 Mac 執行個體加入 AWS Managed Microsoft AD Active Directory。您現在可以使用 AWS Managed Microsoft AD Active Directory 登入資料登入 Mac 執行個體。

當您第一次登入 Mac 執行個體時，應該會提供選項讓您以「其他」使用者身分登入。此時，您可以使用 Active Directory 網域登入資料來登入 Mac 執行個體。如果您在完成這些步驟後，未在登入畫面上收到「其他」，請以 ec2-user 身分登入，然後登出。

若要搭配網域使用者使用圖形使用者界面登入，請遵循 Amazon EC2 使用者指南中連線至執行個體的圖形使用者界面 (GUI) 中的步驟。

委派 AWS Managed Microsoft AD 的目錄聯結權限

若要將電腦加入 AWS Managed Microsoft AD，您需要具有將電腦加入目錄權限的帳戶。

使用 AWS Directory Service for Microsoft Active Directory，管理員和AWS 委派伺服器管理員群組的成員具有這些權限。

不過，最佳實務是您應該使用只有所需最低權限的帳戶。下列程序示範如何建立稱為 `Joiners` 的新群組，並將權限委派給需要將電腦加入目錄的這個群組。

您必須在已加入您的目錄，並已安裝 Active Directory User and Computers (Active Directory 使用者和電腦) MMC 嵌入的電腦上執行此程序。您也必須以網域管理員的身分登入。

委派 AWS Managed Microsoft AD 的加入權限

1. 開啟Active Directory使用者和電腦，然後選取導覽樹狀目錄中具有您 NetBIOS 名稱的組織單位 (OU)，然後選取使用者 OU。

   > **Important**
   >
   > 當您啟動 AWS Directory Service for Microsoft Active Directory 時， 會 AWS 建立組織單位 (OU)，其中包含您目錄的所有物件。此 OU 有您在建立目錄時所輸入的 NetBIOS 名稱，位於根網域中。網域根由 擁有和管理 AWS。您不能變更根網域本身；因此，您必須在具有您 NetBIOS 名稱的 OU 內建立 **`Joiners`** 群組。

2. 開啟 Users (使用者) 的內容選單 (按一下右鍵) 選單，選擇 New (新增)，然後選擇 Group (群組)。
3. 在 New Object - Group (新增物件 - 群組) 對話方塊中輸入如下內容，並選擇 OK (確定)。
   - 在 Group Name (群組名稱) 中，輸入 **`Joiners`**。
   - 針對 Group scope (群組範圍) 選擇 Global (全域)。
   - 針對 Group type (群組類型)，選擇 Security (安全性)。
4. 在導覽樹狀目錄中，選取您 NetBIOS 名稱下的 Computers (電腦) 容器。從 Action (動作) 選單，選擇 Delegate Control (委派控制)。
5. 在 Delegation of Control Wizard (委派控制精靈) 頁面，選擇 Next (下一步)，然後選擇 Add (新增)。
6. 在 Select Users, Computers, or Groups (選取使用者、電腦或群組) 對話方塊中輸入 `Joiners`，並選擇 OK (確定)。如果找到多個物件，請選取在上述步驟中建立的 `Joiners` 群組。選擇下一步。

7. 在 Tasks to Delegate (要委派的任務) 頁面上，選取 Create a custom task to delegate (建立要委派的自訂任務)，然後選擇 Next (下一步)。
8. 選取 Only the following objects in the folder (僅限資料夾中的下列物件)，然後選取 Computer objects (電腦物件)。
9. 選取 Create selected objects in this folder (在此資料夾中建立選取的物件) 和 Delete selected objects in this folder (在此資料夾中刪除選取的物件)。然後選擇下一步。
10. 選取 Read (讀取) 和 Write (寫入)，然後選擇 Next (下一步)。
11. 驗證 Completing the Delegation of Control Wizard (完成委派控制精靈) 頁面中的資訊，然後選擇 Finish (完成)。
12. 建立使用高強度密碼的使用者，並將此使用者新增至 `Joiners` 群組。這個使用者必須位在您 NetBIOS 名稱下的 Users (使用者) 容器中。然後，使用者就會有足夠的權限將執行個體連線到目錄。

建立或變更 AWS Managed Microsoft AD 的 DHCP 選項集

AWS 建議您為 AWS Directory Service 目錄建立 DHCP 選項集，並將 DHCP 選項集指派給目錄所在的 VPC。這可讓該 VPC 中的任何執行個體指向指定的網域和 DNS 伺服器，以解析其網域名稱。

如需 DHCP 選項集的詳細資訊，請參閱《Amazon VPC 使用者指南》https://docs.aws.amazon.com/vpc/latest/userguide/VPC_DHCP_Options.html中的 DHCP 選項集。

為目錄建立 DHCP 選項集

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 DHCP Options Sets (DHCP 選項集)，然後選擇 Create DHCP options set (建立 DHCP 選項集)。
3. 在 Create DHCP options set (建立 DHCP 選項集) 頁面上，輸入您目錄的下列值：

   名稱

   選項集的選用標籤。

   網域名稱

   您目錄的完整名稱，例如 `corp.example.com`。

Domain name servers (網域名稱伺服器)

您 AWS提供的目錄 DNS 伺服器的 IP 地址。

> **Note**
>
> 您可以前往 AWS Directory Service 主控台導覽窗格，選取目錄，然後選擇正確的目錄 ID，來找到這些地址。

NTP servers (NTP 伺服器)

將此欄位留白。

NetBIOS name servers (NetBIOS 名稱伺服器)

將此欄位留白。

NetBIOS node type (NetBIOS 節點類型)

將此欄位留白。

4. 選擇 Create DHCP options set (建立 DHCP 選項集)。DHCP 選項清單會隨即顯示新的 DHCP 選項集。
5. 記下新 DHCP 選項集的 ID (dopt-*xxxxxxxx*)。您可以使用它建立新選項集與 VPC 的關聯。

變更與 VPC 相關的 DHCP 選項集

建立 DHCP 選項集之後，便無法再進行修改。如果您希望 VPC 使用不同的 DHCP 選項集，則必須建立新選項集，並與 VPC 建立關聯。您也可以將 VPC 設定為完全不使用 DHCP 選項。

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 選取 VPC，然後選擇動作、編輯 VPC 設定。
4. 對於 DHCP 選項集，選取選項集或選取無 DHCP 選項集，然後選取儲存。

若要使用命令列變更與 VPC 相關聯的 DHCP 選項集，請參閱以下內容：

- AWS CLI：associate-dhcp-options
- AWS Tools for Windows PowerShell：Register-EC2DhcpOption

AWS Managed Microsoft AD 中的使用者和群組管理

您可以在 AWS Managed Microsoft AD 中管理使用者和群組。您可以建立使用者來代表可存取您目錄的個人或實體。您也可以建立群組，一次授予和拒絕多個使用者的許可。您不僅可以將使用者新增至群組，也可以將群組新增至群組。當您將使用者新增至群組時，使用者會繼承指派給群組的角色和許可。當您將群組新增至群組時，群組會共用父子關係，其中子群組會繼承指派給父群組的角色和許可。您也可以將使用者的群組成員資格複製到另一個使用者。

您可以使用下列方法the section called “目錄服務資料”使用 管理使用者和群組：

- AWS Management Console
- AWS CLI
- AWS Directory Service Data API
- AWS Tools for Windows PowerShell

如需 AWS Directory Service Data CLI 的示範，請參閱下列YouTube影片。

使用 CRUD APIs 管理 AWS Managed Microsoft AD 中的使用者和群組

或者，您可以使用加入網域的執行個體。

使用 管理使用者和群組 AWS Management Console

您可以使用 AWS Management Console AWS Directory Service Data 管理使用者和群組。Directory Service Data 是 的延伸 AWS Directory Service ，可讓您執行內建的物件管理任務。其中一些任務包括建立使用者和群組，以及將使用者新增至群組，以及將群組新增至群組。

如需詳細資訊，請參閱使用 管理 AWS Managed Microsoft AD 使用者和群組 AWS Management Console。

> **Note**
>
> 若要使用此功能，必須啟用此功能。如需詳細資訊，請參閱啟用使用者和群組管理。
> 您只能 AWS Management Console 從目錄的主要 AWS 區域 使用 管理使用者和群組。如需詳細資訊，請參閱主要區域與額外區域。
> 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始將許可授予使用者和工作負

載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。

使用 管理使用者和群組 AWS CLI

您可以透過 AWS CLI AWS Directory Service Data API 使用 管理使用者和群組。Directory Service Data 是 的延伸 AWS Directory Service ，可讓您使用 ds-data 命名空間執行內建物件管理任務。其中一些任務包括建立使用者和群組，以及將使用者新增至群組，以及將群組新增至群組。

使用 AWS 目錄服務資料 CLI 建立使用者

以下是使用 ds-data 命名空間來建立使用者的範例 AWS CLI 命令。

```
aws ds-data create-user --directory-id d-1234567890 --sam-account-name "jane.doe" --
region your-Primary-Region-name
```

> **Note**
>
> 若要使用此功能 AWS CLI，必須啟用。如需詳細資訊，請參閱啟用或停用使用者和群組管理或 AWS Directory Service Data。
> 您只能從目錄 AWS 區域 的主要 使用 AWS Directory Service Data CLI 管理使用者和群組。如需詳細資訊，請參閱主要區域與額外區域。
> 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始授予許可給使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需詳細資訊，請參閱 IAM 中的安全最佳實務。

如需詳細資訊，請參閱使用 管理 AWS Managed Microsoft AD 使用者和群組 AWS CLI。

使用 管理使用者和群組 AWS Tools for PowerShell

AWS Tools for PowerShell 提供兩個用於管理的個別模組 AWS Directory Service：AWS.Tools.DirectoryService(DS) 和 AWS.Tools.DirectoryServiceData(DSD)。使用 時 AWS Directory Service，請確定您使用適用於預期操作的適當模組。

- `DirectoryService` 模組包含用於管理目錄服務組態和管理的 cmdlet，包括 `Enable-DSDirectoryDataAccess`、 `Disable-DSDirectoryDataAccess`和 等 cmdlet`Reset-DSUserPassword`。
- `DirectoryServiceData` 模組包含用於在目錄中執行操作的 cmdlet，特別著重於使用者和群組管理。這些 DSD cmdlet 包括使用者管理操作 (`New-DSDUser`、`Update-DSDUser`、 和 `Remove-DSDUser`)`Get-DSDUser`、群組管理操作 (`New-DSDGroup`、 和 `Update-DSDGroup`、`Remove-DSDGroup`)`Get-DSDGroup`、群組成員資格管理 (`Add-DSDGroupMember`和 `Remove-DSDGroupMember`)，以及搜尋功能 (`Search-DSDUser` 和)`Search-DSDGroup`。

使用內部部署執行個體或 Amazon EC2 執行個體管理使用者和群組

如果 AWS Directory Service Data 不支援您的使用案例，建議您使用內部部署或 EC2 執行個體管理使用者和群組。

若要在 AWS Managed Microsoft AD 中建立使用者和群組，您可以使用已加入 AWS Managed Microsoft AD 的任何執行個體 （ 從內部部署或 EC2)。您需要以具有建立使用者和群組權限的使用者身分登入。您也需要在執行個體上安裝Active Directory工具，以便使用使用者和電腦工具新增Active Directory使用者和群組。

- 您可以從管理 AWS Directory Service 主控台部署預先安裝Active Directory管理工具的預先設定 EC2 執行個體。如需詳細資訊，請參閱在 AWS Managed Microsoft AD 中啟動目錄管理執行個體 Active Directory。
- 如果您需要使用管理工具部署自我管理的 EC2 執行個體並安裝必要的工具，請參閱 步驟 3：部署 Amazon EC2 執行個體以管理您的 AWS Managed Microsoft AD Active Directory。

主題

- 使用 AWS Management ConsoleAWS CLI或 管理 AWS Managed Microsoft AD 使用者和群組 AWS Tools for PowerShell
- 使用 Amazon EC2 執行個體管理使用者和群組

使用 AWS Management ConsoleAWS CLI或 管理 AWS Managed Microsoft AD 使用者和群組 AWS Tools for PowerShell

您可以使用 AWS Management Console AWS CLI或 AWS Tools for PowerShell ，透過 管理您的 AWS Managed Microsoft AD 使用者和群組AWS 目錄服務資料。 AWS Directory Service Data CLI 使

用 ds-data 命名空間。如需 的詳細資訊 AWS CLI，請參閱 入門 AWS CLI。如需 的詳細資訊 AWS Tools for PowerShell，請參閱 AWS Tools for PowerShell 使用者指南。

如需建立、檢視、更新和刪除 AWS Managed Microsoft AD 使用者和群組的詳細資訊，請參閱下列程序。

使用者和群組管理程序

- 啟用或停用使用者和群組管理或 AWS Directory Service Data
- 建立 AWS Managed Microsoft AD 使用者
- 檢視和更新 AWS Managed Microsoft AD 使用者
- 刪除 AWS Managed Microsoft AD 使用者
- 停用 AWS Managed Microsoft AD 使用者
- 重設和啟用 AWS Managed Microsoft AD 使用者的密碼
- 建立 AWS Managed Microsoft AD 群組
- 檢視和更新 AWS Managed Microsoft AD 群組的詳細資訊
- 刪除 AWS Managed Microsoft AD 群組
- 將 AWS Managed Microsoft AD 成員新增至群組，並將群組新增至群組
- 在 中複製 AWS Managed Microsoft AD 群組成員資格 AWS Management Console

啟用或停用使用者和群組管理或 AWS Directory Service Data

若要使用使用者和群組管理或 AWS Directory Service Data，必須啟用它。啟用後，您可以從 AWS Management Console AWS CLI或 管理使用者和群組 AWS Tools for PowerShell。

> **Important**
>
> - 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
> - 如需支援 AWS Directory Service Data 的區域清單，請參閱 AWS 區域 支援 Directory Service Data。
> - AWS Directory Service Data 的存取控制與 Amazon WorkSpaces、Amazon QuickSight 和 Amazon WorkMail AWS 服務 等 的存取控制不同。如需詳細資訊，請參閱AWS 具有 Directory Service Data 的應用程式授權。

啟用 AWS 目錄服務資料

使用下列程序，透過 AWS Management Console AWS CLI、 或 為現有的 AWS Managed Microsoft AD 啟用使用者和群組管理或 AWS 目錄服務資料 AWS Tools for PowerShell。

AWS Management Console

您可以使用 啟用使用者和群組管理 AWS Management Console。

啟用使用者和群組管理

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 在目錄詳細資訊頁面上，若要啟用使用者和群組管理，請選取啟用。
3. 在啟用使用者和群組管理對話方塊中，選取啟用。

AWS CLI

以下說明如何格式化啟用 AWS Directory Service Data CLI 的請求。您必須在請求中包含目錄 ID 號碼。

> **Note**
>
> enable AWS Directory Service Data CLI 命令使用 `aws ds`。

啟用 AWS 目錄服務資料 CLI

- 開啟 AWS CLI，然後執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
aws ds enable-directory-data-access --directory-id d-1234567890
```

AWS Tools for PowerShell

使用 Tools for PowerShell 啟用目錄服務資料

- 開啟 PowerShell，然後執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
Enable-DSDirectoryDataAccess -DirectoryId d-1234567890
```

停用 AWS 目錄服務資料

使用下列程序，使用 AWS Management Console AWS CLI、 或 停用現有 AWS Managed Microsoft AD 的使用者和群組管理或 AWS 目錄服務資料 AWS Tools for PowerShell。

AWS Management Console

您可以使用 停用使用者和群組管理 AWS Management Console。

停用使用者和群組管理

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 在目錄詳細資訊頁面上，若要停用使用者和群組管理，請選取停用。
3. 在停用使用者和群組管理對話方塊中，選取停用。

AWS CLI

以下說明如何格式化停用 AWS Directory Service Data CLI 的請求。您必須在請求中包含目錄 ID 號碼。

> **Note**
>
> 停用 AWS Directory Service Data CLI 命令使用 `aws ds`。

停用 AWS Directory Service Data CLI

- 開啟 AWS CLI，然後執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
aws ds disable-directory-data-access --directory-id d-1234567890
```

AWS Tools for PowerShell

使用 Tools for PowerShell 停用目錄服務資料

- 開啟 PowerShell，然後執行下列命令，將目錄 ID 取代為您的 AWS Managed Microsoft AD Directory ID：

```
Disable-DSDirectoryDataAccess -DirectoryId d-123456789
```

建立 AWS Managed Microsoft AD 使用者

使用下列程序，在 AWS Management Console AWS CLI或 中建立具有使用者和群組管理或 AWS Directory Service Data 的新 AWS Managed Microsoft AD 使用者 AWS Tools for PowerShell。

開始任一程序之前，您需要完成下列各項：

- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始將許可授予使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。

AWS Management Console

您可以在 中建立新的 AWS Managed Microsoft AD 使用者帳戶 AWS Management Console。當您建立新的使用者帳戶時，您可以指定新使用者的詳細資訊，並決定是否要將新使用者新增至群組，還是將其他使用者的群組成員資格複製到新使用者。

如需詳細資訊，請參閱AWS Directory Service Data 屬性及群組類型和群組範圍。

使用 建立 AWS Managed Microsoft AD 使用者 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。

2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 在目錄詳細資訊頁面的使用者區段下，選擇建立使用者帳戶。
5. 隨即開啟指定使用者詳細資訊頁面。在必要資訊區段下，輸入使用者登入名稱和密碼。使用者登入名稱必須符合下列條件：

   - 必須是唯一的登入名稱
   - 長度上限為 20 個字元
   - 只能包含英數字元
   - ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
   - 密碼必須遵循您的密碼政策要求。如需詳細資訊，請洽詢您的 AWS 管理員。

   > ⚠ Warning
   >
   > 建立使用者之後，無法變更使用者登入名稱。

   a. （選用）在主要資訊區段下，您可以輸入使用者的名字和姓氏。您也可以輸入使用者的顯示名稱和描述。
   b. （選用）在聯絡方法區段下，您可以輸入使用者的電子郵件地址和電話號碼。
   c. （選用）在工作相關資訊區段下，您可以輸入使用者的部門、經理、辦公室和公司。
   d. （選用）在地址區段下，您可以輸入使用者的地址。
   e. （選用）在帳戶設定區段下，您可以輸入使用者的備註、偏好語言和服務主體名稱。

   如需使用者屬性的詳細資訊，請參閱 AWS Directory Service Data 屬性和 Microsoft 文件。
6. 提供使用者帳戶詳細資訊後，請選擇下一步。
7. 在將使用者新增至群組 - 選用頁面上，您可以將使用者新增至新群組或現有群組。您也可以將現有使用者的群組成員資格複製到新使用者。如果您不想將使用者新增至群組，請選擇下一步。移至步驟 12 以繼續此程序。
8. （選用）若要建立新群組，請參閱建立 AWS 受管 Microsoft AD 群組。
9. （選用）若要將新使用者新增至現有群組：

- 在群組區段中，選取要將新使用者新增至其中的群組。若要尋找群組，請在搜尋方塊中輸入群組名稱。

10. （選用）若要將現有使用者的群組成員資格複製到新使用者：

    a. 選擇從使用者索引標籤複製群組成員資格。若要尋找具有您要複製之群組成員資格的使用者，請在使用者區段下的搜尋方塊中輸入使用者登入名稱。

    b. 在選取的群組區段中，選取新使用者應成為其成員的群組。

11. 當您準備好建立新的使用者帳戶時，請選擇下一步。
12. 在檢閱和建立使用者頁面上，檢閱您所做的所有選擇。選擇 Create user (建立使用者)。
13. 設定使用者後，您已前往新使用者的詳細資訊頁面。隨即出現橫幅，指出使用者已成功建立。

> **Important**
>
> 如果您收到錯誤訊息，告知您沒有建立使用者的許可，請遵循錯誤訊息中的指示，請求您的管理員授予您存取權。

AWS CLI

以下說明如何使用 AWS Directory Service Data CLI 格式化建立新 AWS Managed Microsoft AD 使用者帳戶的請求。您必須在請求中包含目錄 ID 號碼和使用者登入名稱。您也可以包含其他屬性，例如具有 `DisplayName` 屬性的使用者顯示名稱。如需詳細資訊，請參閱AWS Directory Service Data 屬性及群組類型和群組範圍。

使用 建立 AWS Managed Microsoft AD 使用者 AWS CLI

- 開啟 AWS CLI，並執行下列命令，將目錄 ID、使用者名稱和顯示名稱取代為您的 AWS Managed Microsoft AD Directory ID 和所需的登入資料：

```
aws ds-data create-user \
  --directory-id d-1234567890 \
  --sam-account-name "jane.doe" \
  --other-attributes '{
    "DisplayName" : { "S": "jane.doe"},
    "Department":{ "S": "Legal"}
    }‘
```

AWS Tools for PowerShell

以下說明如何格式化建立新 AWS Managed Microsoft AD 使用者帳戶的請求 AWS Tools for PowerShell。您必須在請求中包含目錄 ID 號碼和使用者登入名稱。您也可以包含其他屬性，例如具有 `DisplayName` 屬性的使用者顯示名稱。如需詳細資訊，請參閱AWS Directory Service Data 屬性及群組類型和群組範圍。

使用 Tools for PowerShell 建立 AWS Managed Microsoft AD 使用者

- 開啟 PowerShell，並執行下列命令，將目錄 ID、使用者名稱和顯示名稱取代為您的 AWS Managed Microsoft AD Directory ID 和所需的登入資料：

```
New-DSDUser `
    -DirectoryId d-1234567890 `
    -SAMAccountName "jane.doe" `
    -OtherAttribute @{
        DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
 'jane.doe' }
        Department = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
 'Legal' }
    }
```

檢視和更新 AWS Managed Microsoft AD 使用者

使用下列程序，透過 、 或 中的使用者和群組管理或 AWS Directory Service Data AWS Management Console AWS CLI，檢視或更新 AWS Managed Microsoft AD 使用者的詳細資訊 AWS Tools for PowerShell。

檢視 AWS Managed Microsoft AD 使用者的詳細資訊

您可以在 AWS Management Console 或 中檢視使用者的詳細資訊 AWS CLI。使用者的詳細資訊包括設定檔和帳戶資訊和群組成員資格。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。

- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始授予許可給使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。
- 建立 AWS Managed Microsoft AD 使用者.

AWS Management Console

您可以在 中檢視 AWS Managed Microsoft AD 使用者的詳細資訊 AWS Management Console。

使用 檢視 AWS Managed Microsoft AD 使用者的詳細資訊和帳戶詳細資訊 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Users (使用者)。標籤顯示目錄中的使用者清單。
5. 選取使用者。系統會將您導向至使用者詳細資訊畫面。使用者詳細資訊畫面會顯示下列資訊：
   - 使用者所屬的群組 （群組成員資格）
   - 設定檔詳細資訊 （例如使用者登入名稱、名字、姓氏等主要資訊）
   - 帳戶設定 （例如帳戶資訊，例如使用者主體名稱、服務主體名稱、辨別名稱等）
   - 帳戶狀態

如需使用者屬性的詳細資訊，請參閱 AWS Directory Service Data 屬性和 Microsoft 文件。

AWS CLI

使用 AWS CLI，您可以檢視使用者的詳細資訊，其中包括設定檔、帳戶資訊和群組成員資格。

使用 檢視 AWS Managed Microsoft AD 使用者的設定檔和帳戶詳細資訊 AWS CLI

以下說明如何使用 AWS Directory Service Data CLI 檢視 AWS Managed Microsoft AD 使用者的詳細資訊。

- 若要檢視使用者的詳細資訊，請開啟 AWS CLI，然後執行下列命令，將目錄 ID 和使用者名稱取代為您的 AWS Managed Microsoft AD Directory ID 和使用者名稱：

```
aws ds-data describe-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

檢視使用者的群組成員資格

以下說明如何使用 AWS Directory Service Data CLI 檢視 AWS Managed Microsoft AD 使用者的群組成員資格。

- 若要檢視使用者的群組成員資格，請開啟 AWS CLI，然後執行下列命令，將目錄 ID 和使用者名稱取代為您的 AWS Managed Microsoft AD Directory ID 和使用者名稱：

```
aws ds-data list-groups-for-member --directory-id d-1234567890 --sam-account-name
 "jane.doe"
```

如需使用者屬性的詳細資訊，請參閱 AWS Directory Service Data 屬性和 Microsoft 文件。

AWS Tools for PowerShell

透過 Tools for PowerShell，您可以檢視使用者的詳細資訊，其中包括設定檔、帳戶資訊和群組成員資格。

使用 Tools for PowerShell 檢視 AWS Managed Microsoft AD 使用者的設定檔和帳戶詳細資訊

以下說明如何使用 Tools for PowerShell 檢視 AWS Managed Microsoft AD 使用者的詳細資訊。

- 若要檢視使用者的詳細資訊，請開啟 PowerShell，然後執行下列命令，將目錄 ID 和使用者名稱取代為您的 AWS Managed Microsoft AD Directory ID 和使用者名稱：

```
Get-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

檢視使用者的群組成員資格

以下說明如何使用 Tools for PowerShell 檢視 AWS Managed Microsoft AD 使用者的群組成員資格。

- 若要檢視使用者的群組成員資格，請開啟 PowerShell，然後執行下列命令，將目錄 ID 和使用者名稱取代為您的 AWS Managed Microsoft AD Directory ID 和使用者名稱：

```
(Get-DSDGroupsForMemberList -DirectoryId d-1234567890 -SAMAccountName
 "jane.doe").Groups
```

如需使用者屬性的詳細資訊，請參閱 AWS Directory Service Data 屬性和 Microsoft 文件。

更新 AWS Managed Microsoft AD 使用者的詳細資訊

使用下列程序，透過 中的使用者和群組管理或 AWS 目錄服務資料 AWS Management Console AWS CLI來更新 AWS Managed Microsoft AD 使用者 AWS Tools for PowerShell。

> **Note**
>
> 屬性長度下限為 1。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始授予許可給使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。
- 建立 AWS Managed Microsoft AD 使用者.

AWS Management Console

您可以在 中更新 AWS Managed Microsoft AD 使用者的詳細資訊 AWS Management Console。

使用 更新 AWS Managed Microsoft AD 使用者的詳細資訊 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。

2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Users (使用者)。標籤顯示目錄中的使用者清單。
5. 選取使用者。若要尋找使用者，請在使用者區段下的搜尋方塊中輸入使用者登入名稱。系統會將您導向使用者詳細資訊畫面。
6. 若要編輯使用者所屬的群組，請選擇群組。您可以從此索引標籤新增和移除群組中的使用者。如需詳細資訊，請參閱將 AWS Managed Microsoft AD 成員新增至群組。
7. 若要編輯使用者的設定檔詳細資訊，請選擇設定檔，然後選擇編輯。或者，選擇動作，然後選擇編輯使用者。進行並檢閱您的更新，然後選擇儲存。

> **Warning**
>
> 建立使用者之後，無法變更使用者登入名稱。

8. 若要編輯使用者帳戶設定，請選擇使用者帳戶設定。或者，選擇動作，然後選擇編輯使用者。進行並檢閱您的更新，然後選擇儲存。

如需使用者屬性的詳細資訊，請參閱 AWS Directory Service Data 屬性和 Microsoft 文件。

AWS CLI

以下說明如何使用 AWS Directory Service Data CLI 格式化更新 AWS Managed Microsoft AD 使用者詳細資訊的請求。

更新使用者帳戶時，您必須包含目錄 ID 號碼和使用者登入名稱。您還必須在請求中包含要更新的更新類型和屬性，例如具有 `Surname` 參數的使用者姓氏。如需詳細資訊，請參閱 AWS Directory Service Data 屬性。

- 若要更新使用者的詳細資訊，請開啟 AWS CLI並執行下列命令，將目錄 ID、使用者名稱、使用者類型和屬性值取代為您的 AWS Managed Microsoft AD Directory ID、使用者名稱，以及所需的使用者類型和屬性值：

```
aws ds-data update-user --directory-id d-1234567890 --sam-account-name "jane.doe" --
update-type "REPLACE" --surname "Doe"
```

> **Note**
>
> 使用 update-user CLI 命令移除使用者屬性時，您必須指定要移除的屬性和確切值。若要判斷使用者屬性，請使用 describe-user 命令。

如需使用者屬性的詳細資訊，請參閱 AWS Directory Service Data 屬性和 Microsoft 文件。

AWS Tools for PowerShell

以下說明如何格式化更新 AWS Managed Microsoft AD 使用者詳細資訊的請求 AWS Tools for PowerShell。

更新使用者帳戶時，您必須包含目錄 ID 號碼和使用者登入名稱。您還必須在請求中包含要更新的更新類型和屬性，例如具有 `Surname` 參數的使用者姓氏。如需詳細資訊，請參閱AWS 目錄服務資料屬性。

- 若要更新使用者的詳細資訊，請開啟 PowerShell，並執行下列命令，將目錄 ID、使用者名稱、使用者類型和屬性值取代為您的 AWS Managed Microsoft AD Directory ID、使用者名稱，以及所需的使用者類型和屬性值：

```
Update-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe" -UpdateType
 "REPLACE" -Surname "Doe"
```

如需使用者屬性的詳細資訊，請參閱 AWS Directory Service Data 屬性和 Microsoft 文件。

刪除 AWS Managed Microsoft AD 使用者

使用下列程序刪除 中具有使用者和群組管理或 AWS Directory Service Data 的 AWS Managed Microsoft AD 使用者 AWS Management Console AWS CLI AWS Tools for PowerShell。

> **Important**
>
> 當您從目錄刪除使用者帳戶時，會移除使用者的所有相關資訊，包括使用者存取其帳戶和應用程式的任何許可。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始將許可授予使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。
- 建立 AWS Managed Microsoft AD 使用者.

AWS Management Console

您可以在 中刪除 AWS Managed Microsoft AD 使用者帳戶 AWS Management Console。

使用 刪除 AWS Managed Microsoft AD 使用者帳戶 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Users (使用者)。標籤顯示目錄中的使用者清單。
5. 選擇您要刪除其帳戶的使用者。若要尋找使用者，請在使用者區段下的搜尋方塊中輸入使用者登入名稱。系統會將您導向使用者詳細資訊畫面。
6. 選擇動作。然後選擇刪除使用者帳戶，然後再次刪除使用者帳戶。

AWS CLI

以下說明如何使用 AWS Directory Service Data CLI 格式化刪除 AWS Managed Microsoft AD 使用者帳戶的請求。

使用 刪除 AWS Managed Microsoft AD 使用者帳戶 AWS CLI

- 開啟 AWS CLI，然後執行下列命令，將目錄 ID 和使用者名稱取代為您的 AWS Managed Microsoft AD Directory ID 和使用者名稱：

```
aws ds-data delete-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

AWS Tools for PowerShell

以下說明如何格式化刪除 AWS Managed Microsoft AD 使用者帳戶的請求 AWS Tools for PowerShell。

使用 刪除 AWS Managed Microsoft AD 使用者帳戶 AWS Tools for PowerShell

- 開啟 PowerShell，然後執行下列命令，將目錄 ID 和使用者名稱取代為您的 AWS Managed Microsoft AD Directory ID 和使用者名稱：

```
Remove-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

停用 AWS Managed Microsoft AD 使用者

使用下列程序，在 AWS Management Console AWS CLI、 或 中停用具有使用者和群組管理或 AWS Directory Service Data 的 AWS Managed Microsoft AD 使用者 AWS Tools for PowerShell。

> **Important**
>
> 當您停用使用者帳戶時，使用者會失去存取其帳戶和應用程式的任何許可。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始將許可授予使用者和工作負載，您

可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。

- 建立 AWS Managed Microsoft AD 使用者.

AWS Management Console

您可以在 中停用 AWS Managed Microsoft AD 使用者帳戶 AWS Management Console。

使用 停用 AWS Managed Microsoft AD 使用者帳戶 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Users (使用者)。標籤顯示目錄中的使用者清單。
5. 選擇您要停用其帳戶的使用者。系統會將您導向使用者詳細資訊畫面。
6. 選擇動作。然後選擇停用使用者帳戶，然後再次停用使用者帳戶。

> **Note**
>
> 若要重新啟用使用者帳戶，您必須重設使用者的密碼。如需詳細資訊，請參閱重設和啟用 AWS Managed Microsoft AD 使用者的密碼。

AWS CLI

以下說明如何使用 AWS Directory Service Data CLI 格式化停用 AWS Managed Microsoft AD 使用者帳戶的請求。

使用 停用 AWS Managed Microsoft AD 使用者帳戶 AWS CLI

- 開啟 AWS CLI，然後執行下列命令，將目錄 ID 和使用者名稱取代為您的 AWS Managed Microsoft AD Directory ID 和使用者名稱：

```
aws ds-data disable-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

> **Note**
>
> 若要重新啟用您的使用者帳戶，您必須重設使用者的密碼。如需詳細資訊，請參閱重設和啟用 AWS Managed Microsoft AD 使用者的密碼。

AWS Tools for PowerShell

以下說明如何格式化停用 AWS Managed Microsoft AD 使用者帳戶的請求 AWS Tools for PowerShell。

使用 停用 AWS Managed Microsoft AD 使用者帳戶 AWS Tools for PowerShell

- 開啟 PowerShell；並執行下列命令，將目錄 ID 和使用者名稱取代為您的 AWS Managed Microsoft AD Directory ID 和使用者名稱：

```
Disable-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

> **Note**
>
> 若要重新啟用您的使用者帳戶，您必須重設使用者的密碼。如需詳細資訊，請參閱重設和啟用 AWS Managed Microsoft AD 使用者的密碼。

重設和啟用 AWS Managed Microsoft AD 使用者的密碼

使用下列程序重設 AWS Managed Microsoft AD 使用者的密碼 AWS Management Console AWS CLI，在 中的使用者和群組管理或 AWS 目錄服務資料啟用其帳戶 AWS Tools for PowerShell。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。

- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始授予許可給使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。
- 建立 AWS Managed Microsoft AD 使用者.

AWS Management Console

您可以重設 AWS Managed Microsoft AD 使用者的密碼，以在 中啟用其帳戶 AWS Management Console。您可以從目錄畫面或目錄詳細資訊畫面執行此任務。

目錄

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇動作，然後選擇重設使用者密碼並啟用帳戶。
   a. 在使用者登入名稱下，輸入您要重設其密碼的使用者登入名稱。
   b. 在新密碼下，輸入使用者的新密碼。
   c. 在確認密碼下，再次輸入使用者的新密碼。
4. 確認使用者的新密碼後，請選擇重設密碼並啟用帳戶。

目錄詳細資訊

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Users (使用者)。標籤顯示目錄中的使用者清單。
5. 選取您要重設密碼的使用者。
6. 選擇動作，然後選擇重設使用者密碼並啟用帳戶。

a. 在新密碼下，輸入使用者的新密碼。

b. 在確認密碼下，再次輸入使用者的新密碼。

7. 確認使用者的新密碼後，請選擇重設密碼並啟用帳戶。

AWS CLI

您可以重設 AWS Managed Microsoft AD 使用的密碼，以透過 AWS Directory Service Data CLI 啟用其帳戶。

> **Note**
>
> 重設使用者的密碼命令使用 `aws ds`。

使用 重設 AWS Managed Microsoft AD 使用者的密碼 AWS CLI

- 若要重設使用者的密碼，請開啟 AWS CLI，並執行下列命令，將目錄 ID、使用者名稱和密碼取代為您的 AWS Managed Microsoft AD Directory ID、使用者名稱和密碼，以及所需的登入資料：

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "your-password"
```

AWS Tools for PowerShell

您可以重設 AWS Managed Microsoft AD 使用的密碼，以啟用其 帳戶 AWS Tools for PowerShell。

使用 重設 AWS Managed Microsoft AD 使用者的密碼 AWS Tools for PowerShell

- 若要重設使用者的密碼，請開啟 PowerShell，然後執行下列命令，將目錄 ID、使用者名稱和密碼取代為您的 AWS Managed Microsoft AD Directory ID、使用者名稱和密碼，以及所需的登入資料：

```
Reset-DSUserPassword -DirectoryId d-1234567890 -UserName "jane.doe" -NewPassword "your-password"
```

建立 AWS Managed Microsoft AD 群組

使用下列程序，在 AWS Management Console AWS CLI、 或 中建立具有使用者和群組管理或 AWS Directory Service Data 的 AWS Managed Microsoft AD 群組 AWS Tools for PowerShell。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始授予許可給使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。

AWS Management Console

您可以在 中建立新的 AWS Managed Microsoft AD 群組 AWS Management Console。建立新群組時，您可以指定群組的詳細資訊，並判斷群組的類型和範圍。您也可以選擇將使用者和子群組新增至新群組，或將新群組新增至父群組。

使用 建立 AWS Managed Microsoft AD 群組 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇群組。標籤顯示 中的群組清單 AWS 區域。
5. 選擇建立群組。系統會將您導向至完成建立新群組的程序。
6. 指定群組詳細資訊頁面隨即開啟。輸入群組名稱。群組名稱必須符合下列條件：
   - 必須是唯一的群組名稱
   - 長度上限為 64 個字元

- 只能包含英數字元
- ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

> **Warning**
>
> 建立群組之後，就無法變更群組名稱。

7. 從下列其中一項中選擇群組類型：
   - 安全性
   - 發佈
     - 如需詳細資訊，請參閱 the section called “Group type (群組類型)”。
8. 從下列其中一項中選擇群組範圍：
   - 網域本機
   - 通用
   - 全域
     - 您可以開啟比較範圍以顯示群組範圍之間相似性和差異的圖表。如需詳細資訊，請參閱 the section called “Group scope (群組範圍)”。
9. 提供主要資訊和聯絡方式後，選擇下一步。
10. 新增使用者至群組 - 選用頁面隨即開啟，您可以將使用者新增至新群組。若要尋找要新增至群組的使用者，請在使用者區段下的搜尋方塊中輸入使用者登入名稱。選取您要新增至群組的使用者，然後選擇下一步。
11. 新增子群組 - 選用頁面隨即開啟，您可以將現有群組新增至新群組。現有群組會成為新建立群組的子群組。當您將子群組新增至群組時，您的群組會成為父群組，而子群組會繼承群組的所有角色和許可。若要尋找要新增的群組，請在新增子群組區段下的搜尋方塊中輸入群組名稱。選取您要新增至新群組的子群組，然後選擇下一步。
12. 新增父群組 - 選用頁面隨即開啟，您可以將新群組新增至現有群組。新群組會成為現有群組的父群組。當您將群組新增至父群組時，您的群組會成為子群組，並繼承父群組的所有角色和許可。若要尋找要新增的群組，請在新增父群組區段下的搜尋方塊中輸入群組名稱。選取您要新增至新群組的父群組，然後選擇下一步。
13. 在檢閱和建立群組頁面上，檢閱您的選擇，然後選擇建立群組。

AWS CLI

以下說明如何使用 AWS Directory Service Data CLI 格式化建立 AWS Managed Microsoft AD 群組的請求。建立新群組時，您必須包含目錄 ID 號碼和群組名稱。您也可以新增其他屬性，例如具有 DisplayName 屬性的群組顯示名稱。如需詳細資訊，請參閱AWS Directory Service Data 屬性及群組類型和群組範圍。

使用 建立 AWS Managed Microsoft AD 群組 AWS CLI

- 開啟 AWS CLI，並執行下列命令，將目錄 ID、使用者名稱和群組顯示名稱取代為您的 AWS Managed Microsoft AD Directory ID、使用者名稱和所需的群組顯示名稱：

```
aws ds-data create-group \
    --directory-id d-1234567890 \
    --sam-account-name "your-group-name" \
    --other-attributes '{
        "DisplayName": { "S": "myGroupDisplayName"}
        "Description":{ "S": "myGroupDescription"}
    }'
```

AWS Tools for PowerShell

以下說明如何格式化使用 建立 AWS Managed Microsoft AD 群組的請求 AWS Tools for PowerShell。建立新群組時，您必須包含目錄 ID 號碼和群組名稱。您也可以新增其他屬性，例如具有 DisplayName 屬性的群組顯示名稱。如需詳細資訊，請參閱AWS Directory Service Data 屬性及群組類型和群組範圍。

使用 建立 AWS Managed Microsoft AD 群組 AWS Tools for PowerShell

- 開啟 PowerShell，然後執行下列命令，將目錄 ID、使用者名稱和群組顯示名稱取代為您的 AWS Managed Microsoft AD Directory ID、使用者名稱和所需的群組顯示名稱：

```
New-DSDGroup `
    -DirectoryId d-1234567890 `
    -SAMAccountName "your-group-name" `
    -OtherAttribute @{
        DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
 'myGroupDisplayName' }
        Description = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
 'myGroupDescription' }
```

```
}
```

檢視和更新 AWS Managed Microsoft AD 群組的詳細資訊

使用下列程序，透過 、 或 中的使用者和群組管理或 AWS 目錄服務資料 AWS Management Console AWS CLI，檢視或更新 AWS Managed Microsoft AD 群組的詳細資訊 AWS Tools for PowerShell。

檢視 AWS Managed Microsoft AD 群組的詳細資訊

您可以在 AWS Management Console AWS CLI、 或 中檢視或更新群組的詳細資訊 AWS Tools for PowerShell。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始授予許可給使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。
- 建立 AWS Managed Microsoft AD 群組。

AWS Management Console

您可以在 中檢視 AWS Managed Microsoft AD 群組的詳細資訊 AWS Management Console。

使用 檢視 AWS Managed Microsoft AD 群組的詳細資訊 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇群組。標籤顯示 中的群組清單 AWS 區域。

5. 選擇群組。若要尋找群組，請在群組區段下的搜尋方塊中輸入群組名稱。系統會將您導向至群組詳細資訊畫面。群組詳細資訊畫面會顯示下列資訊：

   - 成員索引標籤列出屬於您群組成員的使用者和子群組。
   - 父群組索引標籤會列出您的群組所屬的父群組。
   - 屬性索引標籤會列出群組屬性（例如群組名稱、群組顯示名稱等主要資訊）。

AWS CLI

您可以使用 AWS Directory Service Data CLI 檢視 AWS Managed Microsoft AD 群組的詳細資訊。

使用 檢視 AWS Managed Microsoft AD 群組的詳細資訊 AWS CLI

以下說明如何使用 檢視 AWS Managed Microsoft AD 群組的詳細資訊 AWS CLI。

- 若要檢視群組的詳細資訊，請開啟 AWS CLI，然後執行下列命令，將目錄 ID 和群組名稱取代為您的 AWS Managed Microsoft AD Directory ID 和群組名稱：

```
aws ds-data describe-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

使用 檢視 AWS Managed Microsoft AD 群組的群組成員 AWS CLI

以下說明如何使用 檢視 AWS Managed Microsoft AD 群組的成員 AWS CLI。

- 若要檢視群組的詳細資訊，請開啟 AWS CLI，然後執行下列命令，將目錄 ID 和群組名稱取代為您的 AWS Managed Microsoft AD Directory ID 和群組名稱：

```
aws ds-data list-group-members --directory-id d-1234567890 --sam-account-name "your-group-name"
```

AWS Tools for PowerShell

您可以使用 檢視 AWS Managed Microsoft AD 群組的詳細資訊 AWS Tools for PowerShell。

若要使用 檢視 AWS Managed Microsoft AD 群組的詳細資訊 AWS Tools for PowerShell

以下說明如何使用 Tools for PowerShell 檢視 AWS Managed Microsoft AD 群組的詳細資訊。

- 若要檢視群組的詳細資訊，請開啟 PowerShell，然後執行下列命令，將目錄 ID 和群組名稱取代為您的 AWS Managed Microsoft AD Directory ID 和群組名稱：

```
Get-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

若要使用 檢視 AWS Managed Microsoft AD 群組的群組成員 AWS Tools for PowerShell

以下說明如何使用 Tools for PowerShell 檢視 AWS Managed Microsoft AD 群組的成員。

- 若要檢視群組的詳細資訊，請開啟 PowerShell，然後執行下列命令，將目錄 ID 和群組名稱取代為您的 AWS Managed Microsoft AD Directory ID 和群組名稱：

```
(Get-DSDGroupMemberList -DirectoryId d-1234567890 -SAMAccountName "your-group-name").Members
```

更新 AWS Managed Microsoft AD 群組的詳細資訊

使用下列程序，在 AWS Management Console AWS CLI、 或 中使用使用者和群組管理或 AWS Directory Service Data 更新 AWS Managed Microsoft AD 群組的詳細資訊 AWS Tools for PowerShell。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始授予許可給使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。
- 建立 AWS Managed Microsoft AD 群組。

AWS Management Console

您可以使用 更新群組的詳細資訊 AWS Management Console。如需詳細資訊，請參閱 AWS Directory Service Data 屬性 和 群組類型和群組範圍

使用 更新 AWS Managed Microsoft AD 群組的詳細資訊 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇群組。標籤顯示 中的群組清單 AWS 區域。
5. 選擇群組。若要尋找群組，請在群組區段下的搜尋方塊中輸入群組名稱。系統會將您導向至群組詳細資訊畫面。
6. 若要編輯屬於您群組成員的使用者和子群組，請選擇成員。您可以從此索引標籤新增和移除 群組中的使用者和子群組。如需詳細資訊，請參閱將成員新增至群組，並將群組新增至群組。
7. 若要編輯群組所屬的父群組，請選擇父群組。在此索引標籤中，您可以從父群組新增和移除您的群組。如需詳細資訊，請參閱將成員新增至群組，並將群組新增至群組。
8. 若要編輯群組屬性，請選擇屬性，然後選擇編輯。或者，選擇動作，然後選擇編輯群組。進行並檢閱您的更新，然後選擇儲存。

AWS CLI

以下說明如何使用 AWS Directory Service Data CLI 格式化更新 AWS Managed Microsoft AD 群組詳細資訊的請求。

更新群組時，您必須包含目錄 ID 號碼和群組名稱。您還必須在請求中包含要更新的更新類型和屬性，例如具有 `EmailAddress` 參數的群組電子郵件地址。如需詳細資訊，請參閱AWS Directory Service Data 屬性及群組類型和群組範圍。

- 使用 更新 AWS Managed Microsoft AD 群組的詳細資訊 AWS CLI

  若要更新群組的詳細資訊，請開啟 AWS CLI並執行下列命令，將目錄 ID、群組名稱、更新類型和屬性取代為您的 AWS Managed Microsoft AD Directory ID、群組名稱，以及所需的更新類型和屬性：

```
aws ds-data update-group --directory-id d-1234567890 --sam-account-name "your-group-name" --update-type "REPLACE" --group-scope "global"
```

AWS Tools for PowerShell

以下說明如何格式化更新 AWS Managed Microsoft AD 群組詳細資訊的請求 AWS Tools for PowerShell。

更新群組時，您必須包含目錄 ID 號碼和群組名稱。您還必須在請求中包含要更新的更新類型和屬性，例如具有 `EmailAddress` 參數的群組電子郵件地址。如需詳細資訊，請參閱AWS Directory Service Data 屬性及群組類型和群組範圍。

- 使用 更新 AWS Managed Microsoft AD 群組的詳細資訊 AWS Tools for PowerShell

  若要更新群組的詳細資訊，請開啟 PowerShell，並執行下列命令，將目錄 ID、群組名稱、更新類型和屬性取代為您的 AWS Managed Microsoft AD Directory ID、群組名稱，以及所需的更新類型和屬性：

```
Update-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name" -UpdateType "REPLACE" -GroupScope "global"
```

刪除 AWS Managed Microsoft AD 群組

使用下列程序，在 AWS Management Console AWS CLI、 或 中刪除具有使用者和群組管理或 AWS Directory Service Data 的 AWS Managed Microsoft AD 群組 AWS Tools for PowerShell。

> **Important**
>
> 當您刪除群組時，會移除群組的所有相關資訊，包括群組成員繼承的任何許可。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。

- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始將許可授予使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。
- 建立 AWS Managed Microsoft AD 群組。

AWS Management Console

您可以在 中刪除 AWS Managed Microsoft AD 群組 AWS Management Console。

使用 刪除 AWS Managed Microsoft AD 群組 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇群組。標籤顯示 中的群組清單 AWS 區域。
5. 選擇您要刪除的群組。若要尋找群組，請在群組區段下的搜尋方塊中輸入群組名稱。系統會將您導向至群組詳細資訊畫面。
6. 選擇 Delete group (刪除群組)。此時會出現一個對話方塊，您可以選擇確認以刪除群組。

AWS CLI

以下說明如何使用 AWS Directory Service Data CLI 格式化刪除 AWS Managed Microsoft AD 群組的請求。

使用 刪除 AWS Managed Microsoft AD 群組 AWS CLI

- 開啟 AWS CLI，然後執行下列命令，將目錄 ID 和群組名稱取代為您的 AWS Managed Microsoft AD Directory ID 和群組名稱：

```
aws ds-data delete-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

AWS Tools for PowerShell

以下說明如何使用 格式化刪除 AWS Managed Microsoft AD 群組的請求 AWS Tools for PowerShell。

使用 刪除 AWS Managed Microsoft AD 群組 AWS Tools for PowerShell

- 開啟 PowerShell，然後執行下列命令，將目錄 ID 和群組名稱取代為您的 AWS Managed Microsoft AD Directory ID 和群組名稱：

```
Remove-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

將 AWS Managed Microsoft AD 成員新增至群組，並將群組新增至群組

使用 AWS Directory Service Data API，成員可以是使用者、群組或電腦。使用者代表可存取您目錄的個人或實體。群組可讓您一次授予和拒絕多個使用者的許可。

使用下列程序，將 AWS Managed Microsoft AD 使用者新增至群組或群組，或在 AWS Management Console AWS CLI、 或 中使用使用者和群組管理或 AWS 目錄服務資料新增至另一個群組 AWS Tools for PowerShell。

將使用者新增至群組

使用下列程序，將 AWS Managed Microsoft AD 使用者新增至 AWS Management Console AWS CLI、 或 中具有使用者和群組管理或 AWS Directory Service Data 的群組 AWS Tools for PowerShell。

> **Important**
>
> 當您將 AWS Managed Microsoft AD 使用者新增至群組時，該使用者會繼承指派給群組的角色和許可。這些角色和許可是使用者群組成員資格的一部分。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。

- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始將許可授予使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。
- 建立 AWS Managed Microsoft AD 使用者。
- 建立 AWS Managed Microsoft AD 群組。

AWS Management Console

您可以使用 將 AWS Managed Microsoft AD 成員新增至群組 AWS Management Console。

使用 將 AWS Managed Microsoft AD 使用者新增至群組 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Groups (群組)。若要尋找群組，請在群組區段下的搜尋方塊中輸入群組名稱。標籤顯示中的群組清單 AWS 區域。
5. 選擇群組。系統會將您導向至群組詳細資訊畫面。
6. 選擇成員。標籤顯示您群組中成員類型的使用者和子群組清單。
7. 在成員索引標籤下，選擇新增成員。
8. 在成員下，選取您要新增至群組的使用者，然後選擇新增成員至群組。若要尋找成員，請在成員區段下的搜尋方塊中輸入使用者的使用者登入名稱和群組名稱。

AWS CLI

以下說明如何使用 AWS Directory Service Data CLI 格式化將 AWS Managed Microsoft AD 成員新增至群組的請求。

使用 將 AWS Managed Microsoft AD 使用者新增至群組 AWS CLI

- 若要將使用者新增至群組，請開啟 AWS CLI，然後執行下列命令，將目錄 ID、群組和成員名稱取代為您的 AWS Managed Microsoft AD Directory ID，以及群組和成員名稱：

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "your-group-name" --member-name "jane.doe"
```

AWS Tools for PowerShell

以下說明如何格式化將 AWS Managed Microsoft AD 成員新增至 群組的請求 AWS Tools for PowerShell。

將 AWS Managed Microsoft AD 使用者新增至具有 的群組 AWS Tools for PowerShell

- 若要將使用者新增至群組，請開啟 PowerShell，並執行下列命令，將目錄 ID、群組和成員名稱取代為您的 AWS Managed Microsoft AD Directory ID，以及群組和成員名稱：

```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -MemberName "jane.doe"
```

從群組中移除使用者

使用 AWS Directory Service Data API，成員可以是使用者、群組或電腦。使用者代表可存取您目錄的個人或實體。群組可讓您一次授予和拒絕多個使用者的許可。

使用下列程序，將 AWS Managed Microsoft AD 使用者移除至 AWS Management Console、 AWS CLI或 中具有使用者和群組管理或 AWS Directory Service Data 的群組 AWS Tools for PowerShell。

> **Important**
>
> 當您從群組中移除 AWS Managed Microsoft AD 使用者時，使用者會失去指派給群組的角色和許可的存取權。這些角色和許可是群組成員資格的一部分。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.

- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始將許可授予使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。
- 建立 AWS Managed Microsoft AD 使用者。
- 建立 AWS Managed Microsoft AD 群組。

AWS Management Console

您可以使用 從 群組中移除 AWS Managed Microsoft AD 成員 AWS Management Console。

使用 從 群組中移除 AWS Managed Microsoft AD 使用者 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Groups (群組)。標籤顯示 中的群組清單 AWS 區域。
5. 選擇群組。若要尋找群組，請在群組區段下的搜尋方塊中輸入群組名稱。系統會將您導向至群組詳細資訊畫面。
6. 選擇成員。標籤會依群組中的成員類型顯示使用者和子群組的清單。
7. 選取您要從群組中移除的使用者，然後選擇移除。若要尋找使用者，請在成員區段下的搜尋方塊中輸入使用者登入名稱。
8. 確認您要從群組中移除使用者，然後再次選擇移除。

AWS CLI

以下說明如何使用 AWS Directory Service Data CLI 格式化從群組中移除 AWS Managed Microsoft AD 成員的請求。

從具有 的群組中移除 AWS Managed Microsoft AD 使用者 AWS CLI

- 若要將使用者移除至群組，請開啟 AWS CLI，然後執行下列命令，將目錄 ID、群組和成員名稱取代為您的 AWS Managed Microsoft AD Directory ID、群組和成員名稱：

```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "your-group-name" --member-name "jane.doe"
```

AWS Tools for PowerShell

以下說明如何格式化從 群組中移除 AWS Managed Microsoft AD 成員的請求 AWS Tools for PowerShell。

從具有 的群組中移除 AWS Managed Microsoft AD 使用者 AWS Tools for PowerShell

- 若要將使用者移除至群組，請開啟 PowerShell，然後執行下列命令，將目錄 ID、群組和成員名稱取代為您的 AWS Managed Microsoft AD Directory ID、群組和成員名稱：

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -MemberName "jane.doe"
```

將群組新增至群組

當您將 AWS Managed Microsoft AD 群組新增至另一個群組時，群組會共用父子關係。子群組可以存取指派給父群組的角色和許可。您可以將子群組新增至您的群組，並將您的群組新增至父群組。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始授予許可給使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。

- 建立 AWS Managed Microsoft AD 群組。

AWS Management Console

您可以使用 將 AWS Managed Microsoft AD 群組新增至群組 AWS Management Console。

使用 將子群組新增至您的群組 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Groups (群組)。標籤顯示 中的群組清單 AWS 區域。
5. 選擇群組。若要尋找群組，請在群組區段下的搜尋方塊中輸入群組名稱。系統會將您導向至群組詳細資訊畫面。
6. 選擇成員。標籤會依群組中的成員類型顯示使用者和子群組的清單。
7. 選擇新增成員。
8. 在成員 （ 成員 ） 下，選取您要新增至群組的子群組，然後選擇新增成員至群組。

使用 將父群組新增至群組 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Groups (群組)。標籤顯示 中的群組清單 AWS 區域。
5. 選擇群組。若要尋找群組，請在群組區段下的搜尋方塊中輸入群組名稱。系統會將您導向至群組詳細資訊畫面。
6. 選擇父群組。標籤顯示您的群組所屬的群組清單。
7. 選擇新增父群組。
8. 在群組 （ 群組 ） 下，選取您要新增群組的群組，然後再次選擇新增父群組。

AWS CLI

以下說明如何使用 AWS Directory Service Data CLI 格式化將 AWS Managed Microsoft AD 群組新增至群組的請求。

使用 將子群組新增至您的群組 AWS CLI

- 若要將子群組新增至父群組，請開啟 AWS CLI，然後執行下列命令，將目錄 ID、群組和成員名稱取代為您的 AWS Managed Microsoft AD Directory ID、群組和成員名稱：

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

AWS Tools for PowerShell

以下說明如何格式化將 AWS Managed Microsoft AD 群組新增至 群組的請求 AWS Tools for PowerShell。

使用 將子群組新增至您的群組 AWS Tools for PowerShell

- 若要將子群組新增至父群組，請開啟 PowerShell，然後執行下列命令，將目錄 ID、群組和成員名稱取代為您的 AWS Managed Microsoft AD Directory ID、群組和成員名稱：

```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -MemberName "child-group-name"
```

從群組中移除群組

當您從另一個群組移除 AWS Managed Microsoft AD 群組時，群組將不再共用父子關係。子群組無法存取指派給父群組的角色和許可。您可以從您的群組移除子群組，並從父群組移除您的群組。

開始任一程序之前，您需要完成下列各項：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。

- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始授予許可給使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。
- 建立 AWS Managed Microsoft AD 群組。

AWS Management Console

您可以使用 將 AWS Managed Microsoft AD 群組移除至群組 AWS Management Console。

使用 從 群組中移除子群組 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Groups (群組)。標籤顯示 中的群組清單 AWS 區域。
5. 選擇群組。系統會將您導向至群組詳細資訊畫面。若要尋找群組，請在群組區段下的搜尋方塊中輸入群組名稱。
6. 選擇成員。標籤顯示您群組中成員類型的使用者和子群組清單。
7. 選取您要從群組中移除的子群組 （ 然後選取移除)。
8. 確認您要從群組中移除的子群組 （ 然後 ），然後再次選擇移除。

使用 從父群組中移除您的群組 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Groups (群組)。標籤顯示 中的群組清單 AWS 區域。
5. 選擇群組。系統會將您導向至群組詳細資訊畫面。若要尋找群組，請在群組區段下的搜尋方塊中輸入群組名稱。

6. 選擇父群組。標籤顯示群組所屬的群組清單。
7. 選取您要從中移除群組的父群組，然後選擇移除父群組。
8. 確認您要從中移除群組的父群組，然後再次選擇移除父群組。

AWS CLI

以下說明如何使用 AWS Directory Service Data CLI，將移除 AWS Managed Microsoft AD 群組的請求格式化為群組。

- 使用 從父群組中移除子群組 AWS CLI

  若要從父群組新增移除子群組，請開啟 AWS CLI，然後執行下列命令，將目錄 ID、群組和成員名稱取代為您的 AWS Managed Microsoft AD Directory ID、群組和成員名稱：

```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

AWS Tools for PowerShell

以下說明如何將移除 AWS Managed Microsoft AD 群組的請求格式化為 群組 AWS Tools for PowerShell。

- 使用 從父群組中移除子群組 AWS Tools for PowerShell

  若要從父群組新增移除子群組，請開啟 PowerShell，然後執行下列命令，將目錄 ID、群組和成員名稱取代為您的 AWS Managed Microsoft AD Directory ID、群組和成員名稱：

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -MemberName "child-group-name"
```

在 中複製 AWS Managed Microsoft AD 群組成員資格 AWS Management Console

您可以將群組成員資格從一個 AWS Managed Microsoft AD 使用者複製到 中的另一個使用者 AWS Management Console。群組成員資格是使用者在將角色和許可新增至群組時繼承的角色和許可。

開始此程序之前，您需要完成下列項目：

- 建立 AWS Managed Microsoft AD.
- 若要使用使用者和群組管理或 AWS Directory Service Data CLI，必須啟用它。如需詳細資訊，請參閱啟用使用者和群組管理或目錄服務資料。
- 您只能從目錄 AWS 區域 的主要 啟用此功能。如需詳細資訊，請參閱主要區域與額外區域。
- 您需要必要的 IAM 許可才能使用 AWS Directory Service Data。如需詳細資訊，請參閱AWS Directory Service API 許可：動作、資源和條件參考。若要開始將許可授予使用者和工作負載，您可以使用 AWS 受管政策： AWSDirectoryServiceDataFullAccess或 等 AWS 受管政策AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess。如需更多詳細資訊，請參閱 IAM 中的安全最佳實務。
- 建立 AWS Managed Microsoft AD 群組。

使用 複製 AWS Managed Microsoft AD 群組成員資格 AWS Management Console

1. 在 https：//https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
2. 從導覽窗格中，選擇 Active Directory，然後選擇目錄。系統會將您導向目錄畫面，您可以在其中檢視 中的目錄清單 AWS 區域。
3. 選擇目錄。系統會將您導向至目錄詳細資訊畫面。
4. 選擇 Groups (群組)。標籤顯示 中的群組清單 AWS 區域。
5. 選擇您要複製其群組成員資格的帳戶。若要尋找使用者，請在使用者區段下的搜尋方塊中輸入使用者登入名稱。系統會將您導向至使用者詳細資訊畫面。
6. 選擇複製所有群組成員資格。系統會將您導向至一個程序，您可以在其中指定要複製的群組。

    a. 對於要複製的驗證群組，在要複製的群組下，選取具有您要複製之角色和許可的群組，然後選擇下一步。

    b. 對於選取目的地帳戶，在帳戶類型下，選擇現有使用者帳戶，將群組成員資格複製到現有使用者帳戶。或者，選擇新使用者帳戶以建立新的使用者，並將群組成員資格複製到新的使用者帳戶。若要尋找群組，請在所選群組區段下的搜尋方塊中輸入群組的名稱。

        i. （選用）如果您選擇現有的使用者帳戶，請選取您要將角色和許可複製到其中的目的地帳戶，然後選擇下一步。

        ii. （選用）如果您選擇新增使用者帳戶，請完成程序，然後選擇下一步。如需建立使用者的資訊，請參閱 建立使用者。

c. 針對檢閱和複製群組成員資格，檢閱您的選擇，然後選擇複製群組成員資格。

使用 Amazon EC2 執行個體管理使用者和群組

本節包含使用已加入 AWS Managed Microsoft AD 的 Amazon EC2 執行個體來管理使用者和群組的程序。

如果 Directory Service Data API 不支援您的使用案例，建議您使用 Amazon EC2 執行個體管理使用者和群組。如需詳細資訊，請參閱 AWS Directory Service Data API 參考。

> **Note**
>
> 在完成下列主題中的任何程序之前，您必須先安裝 Active Directory 管理工具。如需詳細資訊，請參閱安裝 Active Directory 管理工具。

主題

- 安裝 AWS Managed Microsoft AD 的 Active Directory 管理工具
- 建立 AWS Managed Microsoft AD 使用者
- 使用 Amazon EC2 執行個體刪除使用者帳戶
- 重設 AWS Managed Microsoft AD 使用者密碼
- 建立 AWS Managed Microsoft AD 群組
- 將 AWS Managed Microsoft AD 使用者新增至群組

安裝 AWS Managed Microsoft AD 的 Active Directory 管理工具

您可以使用 Active Directory 管理您的 AWS Managed Microsoft ADActive Directory Domain Services and Active Directory Lightweight Directory Services Tools。若要使用 Active Directory Domain Services and Active Directory Lightweight Directory Services Tools，您需要安裝它們。下列程序會逐步解說如何在 Amazon EC2 Windows Server 執行個體或 PowerShell命令上安裝這些工具。或者，您可以啟動已安裝這些工具的目錄管理 EC2 執行個體。

EC2 Windows Server instance

請先完成下列步驟，才能開始此程序：

1. 建立 AWS Managed Microsoft ADActive Directory。如需詳細資訊，請參閱建立 AWS Managed Microsoft AD。
2. 啟動 EC2 Windows Server 執行個體並將其加入您的 AWS Managed Microsoft AD Active Directory。EC2 執行個體需要下列政策才能建立使用者和群組：**AmazonSSMManagedInstanceCore**和 **AmazonSSMDirectoryServiceAccess**。如需詳細資訊，請參閱在 AWS Managed Microsoft AD 中啟動目錄管理執行個體 Active Directory及將 Amazon EC2 Windows 執行個體加入您的 AWS Managed Microsoft AD Active Directory。
3. 您將需要Active Directory網域管理員的登入資料。這些登入資料是在 AWS Managed Microsoft AD 建立時建立的。如果您遵循 中的程序建立 AWS Managed Microsoft AD，您的管理員使用者名稱會包含您的 NetBIOS 名稱 **corp\admin**。

在 EC2 Windows Server 執行個體上安裝Active Directory管理工具

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在 Amazon EC2 主控台中，選擇 執行個體並選取您剛建立的執行個體，然後選擇連線。
3. 在連線至執行個體頁面中，選擇 RDP 用戶端。
4. 在 RDP 用戶端索引標籤中，選擇下載遠端桌面檔案，然後選擇取得密碼以擷取密碼。
5. 在取得 Windows 密碼中，選擇上傳私有金鑰檔案。選擇與 Windows Server 執行個體關聯的 .pem 私有金鑰檔案。上傳私有金鑰檔案後，選取解密密碼。
6. 在 Windows 安全對話方塊中，複製 Windows Server 電腦的本機管理員登入資料以登入。使用者名稱可以是下列格式：***NetBIOS-Name*\admin**或***DNS-Name*\admin**。例如，如果您遵循中的程序，**corp\admin** 會是使用者名稱建立 AWS Managed Microsoft AD。
7. 登入 Windows Server 執行個體後，請選擇 Server Manager，從開始功能表開啟 Server Manager。
8. 在伺服器管理員儀表板中，選擇新增角色和功能。
9. 在 Add Roles and Features Wizard (新增角色和功能精靈) 中選擇 Installation Type (安裝類型)，並選取 Role-based or feature-based installation (角色型或功能型安裝)，接著選擇 Next (下一步)。
10. 在 Server Selection (伺服器選項) 下，請確認本機伺服器已選取，然後在左側導覽窗格中選擇 Features (功能)。
11. 在功能樹狀目錄中，開啟遠端伺服器管理工具和角色管理工具，接著選取 AD DS 和 AD LDS 工具。選取 AD DS 和 AD LDS 工具後，會選取 、AD DS 工具和 AD LDS Snap-in 和 Command-Line Tools Active Directory的模組PowerShell。向下捲動並選取 DNS 伺服器工具，然後選擇下一步。

12. 請檢閱資訊，然後選擇 Install (安裝)。功能安裝完成後，即可在「開始」功能表的系統管理工具 資料夾中，使用 Active Directory 域服務和 Active Directory 輕量型目錄服務工具。

PowerShell

您可以使用 安裝 Active Directory 管理工具PowerShell。例如，您可以從 PowerShell 提示字元使用 `Install-WindowsFeature RSAT-ADDS` 來安裝 Active Directory 遠端管理工具。如需詳細資訊，請參閱 Microsoft 網站上的 Install-WindowsFeature。

Directory administration instance

您可以依照 中的程序，在已安裝 Active Directory Domain Services 和 Active Directory Lightweight Directory Services Tools 的 AWS Management Console 中啟動目錄管理 EC2 執行個體在 AWS Managed Microsoft AD 中啟動目錄管理執行個體 Active Directory。

建立 AWS Managed Microsoft AD 使用者

您可以使用 Active Directory管理工具和 建立 AWS Managed Microsoft AD 使用者PowerShell。您必須先完成 中的程序，才能使用 Active Directory管理工具建立使用者安裝 AWS Managed Microsoft AD 的 Active Directory 管理工具。

Active Directory Administration Tools

使用下列程序透過 Active Directory管理工具建立 AWS Managed Microsoft AD 使用者。

1. 連線至安裝了 Active Directory 管理工具的執行個體。
2. 從 Windows 開始功能表開啟 Active Directory 使用者和電腦工具。您可以在 Windows 管理工具資料夾中找到此工具的捷徑。

> **Tip**
>
> 您可以在執行個體上透過命令提示執行下列命令，以直接開啟 Active Directory 使用者和電腦工具箱。
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. 在目錄樹狀目錄中，選取您要存放使用者的目錄 NetBIOS 名稱 OU 下的 OU （例如 **corp\Users**)。如需 中目錄使用的 OU 結構的詳細資訊 AWS，請參閱 使用 AWS Managed Microsoft AD 建立的內容。

4. 在動作選單上，選擇新增，再選擇使用者開啟新增使用者精靈。
5. 在精靈的第一頁上，輸入下列欄位的值，然後選擇下一步。
   - 名字
   - 姓氏
   - User logon name (使用者登入名稱)
6. 在精靈的第二頁上，針對密碼和確認密碼輸入臨時密碼。確定使用者必須在下次登入時變更密碼選項已選取。其他選項則不需選取。選擇下一步。
7. 在精靈的第三頁上，確認新使用者的資訊正確，然後選擇完成。新使用者就會顯示在 Users (使用者) 資料夾中。

PowerShell

使用下列程序透過 建立 AWS Managed Microsoft AD 使用者PowerShell。

1. 以Active Directory管理員身分連線至加入您Active Directory網域的執行個體。
2. 打開 PowerShell.
3. 輸入下列命令，將使用者名稱取代為您要建立**jane.doe**的使用者名稱。系統會提示您為新使用者PowerShell提供密碼。如需Active Directory密碼複雜性需求的詳細資訊，請參閱 Microsoft 文件。如需 New-ADUser 命令的詳細資訊，請參閱 Microsoft 文件。

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -
AsSecureString 'Password')
```

使用 Amazon EC2 執行個體刪除使用者帳戶

您可以使用下列程序來刪除已加入 AWS Managed Microsoft AD 的 Amazon EC2 執行個體的使用者。

> **Note**
>
> 完成此程序之前，您必須安裝 Active Directory 管理工具。如需詳細資訊，請參閱安裝 Active Directory 管理工具。

若要刪除使用者

1. 開啟 Active Directory 使用者和電腦工具。Windows 系統管理工具資料夾具有此工具的捷徑。

   > **Tip**
   >
   > 您可以在執行個體上透過命令提示執行下列命令，以直接開啟 Active Directory 使用者和電腦工具箱。
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

2. 在目錄樹中，選取包含要刪除的使用者的 OU (例如，"Corp\Users")。
3. 選取要刪除的使用者。在動作功能表上，選擇刪除。
4. 將出現一個對話方塊，提示您確認要刪除該使用者。選擇是以刪除使用者。

刪除的使用者暫時儲存在 AD 資源回收筒。如需 AD 資源回收筒的詳細資訊，請參閱 Microsoft 的 Ask the Directory Services Team 部落格中的 The AD Recycle Bin: Understanding, Implementing, Best Practices, and Troubleshooting 一文。

重設 AWS Managed Microsoft AD 使用者密碼

使用者必須遵守 中定義的密碼政策Active Directory。有時這可以充分利用使用者，包括Active Directory管理員，他們忘記密碼。發生這種情況時， AWS Directory Service 如果使用者駐留 AWS Managed Microsoft AD，您可以使用 快速重設使用者的密碼。

您必須以具有重設密碼所需許可的使用者身分登入。如需許可的詳細資訊，請參閱「管理 AWS Directory Service 資源存取許可的概觀」。

您可以為 中的任何使用者重設密碼，Active Directory但有下列例外：

- 您可以根據建立 時使用的 NetBIOS 名稱，重設組織單位 (OU) 內任何使用者的密碼Active Directory。例如，如果您遵循 建立 AWS Managed Microsoft AD NetBIOS 名稱中的程序將是 CORP，而您可以重設的使用者密碼將是 Corp/Users OU 的成員。
- 您無法根據建立 時所使用的 NetBIOS 名稱，重設 OU 外任何使用者的密碼Active Directory。例如，您無法重設AWS 預留 OU 中使用者的密碼。如需 AWS Managed Microsoft AD 的 OU 結構的詳細資訊，請參閱 使用 AWS Managed Microsoft AD 建立的內容。

如需在 AWS Managed Microsoft AD 中重設密碼時如何套用密碼政策的詳細資訊，請參閱 如何套用密碼政策。

您可以使用下列任一工具來重設 AWS Managed Microsoft AD 使用者密碼：

- AWS Management Console
- AWS CLI
- PowerShell

AWS Management Console

使用下列程序，使用 重設 AWS Managed Microsoft AD 使用者密碼 AWS Management Console。

1. 在AWS Directory Service 主控台導覽窗格的 Active Directory 下，選擇目錄，然後在清單中選取Active Directory您要重設使用者密碼的 。
2. 在目錄詳細資訊頁面上，選擇動作，然後選擇重設密碼。
3. 在重設使用者密碼對話方塊中，在使用者名稱中輸入密碼需要變更的使用者名稱。
4. 在新密碼和確認密碼中輸入密碼，然後選擇重設密碼。

AWS CLI

使用下列程序，透過 重設 AWS Managed Microsoft AD 使用者密碼 AWS CLI。

1. 若要安裝 AWS CLI，請參閱安裝或更新最新版本的 AWS CLI。
2. 開啟 AWS CLI。
3. 輸入下列命令，並將目錄 ID、使用者名稱和密碼取代**`jane.doeP@ssw0rd`**為您的Active Directory目錄 ID 和所需登入資料。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 reset-user-password 一節。

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

PowerShell

使用下列程序，透過 重設 AWS Managed Microsoft AD 使用者密碼PowerShell。

1. 以Active Directory管理員身分連線至加入您Active Directory網域的執行個體。
2. 打開 PowerShell.
3. 輸入下列命令，將使用者名稱 **jane.doe**、目錄 ID 和密碼**P@ssw0rd**取代為您的Active Directory目錄 ID 和所需登入資料。如需詳細資訊，請參閱 Reset-DSUserPassword Cmdlet。

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

建立 AWS Managed Microsoft AD 群組

您可以在 AWS Managed Microsoft AD 中建立群組。使用下列程序，以加入 AWS Managed Microsoft AD 目錄的 Amazon EC2 執行個體建立安全群組。在建立安全群組之前，您需要完成安裝 Active Directory 管理工具中所述的程序。

Active Directory Administration Tools

使用下列程序，透過 Active Directory管理工具建立 AWS Managed Microsoft AD 群組。

建立群組

1. 連線至安裝了 Active Directory 管理工具的執行個體。
2. 開啟 Active Directory 使用者和電腦工具。系統管理工具資料夾具有此工具的捷徑。

> **Tip**
>
> 您可以在執行個體上透過命令提示執行下列命令，以直接開啟 Active Directory 使用者和電腦工具箱。
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. 在樹狀目錄中，在目錄的 NetBIOS 名稱 OU 下選取要在其中儲存群組的 OU (例如，"Corp \Users")。如需 中目錄使用的 OU 結構的詳細資訊 AWS，請參閱 使用 AWS Managed Microsoft AD 建立的內容。

4. 在 Action (動作) 選單上，按一下 New (新增)，再按一下 Group (群組) 開啟新增群組精靈。
5. 在群組名稱中輸入群組名稱，選取滿足您需求的群組範圍，然後為群組類型選取安全性。如需 Active Directory 群組範圍和安全群組的詳細資訊，請參閱 Microsoft Windows Server 文件中的 Active Directory 安全群組一節。
6. 按一下 OK (確定)。新安全群組就會顯示在使用者資料夾中。

PowerShell

您可以使用 PowerShell 命令來建立群組。如需詳細資訊，請參閱 Windows Server 2022 PowerShell 文件中的 New–ADGroup 一節。

將 AWS Managed Microsoft AD 使用者新增至群組

您可以將 AWS Managed Microsoft AD 使用者新增至群組。使用下列程序，將使用者新增至已加入 AWS Managed Microsoft AD 目錄的 Amazon EC2 執行個體的安全群組。

Active Directory Administration Tools

將使用者新增至群組

1. 連線至安裝了 Active Directory 管理工具的執行個體。
2. 開啟 Active Directory 使用者和電腦工具。系統管理工具資料夾具有此工具的捷徑。

> **Tip**
>
> 您可以在執行個體上透過命令提示執行下列命令，以直接開啟 Active Directory 使用者和電腦工具箱。
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. 在樹狀目錄中，選取目錄的 NetBIOS 名稱 OU 下儲存群組的 OU，然後選取要向其新增使用者為成員的群組。

4. 在動作選單上，按一下屬性開啟群組的屬性對話方塊。
5. 選取成員索引標籤，然後按一下新增...。
6. 對於輸入要選取的物件名稱，輸入您要新增的使用者名稱，然後按一下確定。相應名稱將顯示在成員清單中。再按一次 OK (確定) 以更新群組成員資格。
7. 透過在使用者資料夾中選取使用者並點選動作選單中的屬性開啟屬性對話方塊，確認使用者現在是否是該群組的成員。選取成員群組索引標籤。您應該可以在群組清單中看到使用者所屬的群組的名稱。

AWS 目錄服務資料

AWS Directory Service Data 是 的延伸 AWS Directory Service。您可以從 AWS Directory Service for Microsoft Active Directory 建立、讀取、更新和 Active Directory(AD) 使用者、群組和成員資格，而無需在 Amazon EC2 執行個體上部署專用 AD 管理執行個體。您也可以跨目錄執行內建的物件管理任務，無需任何直接網路連線。這可簡化佈建和存取管理，以實現全自動化部署。如需詳細資訊，請參閱 AWS Directory Service Data API 參考 。

Directory Service Data 支援組織單位 (OU) 中 AWS Managed Microsoft AD 內的使用者和群組寫入操作`CreateGroup`，例如 `CreateUser`和 。Directory Service Data 支援讀取操作，例如 `ListUsers`和 `ListGroups`，適用於 AWS Managed Microsoft AD 和受信任領域內的所有使用者、群組和群組成員資格。Directory Service Data 支援從 OU 和 AWS 委派群組 OU 中的群組新增和移除群組成員，因此您可以透過將使用者新增至特定委派群組物件來委派許可。如需詳細資訊，請參閱AWS Managed Microsoft AD 中的使用者和群組管理。

> **Note**
>
> Directory Service Data 僅適用於您的主要區域。如需詳細資訊，請參閱主要區域與其他區域。

主題

- 複寫和一致性
- AWS Directory Service Data 屬性
- 群組類型和群組範圍

複寫和一致性

Directory Service Data API 會連線至 AWS Managed Microsoft AD 網域控制站，以對基礎目錄物件執行操作。 Active Directory是最終一致的平台，而且在 AWS Directory Service 目錄網域控制站之間會持續進行複寫。根據預設，每個 AWS Directory Service 目錄都是使用兩個網域控制站建立的。

Directory Service Data 會嘗試跨請求使用相同的網域控制站來維持一致的體驗。如果網域控制站無法使用， Directory Service Data 會切換到替代網域控制站。在這些事件期間，您可能會注意到網域控制站之間的最終一致性，而物件會跨網域控制站複寫。

目錄限制因 AWS Managed Microsoft AD 版本而異：

- 標準版 – 支援讀取操作每秒 8 次交易，每個目錄寫入操作每秒 4 次 TPS。
- 企業版 – 支援讀取操作每秒 16 筆交易，每個目錄寫入操作每秒 8 筆 TPS。

> **Note**
>
> 標準版和企業版的並行請求有 10 個並行限制。

- AWS 帳戶 – 支援所有目錄的 Directory Service Data 操作每秒總共 100 筆交易。

AWS Directory Service Data 屬性

本主題說明如何使用 AWS Directory Service Data API 參考中的屬性。

請求屬性

必須在請求內文參數中定義下列屬性。如需如何定義這些屬性的範例，請參閱 AWS Directory Service Data API 參考中的 CreateGroup。

Directory Service Data 屬性名稱	LDAP 顯示名稱	AWS Management Console	PowerShell 別名	存取類型	物件類型	屬性值	可搜尋
DistinguishedName	distinguishedName	辨別名稱	無	ReadOnly	使用者、群組	字串	否

Directory Service Data 屬性名稱	LDAP 顯示名稱	AWS Management Console	PowerShell 別名	存取類型	物件類型	屬性值	可搜尋
EmailAddress	郵件	電子郵件地址	EmailAddress	可建立	使用者	字串	是
已啟用	無	已啟用	已啟用	Mutable	使用者	Boolean	否
GivenName	givenName	名字	GivenName	可建立	使用者	字串	是
GroupScope	groupScope	Group scope (群組範圍)	無	可建立	群組	列舉	否
GroupType	groupType	Group type (群組類型)	無	可建立	群組	列舉	否
SamAccountName	sAMAccountName	User logon name (使用者登入名稱)	sAMAccountName	可建立	使用者、群組	字串	是
SID	objectSid	使用者/群組安全識別符 (SID)	SID	ReadOnly	使用者、群組	字串	否
姓氏	sn	姓氏	Surname	可建立	使用者	字串	是
UserPrincipalName	userPrincipalName	使用者主體名稱	UserPrincipalName	ReadOnly	使用者	字串	否

其他屬性

下列屬性必須在 中定義`OtherAttributes`，且不對應至任何請求內文參數。當您在請求中定義其他屬性時，您必須指定屬性名稱、資料類型和每個屬性的值。如需如何定義這些屬性的範例，請參閱 AWS Directory Service Data API 參考中的 CreateUser。

> **Note**
>
> 這些屬性的名稱在做為輸入提供時不區分大小寫，且相當於 LDAP 顯示名稱。

Directory Service Data 屬性名稱	LDAP 顯示名稱	AWS Management Console	PowerShell 別名	存取類型	物件類型	屬性值	可搜尋
助理	助理	助理	無	ReadOnly	使用者	字串	否
Cn	cn	Common Name (通用名稱)	無	ReadOnly	使用者、群組	字串	否
Co	Co	國家/區域	Country	Mutable	使用者	字串	否
公司	company	公司	公司	可建立	使用者	字串	否
部門	department	Department	Department	可建立	使用者	字串	否
Description	description	描述	描述	可建立	使用者、群組	字串	否
DirectReports	directReports	直屬員工	無	ReadOnly	使用者	字串集	否
DisplayName	displayName	顯示名稱	DisplayName	可建立	使用者、群組	字串	是

Directory Service Data 屬性名稱	LDAP 顯示名稱	AWS Management Console	PowerShell 別名	存取類型	物件類型	屬性值	可搜尋
Facsimile Telephone Number	facsimile Telephone Number	Fax	Fax	可建立	使用者、群組	字串	否
HomePhon	homePhone	住家電話號碼	HomePhon	可建立	使用者	字串	否
Info (資訊)	info	備註	無	Mutable	使用者、群組	字串	否
縮寫	初始	Initials	Initials	ReadOnly	使用者	字串	否
IpPhone	ipPhone	IP 電話	無	Mutable	使用者	字串	否
L	l	City	City	可建立	使用者	字串	是
管理員	manager	管理員	管理員	Mutable	使用者	字串	否
Mail (信件)	郵件	電子郵件地址	EmailAddress	Mutable	群組	字串	是
行動應用程式	mobile	行動電話號碼	MobilePhone	Mutable	使用者	字串	否
ObjectClass	objectClass	使用者/群組	無	ReadOnly	群組	字串	否
ObjectGUID	objectGUID	全域唯一識別符 (GUID)	無	ReadOnly	使用者、群組	字串	否
分頁器	分頁器	分頁器	無	Mutable	使用者	字串	否

Directory Service Data 屬性名稱	LDAP 顯示名稱	AWS Management Console	PowerShell 別名	存取類型	物件類型	屬性值	可搜尋
PhysicalDeliveryOfficeName	physicalDeliveryOfficeName	辦公室	無	可建立	使用者	字串	是
PostalCode	postalCode	郵遞區號	PostalCode	可建立	使用者	字串	否
PreferredLanguage	preferredLanguage	偏好的語言	無	Mutable	使用者	字串	否
ProxyAddresses	proxyAddresses	Proxy 地址	無	ReadOnly	使用者、群組	多值字串	是
ServicePrincipalName	servicePrincipalName	服務委託人名稱	ServicePrincipalName	Mutable	使用者	多值字串	否
聖	st	州/省	State	可建立	使用者	字串	否
StreetAddress	streetAddress	街道地址	StreetAddress	可建立	使用者	字串	否
TelephoneNumber	telephoneNumber	電話號碼	OfficePhone	可建立	使用者	字串	否
標題	標題	職稱	Title	ReadOnly	使用者	字串	否
WhenChanged	whenChanged	上次更新	無	ReadOnly	使用者、群組	字串	否
WWWHomePage	wWWHomePage	首頁 URL	wWWHomePage	Mutable	使用者、群組	字串	否

群組類型和群組範圍

AWS Managed Microsoft AD 中的群組同時具有群組類型和群組範圍。如需每個章節的詳細資訊，請參閱下列各節。

主題

- Group type (群組類型)
- Group scope (群組範圍)

Group type (群組類型)

群組類型決定Active Directory群組成員可存取哪些共用資源。有兩種群組類型：

- 安全性 - 您可以指派許可給這些群組，讓群組成員存取共用Active Directory資源。
- 分佈 - 您可以使用此類型建立電子郵件分佈清單。這些群組成員無法存取Active Directory共用資源。

在群組類型之間變更時沒有限制。

如需群組類型的詳細資訊，請參閱 Microsoft 文件。

Group scope (群組範圍)

群組範圍決定如何使用網域樹狀目錄或樹系定義群組成員。有三個群組範圍：

- 網域本機 - 將許可指派給位於相同網域中的群組成員。
- 通用 - 將許可指派給位於任何網域中的群組成員。
- 全域 - 將許可指派給位於任何網域或樹系中的群組成員。

變更群組範圍時有限制。下列清單和圖表概述了這些限制。

- 將群組範圍從網域本機變更為全域 - 是
  - 除非網域本機群組是另一個網域本機群組的父系。
- 將群組範圍從全域變更為網域本機 - 是
  - 除非通用群組是另一個通用群組的子群組。
- 將群組範圍從全域變更為全域 - 是
  - 除非通用群組是另一個通用群組的父群組。

- 將群組範圍從全域變更為全域 - 是
  - 除非全域群組是另一個全域群組的子群組。

如需群組範圍的詳細資訊，請參閱 Microsoft 文件。

將您的 AWS Managed Microsoft AD 連線至 Microsoft Entra Connect Sync

本教學課程會逐步解說安裝 的必要步驟Microsoft Entra Connect Sync，以將 同步Microsoft Entra ID至 AWS Managed Microsoft AD。

在此教學課程中，您將執行下列操作：

1. 建立 AWS Managed Microsoft AD 網域使用者。
2. 下載 Entra Connect Sync。
3. 使用 PowerShell執行指令碼，為新建立的使用者佈建適當的許可。
4. 安裝 Entra Connect Sync。

先決條件

完成本教學課程需要以下各項：

- AWS Managed Microsoft AD。如需詳細資訊，請參閱the section called “建立 AWS Managed Microsoft AD”。
- 加入 AWS Managed Microsoft AD 的 Amazon EC2 Windows Server 執行個體。如需詳細資訊，請參閱加入 Windows 執行個體。
- 安裝 Active DirectoryAdministration Tools以管理 AWS Managed Microsoft AD 的 EC2 Windows 伺服器。如需詳細資訊，請參閱the section called “安裝 AD 管理工具”。

建立Active Directory網域使用者

本教學課程假設您已經安裝 AWS Managed Microsoft AD 和 EC2 Windows Server 執行個體Active DirectoryAdministration Tools。如需詳細資訊，請參閱the section called “安裝 AD 管理工具”。

1. 連線至安裝 Active Directory Administration Tools 的執行個體。
2. 建立 AWS Managed Microsoft AD 網域使用者。此使用者將成為 Active Directory Directory Service (AD DS) Connector account的 Entra Connect Sync。如需此程序的詳細步驟，請參閱 the section called “建立使用者”。

下載 Entra Connect Sync

- Entra Connect Sync 從 Microsoft網站下載到做為 AWS Managed Microsoft AD 管理員的 EC2 執行個體。

> **Warning**
>
> Entra Connect Sync 此時請勿開啟或執行 。後續步驟將為步驟 1 中建立的網域使用者佈建必要的許可。

執行PowerShell指令碼

- 以管理員PowerShell身分開啟 並執行下列指令碼。

  指令碼執行時，系統會要求您為步驟 1 中新建立的網域使用者輸入 sAMAccountName。

  > **Note**
  >
  > 如需執行指令碼的詳細資訊，請參閱下列內容：
  >
  > - 您可以將具有 ps1副檔名的指令碼儲存到類似 的資料夾**temp**。然後，您可以使用下列PowerShell命令載入指令碼：
  >
  >   ```
  >   import-module "c:\temp\entra.ps1"
  >   ```
  >
  > - 載入指令碼後，您可以使用下列命令來設定執行指令碼的必要許可，以您的Entra服務帳戶名稱取代 *Entra_Service_Account_Name*：
  >
  >   ```
  >   Set-EntraConnectSvcPerms -ServiceAccountName Entra_Service_Account_Name
  >   ```

```
$modulePath = "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig
\AdSyncConfig.psm1"

try {
    # Attempt to import the module
    Write-Host -ForegroundColor Green "Importing Module for Azure Entra Connect..."
    Import-Module $modulePath -ErrorAction Stop
    Write-Host -ForegroundColor Green "Success!"
}
catch {
    # Display the exception message
    Write-Host -ForegroundColor Red "An error occurred: $($_.Exception.Message)"
}

Function Set-EntraConnectSvcPerms {
    [CmdletBinding()]
    Param (
        [String]$ServiceAccountName
    )

    #Requires -Modules 'ActiveDirectory' -RunAsAdministrator

    Try {
        $Domain = Get-ADDomain -ErrorAction Stop
    } Catch [System.Exception] {
        Write-Output "Failed to get AD domain information $_"
    }

    $BaseDn = $Domain | Select-Object -ExpandProperty 'DistinguishedName'
    $Netbios = $Domain | Select-Object -ExpandProperty 'NetBIOSName'

    Try {
        $OUs = Get-ADOrganizationalUnit -SearchBase "OU=$Netbios,$BaseDn" -
SearchScope 'Onelevel' -Filter * -ErrorAction Stop | Select-Object -ExpandProperty
 'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get OUs under OU=$Netbios,$BaseDn $_"
    }

    Try {
        $ADConnectorAccountDN = Get-ADUser -Identity $ServiceAccountName -ErrorAction
 Stop | Select-Object -ExpandProperty 'DistinguishedName'
    } Catch [System.Exception] {
```

```
        Write-Output "Failed to get service account DN $_"
    }

    Foreach ($OU in $OUs) {
        try {
        Set-ADSyncMsDsConsistencyGuidPermissions -ADConnectorAccountDN
 $ADConnectorAccountDN -ADobjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Permissions set successfully for $ADConnectorAccountDN and $OU"

        Set-ADSyncBasicReadPermissions -ADConnectorAccountDN $ADConnectorAccountDN -
ADobjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Basic read permissions set successfully for $ADConnectorAccountDN
 on OU $OU"
    }
    catch {
        Write-Host "An error occurred while setting permissions for
 $ADConnectorAccountDN on OU $OU : $_"
    }
    }
}
```

安裝 Entra Connect Sync

1. 指令碼完成後，您可以執行下載的 Microsoft Entra Connect (先前稱為 Azure Active Directory Connect) 組態檔案。
2. 在執行上一個步驟的組態檔案之後，會開啟一個MicrosoftAzure Active Directory Connect視窗。在快速設定視窗中，選取自訂。

3. 在安裝必要的元件視窗中，選取使用現有的服務帳戶核取方塊。在服務帳戶名稱和服務帳戶密碼中，輸入您在步驟 1 中建立AD DS Connector account的使用者名稱和密碼。例如，如果您AD DS Connector account的名稱是 `entra`，帳戶名稱會是 `corp\entra`。然後選取安裝。

4. 在使用者登入視窗中，選取下列其中一個選項：

    a. 傳遞身分驗證 - 此選項可讓您Active Directory使用使用者名稱和密碼登入您的 。

    b. 請勿設定 - 這可讓您搭配 Microsoft Entra (先前稱為 Azure Active Directory(Azure AD)) 或 使用聯合登入Office 365。

    然後選取下一步。

5. 在連線至Azure視窗中，輸入 的全域管理員使用者名稱和密碼Entra ID，然後選取下一步。
6. 在連接目錄視窗中，選擇 Active Directory 作為目錄類型。選擇 AWS Managed Microsoft AD for FOREST 的樹系。然後選取新增目錄。
7. 隨即出現一個快顯方塊，要求您提供帳戶選項。選取使用現有的 AD 帳戶。輸入在步驟 1 中建立的AD DS Connector account使用者名稱和密碼，然後選取確定。然後選取下一步。
8. 在Azure AD登入視窗中，選取繼續，而不將所有 UPN 尾碼與已驗證網域相符，只有在您沒有將已驗證的虛設網域新增至 時Entra ID。然後選取下一步。
9. 在網域/OU 篩選視窗中，選取符合您需求的選項。如需詳細資訊，請參閱 Entra Connect Sync：在文件中設定篩選。 Microsoft然後選取下一步。
10. 在識別使用者、篩選和選用功能視窗中，保留預設值，然後選取下一步。
11. 在設定視窗中，檢閱組態設定，然後選取設定。的安裝Entra Connect Sync將完成，使用者將開始與 同步Microsoft Entra ID。

AWS Managed Microsoft AD 測試實驗室教學課程

本節提供一系列引導式教學課程，協助您在 中建立測試實驗室環境，您可以在 AWS 其中實驗 AWS Managed Microsoft AD。

主題

- 教學課程：在 中設定您的基礎 AWS Managed Microsoft AD 測試實驗室 AWS
- 教學課程：在 Amazon EC2 上建立從 AWS Managed Microsoft AD 到自我管理 Active Directory 安裝的信任

教學課程：在 中設定您的基礎 AWS Managed Microsoft AD 測試實驗室 AWS

本教學課程說明如何設定您的 AWS 環境，以準備新的 AWS Managed Microsoft AD 安裝，該安裝使用執行 Windows Server 2019 的新 Amazon EC2 執行個體。然後，它會教導您使用典型的 Active Directory 管理工具，從 EC2 Windows 執行個體管理 AWS Managed Microsoft AD 環境。完成教學課程時，您將設定網路先決條件，並設定新的 AWS Managed Microsoft AD 樹系。

如下圖所示，您從本教學課程中建立的實驗室是實際了解 AWS Managed Microsoft AD 的基礎元件。您可以稍後新增選用教學，以取得更多實作體驗。此教學系列適合所有剛開始使用 AWS Managed Microsoft AD，並需要測試實驗室進行評估的人。此教學約需 1 小時方能完成。

步驟 1：設定 Managed AWS Microsoft AD Active Directory AWS 的環境

完成先決條件任務後，您可以在 EC2 執行個體中建立和設定 Amazon VPC。

步驟 2：建立 AWS Managed Microsoft AD Active Directory

在此步驟中，您 AWS 第一次在 中設定 AWS Managed Microsoft AD。

步驟 3：部署 Amazon EC2 執行個體以管理您的 AWS Managed Microsoft AD Active Directory

在此步驟中，您會演練讓用戶端電腦連線到新的網域，並在 EC2 中設定新 Windows Server 系統所需的各種部署後任務。

步驟 4：確認基礎測試實驗室可運作

最後，身為管理員，您會確認可從 EC2 中的 Windows Server 系統登入並連線到 AWS Managed Microsoft AD。一旦成功測試實驗室可運作，您可以繼續新增其他測試實驗室指南模組。

先決條件

如果您只打算使用此教學中的 UI 步驟來建立測試實驗室，則可以略過「必要條件」一節並前往「步驟 1」。不過，如果您打算使用 AWS CLI 命令或 AWS Tools for Windows PowerShell 模組來建立測試實驗室環境，您必須先設定下列項目：

- 具有存取和私密存取金鑰的 IAM 使用者 – 如果您想要使用 AWS CLI 或 AWS Tools for Windows PowerShell 模組，則需要具有存取金鑰的 IAM 使用者。如果您沒有存取金鑰，請參閱建立、修改和檢視存取金鑰 (AWS Management Console)。
- AWS Command Line Interface （選用） – 在 Windows AWS CLI 下載並安裝 。安裝完成後，開啟命令提示字元或PowerShell視窗，然後輸入 `aws configure`。請注意，您需要存取金鑰和私密金鑰才能完成設定。請參閱第一個必要條件中的做法步驟。系統會提示您輸入下列資訊：
  - AWS 存取金鑰 ID 【無】： `AKIAIOSFODNN7EXAMPLE`
  - AWS 私密存取金鑰 【無】： `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
  - 預設區域名稱 [無]：`us-west-2`
  - 預設輸出格式 [無]：`json`
- AWS Tools for Windows PowerShell (選用) – 從 https://aws.amazon.com/powershell/ 下載並安裝最新版 AWS Tools for Windows PowerShell ，然後執行下列命令。請注意，您需要存取金鑰和私密金鑰才能完成設定。請參閱第一個必要條件中的做法步驟。

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey
{wJalrXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY} -StoreAs {default}
```

步驟 1：設定 Managed AWS Microsoft AD Active Directory AWS 的環境

您必須先設定 Amazon EC2 金鑰對，以便加密所有登入資料，才能在 AWS 測試實驗室中建立 AWS Managed Microsoft AD。

建立金鑰對

如果您已有金鑰對，則可以略過此步驟。如需 Amazon EC2 金鑰對的詳細資訊，請參閱建立金鑰對。

建立一組金鑰對

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/ec2/ ：// 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 Network & Security (網路與安全) 下，選擇 Key Pairs (金鑰對)，然後選擇 Create Key Pair (建立金鑰對)。
3. 在 Key pair name (金鑰對名稱) 中，輸入 **`AWS-DS-KP`**。在 Key pair file format (金鑰對檔案格式) 中，選取 pem，然後選擇 Create (建立)。
4. 您的瀏覽器會自動下載私有金鑰檔案。檔案名稱是您在建立金鑰對時所指定的名稱，副檔名為 `.pem`。將私有金鑰檔案存放在安全的地方。

> **Important**
>
> 這是您儲存私有金鑰檔案的唯一機會。當您每次解密執行個體密碼來啟動執行個體與對應的私有金鑰時，都需要提供您的金鑰對名稱。

建立、設定和對等兩個 Amazon VPCs

如下圖所示，完成此多步驟程序時，您將建立並設定兩個公有 VPC、每個 VPC 兩個公有子網路、每個 VPC 一個網際網路閘道，並在 VPC 之間設定一個 VPC 對等連線。為求簡單易用和成本考量，我們選擇使用公有 VPC 和子網路。對於生產工作負載，建議您使用私有 VPC。如需更多改善 VPC 安全的相關資訊，請參閱 Security in Amazon Virtual Private Cloud (Amazon Virtual Private Cloud 的安全)。

所有 AWS CLI 和 PowerShell 範例都使用來自下方的 VPC 資訊，並內建於 us-west-2 中。您可以選擇任何支援的區域來建立您的環境。如需一般資訊，請參閱 What is Amazon VPC? (什麼是 Amazon VPC)？。

步驟 1：建立兩個 VPC

在此步驟中，您需要使用下表中指定的參數在相同帳戶中建立兩個 VPCs。 AWS 受管 Microsoft AD 支援使用具有 共用您的 AWS Managed Microsoft AD功能的個別帳戶。第一個 VPC 將用於 AWS Managed Microsoft AD。第二個 VPC 將用於稍後可在 教學課程：在 Amazon EC2 上建立從 AWS Managed Microsoft AD 到自我管理 Active Directory 安裝的信任 中使用的資源。

Managed Active Directory VPC 資訊	內部部署 VPC 資訊
名稱標籤： AWS-DS-VPC01	名稱標籤： AWS-OnPrem-VPC01
IPv4 CIDR 區塊：10.0.0.0/16	IPv4 CIDR 區塊：10.100.0.0/16
IPv6 CIDR block (IPv6 CIDR 區塊): 無 IPv6 CIDR 區塊	IPv6 CIDR block (IPv6 CIDR 區塊): 無 IPv6 CIDR 區塊
租用：預設	租用：預設

如需詳細說明，請參閱 Creating a VPC (建立 VPC)。

步驟 2：為每個 VPC 建立兩個子網路

建立 VPC 後，您需要使用下表的指定參數，為每個 VPC 建立兩個子網路。對於這個測試實驗室，每個子網路都會是 /24。這將讓每個子網路發出多達 256 個地址。每個子網路都必須位於不同可用區域中。將每個子網路放在不同可用區域中的獨立子網路是 建立 AWS Managed Microsoft AD 的先決條件的其中之一。

AWS-DS-VPC01 子網路資訊：	AWS-OnPrem-VPC01 子網路資訊
名稱標籤： AWS-DS-VPC01-Subnet01	名稱標籤： AWS-OnPrem-VPC01-Subnet01
VPC：vpc-xxxxxxxxxxxxxxxxx AWS-DS-VPC01	VPC：vpc-xxxxxxxxxxxxxxxxx AWS-OnPrem-VPC01
可用區域：us-west-2a	可用區域：us-west-2a

AWS-DS-VPC01 子網路資訊：	AWS-OnPrem-VPC01 子網路資訊
IPv4 CIDR 區塊：10.0.0.0/24	IPv4 CIDR 區塊：10.100.0.0/24
名稱標籤： AWS-DS-VPC01-Subnet02 VPC：vpc-xxxxxxxxxxxxxxxxx AWS-DS-VPC01 可用區域：us-west-2b IPv4 CIDR 區塊：10.0.1.0/24	名稱標籤： AWS-OnPrem-VPC01-Subnet02 VPC：vpc-xxxxxxxxxxxxxxxxx AWS-OnPrem-VPC01 可用區域：us-west-2b IPv4 CIDR 區塊：10.100.1.0/24

如需詳細說明，請參閱 Creating a subnet in your VPC (在 VPC 中建立子網路)。

步驟 3：建立網際網路閘道並連接到您的 VPC

由於我們使用的是公有 VPC，因此您將需要使用下表中的指定參數來建立網際網路閘道並將其連接到您的 VPC。這可讓您連接和管理 EC2 執行個體。

AWS-DS-VPC01 網際網路閘道資訊	AWS-OnPrem-VPC01 網際網路閘道資訊
名稱標籤： AWS-DS-VPC01-IGW VPC：vpc-xxxxxxxxxxxxxxxxx AWS-DS-VPC01	名稱標籤： AWS-OnPrem-VPC01-IGW VPC：vpc-xxxxxxxxxxxxxxxxx AWS-OnPrem-VPC01

如需詳細說明，請參閱 Internet gateways (網際網路閘道)。

步驟 4：在 AWS-DS-VPC01 和 AWS-OnPrem-VPC01 之間設定 VPC 對等互連

由於您先前已建立兩個 VPC，因此您將需要使用下表中的指定參數，使用 VPC 對等連線將它們連線在一起。雖然有許多方法可以連接您的 VPCs，但本教學課程將使用 VPC 對等互連。 AWS 受管 Microsoft AD 支援許多解決方案來連接您的 VPCs，其中一些解決方案包括 VPC 對等互連、Transit Gateway 和 VPN。

對等連線名稱標籤： AWS-DS-VPC01&AWS-OnPrem-VPC01-Peer
VPC （請求者）：vpc-xxxxxxxxxxxxxxxxx AWS-DS-VPC01

帳戶：我的帳戶

區域：此區域

VPC （接受者）：vpc-xxxxxxxxxxxxxxxxx AWS-OnPrem-VPC01

如需有關如何使用帳戶中的另一個 VPC 建立 VPC 對等連線的說明，請參閱 Creating a VPC peering connection with another VPC in your account (使用帳戶中的另一個 VPC 建立 VPC 對等連線)。

步驟 5：將兩個路由新增至每個 VPC 的主要路由表

為了讓在先前步驟中建立的網際網路閘道和 VPC 對等連線正常運作，您必須使用下表中的指定參數來更新兩個 VPC 的主路由表。您將新增兩個路由：將路由到路由表未明確知道的所有目的地的 0.0.0.0/0，以及將透過上面建立的 VPC 對等連接路由到每個 VPC 的 10.0.0.0/16 或 10.100.0.0/16。

您可以篩選 VPC 名稱標籤 (AWS-DS-VPC01 或 AWS-OnPrem-VPC01)，輕鬆找到每個 VPC 的正確路由表。

AWS-DS-VPC01 路由 1 資訊	AWS-DS-VPC01 路由 2 資訊	AWS-OnPrem-VPC01 路由 1 資訊	AWS-OnPrem-VPC01 路由 2 資訊
目的地：0.0.0.0/0 目標：igw-xx xxxxxxxxxxxxxxx AWS-DS-VPC01-IGW	目的地：10.10 0.0.0/16 目標：pcx-xx xxxxxxxxxxxxxxx AWS-DS-VP C01&AWS-OnPrem-VPC01-Peer	目的地：0.0.0.0/0 目標：igw-xx xxxxxxxxxxxxxxx AWS-Onprem-VPC01	目的地：10.0.0.0/16 目標：pcx-xx xxxxxxxxxxxxxxx AWS-DS-VP C01&AWS-OnPrem-VPC01-Peer

如需如何將路由新增至 VPC 路由表的說明，請參閱 Adding and removing routes from a route table (從路由表新增和移除路由)。

建立 Amazon EC2 執行個體的安全群組

根據預設， AWS 受管 Microsoft AD 會建立安全群組來管理其網域控制站之間的流量。在本節中，您將需要建立 2 個安全群組 (每個 VPC 一個)，這兩組將用來使用下表中的指定參數，管理 EC2 執行個體 VPC 內的流量。您也會新增一項規則，允許從任何地方傳入的 RDP (3389)，以及從本機 VPC 傳入的所有流量類型。如需詳細資訊，請參閱 Windows 執行個體的 Amazon EC2 安全群組。

AWS-DS-VPC01 安全群組資訊：
安全群組名稱： AWS DS Test Lab 安全群組
描述： AWS DS Test Lab 安全群組
VPC：vpc-xxxxxxxxxxxxxxxxx AWS-DS-VPC01

適用於 AWS-DS-VPC01 的安全群組傳入規則

Type	通訊協定	連接埠範圍	來源	流量類型
自訂 TCP 規則	TCP	3389	我的 IP	遠端桌面
所有流量	全部	全部	10.0.0.0/16	所有本機 VPC 流量

適用於 AWS-DS-VPC01 的安全群組傳出規則

Type	通訊協定	連接埠範圍	目的地	流量類型
所有流量	全部	全部	0.0.0.0/0	所有流量

AWS-OnPrem-VPC01 安全群組資訊：
安全群組名稱： AWS OnPrem Test Lab 安全群組。
Description： AWS OnPrem Test Lab 安全群組。
VPC：vpc-xxxxxxxxxxxxxxxxx AWS-OnPrem-VPC01

安全群組輸入規則，適用於 AWS-OnPrem-VPC01

Type	通訊協定	連接埠範圍	來源	流量類型
自訂 TCP 規則	TCP	3389	我的 IP	遠端桌面
自訂 TCP 規則	TCP	53	10.0.0.0/16	DNS
自訂 TCP 規則	TCP	88	10.0.0.0/16	Kerberos
自訂 TCP 規則	TCP	389	10.0.0.0/16	LDAP
自訂 TCP 規則	TCP	464	10.0.0.0/16	Kerberos 更改/設定密碼
自訂 TCP 規則	TCP	445	10.0.0.0/16	SMB/CIFS
自訂 TCP 規則	TCP	135	10.0.0.0/16	複寫
自訂 TCP 規則	TCP	636	10.0.0.0/16	LDAP SSL
自訂 TCP 規則	TCP	49152 - 65535	10.0.0.0/16	RPC
自訂 TCP 規則	TCP	3268-3269	10.0.0.0/16	LDAP GC 和 LDAP GC SSL
自訂 UDP 規則	UDP	53	10.0.0.0/16	DNS
自訂 UDP 規則	UDP	88	10.0.0.0/16	Kerberos
自訂 UDP 規則	UDP	123	10.0.0.0/16	Windows 時間
自訂 UDP 規則	UDP	389	10.0.0.0/16	LDAP
自訂 UDP 規則	UDP	464	10.0.0.0/16	Kerberos 更改/設定密碼
所有流量	全部	全部	10.100.0.0/16	所有本機 VPC 流量

安全群組傳出規則，適用於 AWS-OnPrem-VPC01

Type	通訊協定	連接埠範圍	目的地	流量類型
所有流量	全部	全部	0.0.0.0/0	所有流量

如需如何建立規則並將規則新增至安全群組的詳細說明，請參閱 Working with security groups (使用安全群組)。

步驟 2：建立 AWS Managed Microsoft AD Active Directory

您可以使用三種不同的方法來建立目錄。您可以使用 程序 AWS Management Console （ 本教學課程建議 ），也可以使用 AWS CLI 或 AWS Tools for Windows PowerShell 程序來建立目錄。

方法 1：建立 AWS Managed Microsoft AD 目錄 (AWS Management Console)

1. 在 AWS Directory Service 主控台中，選擇目錄，然後選擇設定目錄。
2. 在選取目錄類型頁面上，選擇 AWS Managed Microsoft AD，然後選擇下一步。
3. 在 Enter directory information (輸入目錄資訊) 頁面上，提供下列資訊，然後選擇 Next (下一步)。
   - 針對版本，選取標準版或企業版。如需版本的詳細資訊，請參閱 AWS Directory Service for Microsoft Active Directory。
   - 在 Directory DNS name (目錄 DNS 名稱) 中，輸入 **`corp.example.com`**。
   - 針對 Directory NetBIOS name (目錄 NetBIOS 名稱)，輸入 **`corp`**。
   - 針對Directory description (目錄描述)，輸入 **`AWS DS Managed`**。
   - 針對 Admin password (管理員密碼)，輸入此帳戶要使用的密碼，然後在 Confirm password (確認密碼) 中再輸入一次密碼。在建立目錄的過程中會自動建立此 Admin (管理員) 帳戶。密碼不得包含 admin 一字。目錄管理員密碼區分大小寫，長度須介於 8 至 64 個字元之間。至少須有一位字元屬於以下四種類型中的三類：
     - 小寫字母 (a-z)
     - 大寫字母 (A-Z)
     - 數字 (0-9)
     - 非英數字元 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
4. 在 Choose VPC and subnets (選擇 VPC 和子網路) 頁面上，提供下列資訊，然後選擇 Next (下一步)。
   - 對於 VPC，選擇開頭為 AWS-DS-VPC01 且結尾為 (10.0.0.0/16) 的選項。

- 在 Subnets (子網路)，選擇 10.0.0.0/24 和 10.0.1.0/24 公有子網路。

5. 在 Review & create (檢閱和建立) 頁面上檢閱目錄資訊，並進行必要的變更。若資訊無誤，請選擇 Create directory (建立目錄)。建立目錄需要 20 到 40 分鐘。建立後，Status (狀態) 值會變更為 Active (作用中)。

方法 2：建立 AWS Managed Microsoft AD (PowerShell)（選用）

1. 打開 PowerShell.
2. 鍵入下列命令。請務必使用上述 AWS Management Console 程序的步驟 4 中提供的值。

```
New-DSMicrosoftAD -Name corp.example.com -ShortName corp -Password P@ssw0rd
 -Description "AWS DS Managed" - VpcSettings_VpcId vpc-xxxxxxxx -
VpcSettings_SubnetId subnet-xxxxxxxx, subnet-xxxxxxxx
```

方法 3：建立 AWS Managed Microsoft AD (AWS CLI)（選用）

1. 開啟 AWS CLI。
2. 鍵入下列命令。請務必使用上述 AWS Management Console 程序的步驟 4 中提供的值。

```
aws ds create-microsoft-ad --name corp.example.com --short-name corp --
password P@ssw0rd --description "AWS DS Managed" --vpc-settings VpcId= vpc-
xxxxxxxx,SubnetIds= subnet-xxxxxxxx, subnet-xxxxxxxx
```

步驟 3：部署 Amazon EC2 執行個體以管理您的 AWS Managed Microsoft AD Active Directory

在此實驗室中，我們使用具有公有 IP 地址的 Amazon EC2 執行個體，以便從任何地方輕鬆存取管理執行個體。在生產設定中，您可以使用私有 VPC 中只能透過 VPN 或 AWS Direct Connect 連結存取的執行個體。具有公有 IP 地址的執行個體則沒有任何需求。

在本節中，您會使用新 EC2 執行個體上的 Windows Server，來演練讓用戶端電腦連線到您網域所需的各種部署後任務。在下一個步驟中，您會使用 Windows Server 來確認實驗室可運作。

選用：為您的目錄在 AWS-DS-VPC01 中建立 DHCP 選項集

在此選用程序中，您會設定 DHCP 選項範圍，讓 VPC 中的 EC2 執行個體自動使用 AWS Managed Microsoft AD 進行 DNS 解析。如需詳細資訊，請參閱 DHCP 選項集。

為目錄建立 DHCP 選項集

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 DHCP Options Sets (DHCP 選項集)，然後選擇 Create DHCP options set (建立 DHCP 選項集)。
3. 在 Create DHCP options set (建立 DHCP 選項集) 頁面上，提供您目錄的下列值：
   - 在 Name (名稱) 輸入 **`AWS DS DHCP`**。
   - 在 Domain name (網域名稱) 中輸入 **`corp.example.com`**。
   - 針對 Domain name servers (網域名稱伺服器)，輸入您 AWS 所提供目錄之 DNS 伺服器的 IP 地址。

     > **Note**
     >
     > 若要尋找這些地址，請前往 AWS Directory Service 目錄頁面，然後選擇適用的目錄 ID。在詳細資訊頁面上，識別並使用 DNS 地址中顯示的 IP。
     > 若要尋找這些地址，您也可以前往 AWS Directory Service 目錄 頁面，然後選擇相應的目錄 ID。然後，選擇擴展和共享。在域控制站下，識別並使用 IP 地址中顯示的 IP。

   - 將 NTP servers (NTP 伺服器)、NetBIOS name servers (NetBIOS 名稱伺服器) 和 NetBIOS node type (NetBIOS 節點類型) 中的設定留白。
4. 選擇建立 DHCP 選項集，然後選擇關閉。新的 DHCP 選項集會隨即出現在您的 DHCP 選項清單中。
5. 記下新 DHCP 選項集的 ID (dopt-***xxxxxxxx***)。在此程序最後要建立新選項集與 VPC 的關聯時會用到。

   > **Note**
   >
   > 無縫網域加入，無須設定 DHCP 選項集。

6. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
7. 在 VPC 清單中，選取 AWS DS VPC 並選擇動作，然後選擇編輯 DHCP 選項集。
8. 在 Edit DHCP options set(編輯 DHCP 選項集) 頁面上，選取您在步驟 5 中記錄的選項集，然後選擇 Save (儲存)。

建立角色以將 Windows 執行個體加入您的 AWS Managed Microsoft AD 網域

使用此程序來設定將 Amazon EC2 Windows 執行個體加入網域的角色。如需詳細資訊，請參閱將 Amazon EC2 Windows 執行個體加入您的 AWS Managed Microsoft AD Active Directory。

設定 EC2，將 Windows 執行個體加入您的網域

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在 IAM 主控台的導覽窗格中，選擇角色，然後選擇建立角色。
3. 在 Select type of trusted entity (選擇可信任執行個體類型) 下，選擇 AWS service (服務)。
4. 緊接在 Choose the service that will use this role (選擇將使用此角色的服務) 下，選擇 EC2，然後選擇 Next: Permissions (下一步：許可)。
5. 在 Attached permissions policy (連結許可政策) 頁面上，執行下列動作：

   - 選取 AmazonSSMManagedInstanceCore 受管政策旁的方塊。此政策提供使用 Systems Manager 服務所需的最低權限。
   - 選取 AmazonSSMDirectoryServiceAccess 受管政策旁的方塊。此政策提供將執行個體加入受 AWS Directory Service管理 Active Directory 的權限。

   如需您可以連接至 Systems Manager IAM 執行個體設定檔的這些受管政策和其他政策的資訊，請參閱《AWS Systems Manager 使用者指南》中的建立 Systems Manager 的 IAM 執行個體設定檔。如需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。
6. 選擇 Next: Tags (下一步：標籤)。
7. (選用) 新增一或多個標籤來組織鍵值對、追蹤或控制存取此角色，然後選擇 Next: Review (下一步：檢視)。
8. 針對角色名稱，輸入角色的名稱，描述這會用於將執行個體加入網域，例如 EC2DomainJoin。
9. (選用) 針對 Role description (角色描述)，輸入描述。
10. 選擇 Create role (建立角色)。系統會讓您回到 Roles (角色) 頁面。

建立 Amazon EC2 執行個體並自動加入目錄

在此程序中，您會在 EC2 執行個體中設定 Windows Server 系統，稍後可用於管理 Active Directory 中的使用者、群組和政策。

建立 EC2 執行個體並自動加入目錄

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 選擇 Launch Instance (啟動執行個體)。
3. 在 Step 1 (步驟 1) 頁面上，選擇 Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxxx*** 旁的 Select (選取)。
4. 在 Step 2 (步驟 2) 頁面上，選取 t3.micro (請注意，您可以選擇更大的執行個體類型)，然後選擇 Next: Configure Instance Details (下一步：設定執行個體詳細資訊)。
5. 在 Step 3 (步驟 3) 頁面上，執行下列動作：
   - 針對網路，選擇以 AWS-DS-VPC01 做為結尾的 VPC (例如 vpc-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01))。
   - 針對子網路，選擇應該已預先設定您慣用之可用區域的 Public subnet 1 (例如 subnet-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01-Subnet01 | ***us-west-2a***)。
   - 針對 Auto-assign Public IP (自動指派公有 IP)，如果該子網路設定未預設為啟用，請選擇 Enable (啟用)。
   - 針對 Domain join directory (網域加入目錄)，選擇 corp.example.com (d-***xxxxxxxxxx***)。
   - 針對 IAM role (IAM 角色)，選擇您在 建立角色以將 Windows 執行個體加入您的 AWS Managed Microsoft AD 網域 中命名的執行個體名稱，例如 EC2DomainJoin。
   - 將其他設定保留為其預設值。
   - 選擇 Next: Add Storage (下一步：新增儲存體)。
6. 在 Step 4 (步驟 4) 頁面上，保留預設設定，然後選擇 Next: Add Tags (下一步：新增標籤)。
7. 在 Step 5 (步驟 5) 頁面上，選擇 Add Tag (新增標籤)。在 Key (金鑰) 下，輸入 **`corp.example.com-mgmt`**，然後選擇 Next: Configure Security Group (下一步：設定安全群組)。
8. 在步驟 6 頁面上，選擇選取現有安全群組並選取 AWS DS RDP 安全群組 (即您之前在基礎教學中設定的值)，然後選擇檢閱和啟動以檢閱您的執行個體。
9. 在 Step 7 (步驟 7) 頁面上，檢閱頁面，然後選擇 Launch (啟動)。
10. 在 Select an existing key pair or create a new key pair (選取現有金鑰對或建立新金鑰對) 對話方塊中，執行下列動作：
    - 選擇 Choose an existing key pair (選擇現有金鑰對)。
    - 在選取金鑰對下，選擇 AWS-DS-KP。

- 選取 I acknowledge... (我確認...) 核取方塊。
- 選擇 Launch Instances (啟動執行個體)。

11. 選擇 檢視執行個體返回 Amazon EC2 主控台並檢視部署的狀態。

在您的 EC2 執行個體上安裝 Active Directory 工具

您可以從兩種方法中進行選擇，在您的 EC2 執行個體上安裝 Active Directory 網域管理工具。您可以使用 Server Manager UI （ 本教學課程建議使用 ） 或 PowerShell。

在您的 EC2 執行個體上安裝 Active Directory 工具 (伺服器管理員)

1. 在 Amazon EC2 主控台中，選擇執行個體並選取您剛建立的執行個體，然後選擇連線。
2. 在連線至執行個體對話方塊中，選擇取得密碼以在您尚未取得密碼時擷取密碼，然後選擇下載遠端桌面檔案。
3. 在 Windows Security (Windows 安全性) 對話方塊中，輸入 Windows Server 電腦的本機管理員登入資料進行登入 (例如 **`administrator`**)。
4. 從開始選單，選擇伺服器管理員。
5. 在儀表板中，選擇新增角色及功能。
6. 在新增角色及功能精靈中，選擇下一步。
7. 在選取安裝類型頁面上，選擇角色型或功能型安裝，然後選擇下一步。
8. 在選取目的地伺服器頁面上，確定已選取本機伺服器，然後選擇下一步。
9. 在選取伺服器角色頁面上，選擇下一步。
10. 在選取功能頁面上，執行下列動作：

    - 選取群組原則管理核取方塊。
    - 展開遠端伺服器管理工具，然後展開角色管理工具。
    - 選取 AD DS 及 AD LDS 工具核取方塊。
    - 選取 DNS 伺服器工具核取方塊。
    - 選擇下一步。

11. 在確認安裝選項頁面上，檢閱資訊，然後選擇安裝。功能安裝完成後，開始選單的 Windows 系統管理工具資料夾中將會提供下列新的工具或嵌入式管理單元。

    - Active Directory 管理中心
    - Active Directory 網域及信任

- 的 Active Directory 模組 PowerShell
- Active Directory 站台及服務
- Active Directory 使用者和電腦
- ADSI 編輯器
- DNS
- 群組原則管理

在 EC2 執行個體上安裝 Active Directory 工具 (PowerShell)（選用）

1. 啟動 PowerShell。
2. 鍵入下列命令。

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-
Tools,RSAT-DNS-Server
```

步驟 4：確認基礎測試實驗室可運作

使用下列程序確認已成功設定測試實驗室，再新增其他測試實驗室指南模組。此程序會驗證您的 Windows Server 是否已正確設定、可以連線至 corp.example.com 網域，並用來管理您的 AWS Managed Microsoft AD 樹系。

確認測試實驗室可運作

1. 登出您以本機管理員身分登入的 EC2 執行個體。
2. 回到 Amazon EC2 主控台，在導覽窗格中選擇執行個體。然後選取您所建立的執行個體。選擇連線。
3. 在 Connect To Your Instance (連線到您的執行個體) 對話方塊中，選擇 Download Remote Desktop File (下載遠端桌面檔)。
4. 在 Windows Security (Windows 安全性) 對話方塊中，輸入 CORP 網域的管理員登入資料進行登入 (例如 **`corp\admin`**)。
5. 登入後，在開始選單的 Windows 系統管理工具下，選擇 Active Directory 使用者和電腦。
6. 您應該會看到 corp.example.com，以及與新網域相關聯的所有預設 OU 和帳戶。在網域控制站下，請注意您在本教學課程的步驟 2 中建立 AWS Managed Microsoft AD 時自動建立的網域控制站名稱。

恭喜您！您的 AWS Managed Microsoft AD 基礎測試實驗室環境現已設定完成。您可以開始新增系列中的下一個測試實驗室。

下一個教學：「教學課程：在 Amazon EC2 上建立從 AWS Managed Microsoft AD 到自我管理 Active Directory 安裝的信任」

教學課程：在 Amazon EC2 上建立從 AWS Managed Microsoft AD 到自我管理 Active Directory 安裝的信任

在本教學課程中，您將了解如何在基本教學課程中建立的 Microsoft Active Directory 樹系的 AWS Directory Service 之間建立信任。您也將了解如何在 Amazon EC2 的 Windows Server 上建立新的原生 Active Directory 樹系。如下圖所示，您從本教學課程建立的實驗室是設定完整的 AWS Managed Microsoft AD 測試實驗室時所需的第二個建置區塊。您可以使用測試實驗室來測試純雲端或混合雲端型 AWS 解決方案。

您應該只需要依此教學建立一次。之後，您可以視需要新增選用教學以取得更多體驗。

步驟 1：設定建立信任的環境

您需要準備好 Amazon EC2 環境，才能在新的 Active Directory 樹系與您於基礎教學中所建立的 AWS Managed Microsoft AD 樹系之間建立信任。若要執行此作業，請先建立 Windows Server 2019 伺服器、將該伺服器升級為網域控制站，然後相應地設定您的 VPC。

步驟 2：建立信任

在此步驟中，您會在 Amazon EC2 中託管的新建立 Active Directory 樹系與 Managed AWS Microsoft AD 樹系之間建立雙向樹系信任關係 AWS。

步驟 3：驗證信任

最後，身為管理員，您可以使用 AWS Directory Service 主控台來驗證新的信任是否可運作。

步驟 1：設定建立信任的環境

在本節中，您會設定 Amazon EC2 環境、部署新的樹系，以及準備 VPC 以建立信任 AWS。

建立 Windows Server 2019 EC2 執行個體

使用下列程序，在 Amazon EC2 中建立 Windows Server 2019 成員伺服器。

建立 Windows Server 2019 EC2 執行個體

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在 Amazon EC2 主控台中，選擇啟動執行個體。
3. 在 Step 1 (步驟 1) 頁面上，於清單中找到 Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxxx***。然後選擇選取。
4. 在 Step 2 (步驟 2) 頁面上，選取 t2.large，然後選擇 Next: Configure Instance Details (下一步：設定執行個體詳細資訊)。
5. 在 Step 3 (步驟 3) 頁面上，執行下列動作：
   - 針對網路，選取 vpc-***xxxxxxxxxxxxxxxxx*** AWS-OnPrem-VPC01 (您之前針對基礎教學中設定的值)。
   - 針對子網路，選取子網路-***xxxxxxxxxxxxxxxxxxxxx*** | AWS-OnPrem-VPC01-Subnet01 | AWS-OnPrem-VPC01。
   - 針對 Auto-assign Public IP (自動指派公有 IP) 清單，選擇 Enable (啟用) (如果此子網路設定未預設為 Enable (啟用))。
   - 將其他設定保留為其預設值。
   - 選擇 Next: Add Storage (下一步：新增儲存體)。
6. 在 Step 4 (步驟 4) 頁面上，保留預設設定，然後選擇 Next: Add Tags (下一步：新增標籤)。
7. 在 Step 5 (步驟 5) 頁面上，選擇 Add Tag (新增標籤)。在 Key (金鑰) 下，輸入 **`example.local-DC01`**，然後選擇 Next: Configure Security Group (下一步：設定安全群組)。
8. 在步驟 6 頁面上，選擇選取現有安全群組並選取 AWS DS RDP 安全群組 (即您之前在基礎教學中設定的值)，然後選擇檢閱和啟動以檢閱您的執行個體。
9. 在 Step 7 (步驟 7) 頁面上，檢閱頁面，然後選擇 Launch (啟動)。
10. 在 Select an existing key pair or create a new key pair (選取現有金鑰對或建立新金鑰對) 對話方塊中，執行下列動作：
    - 選擇 Choose an existing key pair (選擇現有金鑰對)。
    - 在選取金鑰對下，選擇 AWS-DS-KP (您之前在基礎教學中設定的值)。
    - 選取 I acknowledge... (我確認...) 核取方塊。
    - 選擇 Launch Instances (啟動執行個體)。
11. 選擇 檢視執行個體返回 Amazon EC2 主控台並檢視部署的狀態。

將您的伺服器升級為域控制站

您必須為新樹系建立第一個網域控制站並加以部署，才能建立信任。在此過程中，您會設定新的 Active Directory 樹系、安裝 DNS，並設定此伺服器使用本機 DNS 伺服器進行名稱解析。您必須在此程序結束時重新啟動伺服器。

> **Note**
>
> 如果您想要在 中建立網域控制站 AWS ，以使用內部部署網路複寫，則必須先手動將 EC2 執行個體加入內部部署網域。之後，您可以將伺服器升級為網域控制站。

將您的伺服器升級為網域控制站

1. 在 Amazon EC2 主控台中，選擇執行個體並選取您剛建立的執行個體，然後選擇連線。
2. 在 Connect To Your Instance (連線到您的執行個體) 對話方塊中，選擇 Download Remote Desktop File (下載遠端桌面檔)。
3. 在 Windows Security (Windows 安全性) 對話方塊中，輸入 Windows Server 電腦的本機管理員登入資料進行登入 (例如 **`administrator`**)。如果您還沒有本機管理員密碼，請回到 Amazon EC2 主控台，在執行個體上按一下滑鼠右鍵，然後選擇取得 Windows 密碼。導覽至您的 `AWS DS KP.pem` 檔案或您個人的 `.pem` 金鑰，然後選擇 Decrypt Password (解密密碼)。
4. 從開始選單，選擇伺服器管理員。
5. 在儀表板中，選擇新增角色及功能。
6. 在新增角色及功能精靈中，選擇下一步。
7. 在選取安裝類型頁面上，選擇角色型或功能型安裝，然後選擇下一步。
8. 在選取目的地伺服器頁面上，確定已選取本機伺服器，然後選擇下一步。
9. 在選取伺服器角色頁面上，選取 Active Directory Domain Services。在新增角色及功能精靈對話方塊中，確認已選取包含管理工具 (如適用) 核取方塊。選擇新增功能，然後選擇下一步。
10. 在選取功能頁面上，選擇下一步。
11. 在 Active Directory Domain Services 頁面上，選擇下一步。
12. 在確認安裝選項頁面上，選擇安裝。
13. 安裝 Active Directory 二進位檔案之後，選擇關閉。
14. 當伺服器管理員開啟時，尋找管理文字頂端附近的標記。當此標記變成黃色時，即表示伺服器已準備好升級。
15. 選擇黃色標記，然後選擇將此伺服器升級為網域控制站。

16. 在部署設定頁面上，選擇新增樹系。在根網域名稱中，輸入 **example.local**，然後選擇 下一步。
17. 在網域控制站選項頁面上，執行下列動作：
    - 在樹系功能等級和網域功能等級中，選擇 Windows Server 2016。
    - 在指定網域控制器功能下，確認已同時選取 DNS 伺服器和全域目錄 (GC)。
    - 輸入目錄服務還原模式 (DSRM) 密碼並確認。然後選擇下一步。
18. 在 DNS 選項頁面上，忽略委派的相關警告，然後選擇下一步。
19. 在 Additional options (其他選項) 頁面上，確定 EXAMPLE 已列為 NetBios 網域名稱。
20. 在路徑頁面上，保留預設值，然後選擇下一步。
21. 在檢閱選項頁面上，選擇下一步。伺服器現在會檢查以確認是否滿足網域控制站的所有必要條件。您可能會看到一些警告，但可以放心地忽略。
22. 選擇 Install (安裝)。一旦安裝完成，伺服器會重新啟動並成為可運作的網域控制站。

設定您的 VPC

下列三個程序將引導您完成設定 VPC 以連線到 AWS的步驟。

設定您的 VPC 輸出規則

1. 在 AWS Directory Service 主控台中，記下您先前在基本教學課程中建立的 AWS corp.example.com Managed Microsoft AD 目錄 ID。
2. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
3. 在導覽窗格中，選擇 Security Groups (安全群組)。
4. 搜尋您的 AWS Managed Microsoft AD 目錄 ID。在搜尋結果中，選取描述為 AWS created security group for d-***xxxxxx*** directory controllers 的項目。

   > **Note**
   >
   > 此安全群組會在您一開始建立目錄時自動建立。

5. 在該安全群組下，選擇 Outbound Rules (輸出規則) 標籤。依序選擇 Edit (編輯) 和 Add another rule (新增其他規則)，然後新增下列值：
    - 針對 Type (類型)，選擇 All Traffic (所有流量)。
    - 針對 Destination (目標)，輸入 **0.0.0.0/0**。

- 將其他設定保留為其預設值。
- 選取 Save (儲存)。

確認已啟用 Kerberos 預先驗證

1. 在 example.local 網域控制站上，開啟伺服器管理員。
2. 在 Tools (工具) 選單上，選擇 Active Directory Users and Computers (Active Directory 使用者和電腦)。
3. 導覽至使用者目錄，在任何使用者上按一下滑鼠右鍵並選取內容，然後選擇帳戶標籤。在帳戶選項清單中，向下捲動並確定 未選取不需要 Kerberos 預先驗證。
4. 對 corp.example.com-mgmt 執行個體中的 corp.example.com 網域執行相同步驟。

設定 DNS 條件式轉寄站

> **Note**
>
> 條件式轉寄站是網路上的 DNS 伺服器，可根據查詢中的 DNS 網域名稱來轉寄 DNS 查詢。例如，您可以設定 DNS 伺服器，將其收到的名稱以 widgets.example.com 結尾的所有查詢轉寄至特定 DNS 伺服器的 IP 地址，或轉寄至多個 DNS 伺服器的 IP 地址。

1. 開啟 AWS Directory Service 主控台。
2. 在導覽窗格中，選擇目錄。
3. 選取 AWS Managed Microsoft AD 的目錄 ID。
4. 記下您目錄的完整域名稱 (FQDN) corp.example.com 和 DNS 地址。
5. 現在，返回您的 example.local 網域控制站，然後開啟伺服器管理員。
6. 在工具選單上，選擇 DNS。
7. 在主控台樹狀目錄中，展開您要設定信任之網域的 DNS 伺服器，然後導覽至條件式轉寄站。
8. 在條件式轉寄站上按一下滑鼠右鍵，然後選擇新增條件式轉寄站。
9. 在 DNS 網域中，輸入 **`corp.example.com`**。
10. 在主要伺服器的 IP 地址下，選擇 <Click here to add ...>，輸入 AWS Managed Microsoft AD 目錄的第一個 DNS 地址（您在上一個程序中記下的），然後按 Enter。對第二個 DNS 地址執行相同步驟。輸入 DNS 地址之後，您可能會收到「逾時」或「無法解析」錯誤。您通常可以忽略這些錯誤。

11. 選取 Store this conditional forwarder in Active Directory, and replicate as follows (在 Active Directory 中儲存此條件式轉寄站，並複寫如下) 核取方塊。在下拉式選單中，選擇這個樹系中的所有 DNS 伺服器，然後選擇確定。

步驟 2：建立信任

在本節中，您會建立兩個不同的樹系信任。一個信任是從 EC2 執行個體上的 Active Directory 網域建立，另一個信任則從 中的 AWS Managed Microsoft AD 建立 AWS。

從 EC2 網域建立對 AWS Managed Microsoft AD 的信任

1. 登入 example.local。
2. 開啟伺服器管理員，然後在主控台樹狀目錄中選擇 DNS。記下所列出的伺服器 IPv4 位址。在下一個程序中，當您建立從 corp.example.com 到 example.local 目錄的條件式轉寄站時會需要用到。
3. 在工具選單中，選擇 Active Directory 網域及信任。
4. 在主控台樹狀目錄中，在 example.local 上按一下滑鼠右鍵，然後選擇內容。
5. 在信任標籤上，選擇新增信任，然後選擇下一步。
6. 在信任名稱頁面上，輸入 **`corp.example.com`**，然後選擇 下一步。
7. 在信任類型頁面上，選擇樹系信任，然後選擇下一步。

> **Note**
>
> AWS Managed Microsoft AD 也支援外部信任。但在此教學課程中，您將建立一個雙向樹系信任。

8. 在信任方向頁面上，選擇雙向，然後選擇下一步。

> **Note**
>
> 如果您稍後決定改用單向信任來嘗試此操作，請確定信任方向已正確設定 (信任網域上的傳出、信任網域上的傳入)。如需一般資訊，請參閱 Microsoft 網站上的 Understanding trust direction 一文。

9. 在信任方頁面上，選擇只建立於這個網域，然後選擇下一步。
10. 在連出信任驗證等級頁面上，選擇 Forest-wide authentication (驗證整個樹系)，然後選擇下一步。

> **Note**
>
> 雖然選項中有 Selective authentication (選擇性身分驗證)，但為了簡化本教學課程，我們建議您不要在此處啟用。設定時，只有受信任網域或樹系中已明確授與位於信任網域或樹系中的電腦物件 (資源電腦) 身分驗證許可的使用者，才能透過外部或樹系信任進行存取。如需詳細資訊，請參閱 Configuring selective authentication settings 一文。

11. 在信任密碼頁面上，輸入兩次信任密碼，然後選擇下一步。您將會在下一個程序中使用此相同的密碼。
12. 在信任選取完成頁面上，檢閱結果，然後選擇下一步。
13. 在信任建立完成頁面上，檢閱結果，然後選擇下一步。
14. 在確認連出信任頁面上，選擇否，不要確認連出信任。然後選擇 Next (下一步)
15. 在確認連入信任頁面上，選擇否，不要確認連入信任。然後選擇 Next (下一步)
16. 在完成新增信任精靈頁面上，選擇完成。

> **Note**
>
> 信任關係是 AWS Managed Microsoft AD 的全域功能。如果您使用 設定 AWS Managed Microsoft AD 的多區域複寫，則必須在 主要區域 中執行下列步驟。變更將自動套用至所有複寫區域。如需詳細資訊，請參閱全域與區域功能。

從 AWS Managed Microsoft AD 建立對 EC2 網域的信任

1. 開啟 AWS Directory Service 主控台。
2. 選擇 corp.example.com 目錄。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取主要區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
4. 在 Trust relationships (信任關係) 區段，選擇 Actions (動作)，然後選取 Add trust relationship (新增信任關係)。
5. 在 Add a trust relationship (新增信任關係) 對話方塊中，執行下列動作：

- 在 Trust type (信任類型) 下，選取 Forest trust (樹系信任)。

> **Note**
>
> 請確定您在此處選擇的信任類型符合先前程序中設定的相同信任類型 （ 從 EC2 網域建立信任至 AWS Managed Microsoft AD)。

- 針對 Existing or new remote domain name (現有或新的遠端網域名稱)，請輸入 example.local。
- 針對 Trust password (信任密碼)，輸入您在上一個程序中提供的相同密碼。
- 在 Trust direction (信任方向)中，選取 Two-way (雙向)。

> **Note**
>
> - 如果您稍後決定改用單向信任來嘗試此操作，請確定信任方向已正確設定 (信任網域上的傳出、信任網域上的傳入)。如需一般資訊，請參閱 Microsoft 網站上的 Understanding trust direction 一文。
> - 雖然選項中有 Selective authentication (選擇性身分驗證)，但為了簡化本教學課程，我們建議您不要在此處啟用。設定時，只有受信任網域或樹系中已明確授與位於信任網域或樹系中的電腦物件 (資源電腦) 身分驗證許可的使用者，才能透過外部或樹系信任進行存取。如需詳細資訊，請參閱 Configuring selective authentication settings 一文。

- 針對 Conditional forwarder (條件式轉寄站)，請輸入 example.local 樹系中 DNS 伺服器的 IP 地址 (您在上一個程序中記下的值)。

> **Note**
>
> 條件式轉寄站是網路上的 DNS 伺服器，可根據查詢中的 DNS 網域名稱來轉寄 DNS 查詢。例如，您可以設定 DNS 伺服器，將其收到的名稱以 widgets.example.com 結尾的所有查詢轉寄至特定 DNS 伺服器的 IP 地址，或轉寄至多個 DNS 伺服器的 IP 地址。

6. 選擇新增。

步驟 3：驗證信任

在本節中，您會測試是否已在 AWS 與 Amazon EC2 上的 Active Directory 之間成功設定信任。

驗證信任

1. 開啟 AWS Directory Service 主控台。
2. 選擇 corp.example.com 目錄。
3. 在目錄詳細資訊頁面上，執行下列其中一項：
   - 如果多區域複寫下顯示多個區域，請選取主要區域，然後選擇聯網和安全索引標籤。如需詳細資訊，請參閱主要區域與其他區域。
   - 如果多區域複寫下沒有顯示任何區域，請選擇聯網和安全索引標籤。
4. 在 Trust relationships (信任關係) 區段，選擇您剛才建立的信任關係。
5. 選擇 Actions (動作)，然後選擇 Verify trust relationship (驗證信任關係)。

一旦驗證完成，您應該會看到 Status (狀態) 欄下顯示 Verified (已驗證)。

恭喜您完成此教學！您現在擁有可運作的多樹系 Active Directory 環境，您可以從中開始測試各種案例。我們規劃在 2018 年推出更多測試實驗室教學，請不時回來查看是否有任何新教學。

AWS Managed Microsoft AD 配額

以下是 AWS Managed Microsoft AD 的預設配額。除非另有說明，否則每項配額都是依區域規定。

AWS Managed Microsoft AD 配額

資源	預設配額
AWS Managed Microsoft AD 目錄 (Standard 和 Enterprise Edition)	20
AWS Managed Microsoft AD 目錄 （混合版本）	5
手動快照 （標準版和企業版） *	每個 AWS Managed Microsoft AD 5 個
手動快照存留期 **	180 天
每個目錄的網域控制站上限數量	20
每個標準 Microsoft AD 的共享域 ***	25

資源	預設配額
每個企業 Microsoft AD 的共享域 ***	500
每個混合 Microsoft AD 的共用網域 ***	125
每個目錄的已登錄憑證授權單位 (CA) 憑證數目上限	5
單一 AWS Managed Microsoft AD (Enterprise Edition) 目錄中 AWS 的區域總數上限 ****	5

* 手動快照配額無法變更。

** 手動快照的支援存留期上限是 180 天，且無法變更。這是由於遭刪除物件的 Tombstone-Lifetime 屬性，該屬性定義了 Active Directory 系統狀態備份有用的存活時間。您無法從超過 180 天的快照進行還原。如需詳細資訊，請參閱 Microsoft 網站上的 Useful shelf life of a system-state backup of Active Directory。

*** 共用域預設配額是指單一目錄可被多少帳戶共用。

**** 這包括 1 個主要區域和最多 4 個其他區域。如需詳細資訊，請參閱主要區域與其他區域。

> **Note**
>
> 您無法將公有 IP 地址連接至 AWS 彈性網路界面 (ENI)。

如需應用程式設計和負載分配的詳細資訊，請參閱程式設計 AWS Managed Microsoft AD 應用程式時的最佳實務相關文章。

有關儲存和物件配額，請參閱 AWS Directory Service 定價頁面上的比較表。

Managed AWS Microsoft AD 故障診斷

以下可協助您疑難排解在建立或使用 AWS Managed Microsoft AD 時可能遇到的一些常見問題Active Directory。

AWS Managed Microsoft AD 的問題

有些故障診斷任務只能由 完成 支援。以下是一些任務：

- 重新啟動 AWS Directory Service您提供的網域控制站。
- 升級您的 AWS Managed Microsoft AD.

若要建立支援案例，請參閱建立支援案例和案例管理。

Netlogon 和安全頻道通訊的問題

為了緩解 CVE-2020-1472， Microsoft 已發佈修補，以修改網域控制站處理 Netlogon 安全頻道通訊的方式。由於引進這些安全的 Netlogon 變更，您的 AWS Managed Microsoft AD 可能不會接受某些 Netlogon 連線 （ 伺服器、工作站和信任驗證 ）。

若要確認問題是否與 Netlogon 或安全通道通訊相關，請在 Amazon CloudWatch Logs 中搜尋事件 ID 5827 (針對與裝置身分驗證相關的問題) 或 5828 (針對與 AD 信任驗證相關的問題)。如需 AWS Managed Microsoft AD 中的 CloudWatch 的資訊，請參閱 啟用 AWS Managed Microsoft AD 的 Amazon CloudWatch Logs 日誌轉送。

如需 CVE-2020-1472 緩解措施的詳細資訊，請參閱 網站上的如何管理 Netlogon 安全通道連線中與 CVE-2020-1472 相關聯的變更。 Microsoft

嘗試重設使用者密碼時，您會收到「回應狀態：400 錯誤請求」錯誤

嘗試重設使用者的密碼時，您會收到類似以下的錯誤訊息：

```
Response Status: 400 Bad Request
```

當您的 AWS Managed Microsoft AD Organizational Unit (OU) 中有相同使用者登入名稱的重複物件時，您可能會遇到此問題。使用者登入名稱必須是唯一的。如需詳細資訊，請參閱 Microsoft 文件中的對目錄資料問題進行故障診斷。

密碼復原

如果使用者忘記密碼或無法登入 AWS Managed Microsoft AD 目錄，您可以使用 AWS Management ConsolePowerShell或 重設密碼 AWS CLI。

如需詳細資訊，請參閱重設 AWS Managed Microsoft AD 使用者密碼。

其他資源

下列資源可協助您在使用 時進行故障診斷 AWS。

- AWS 知識中心 – 尋找FAQs和其他資源的連結，以協助您疑難排解問題。
- AWS 支援中心 - 取得技術支援。
- AWS 進階支援中心 - 取得進階技術支援。

下列資源可協助您疑難排解Active Directory常見問題。

- Active Directory 文件
- AD DS疑難排解

主題

- Amazon EC2 Linux 執行個體網域聯結錯誤
- AWS Managed Microsoft AD 低可用儲存空間
- 結構描述延伸錯誤
- 信任建立狀態原因

Amazon EC2 Linux 執行個體網域聯結錯誤

下列可協助您疑難排解將 Amazon EC2 Linux 執行個體加入 AWS Managed Microsoft AD 目錄時可能遇到的一些錯誤訊息。

Linux 執行個體無法加入網域或驗證

Ubuntu 14.04、16.04 和 18.04 執行個體必須在 DNS 中反向解析，領域才能搭配 Microsoft Active Directory 使用。否則，您可能會遇到以下兩種情況之一：

情況 1：尚未加入領域的 Ubuntu 執行個體

對於嘗試加入領域的 Ubuntu 執行個體，`sudo realm join` 命令可能無法提供加入網域的所需許可，並可能顯示以下錯誤：

! Couldn't authenticate to active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) adcli: couldn't connect to EXAMPLE.COM domain: Couldn't authenticate to

active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) ! Insufficient permissions to join the domain realm: Couldn't join realm: Insufficient permissions to join the domain

情況 2：已加入領域的 Ubuntu 執行個體

對於已加入 Microsoft Active Directory 網域的 Ubuntu 執行個體，嘗試使用網域憑證將 SSH 加入執行個體時，可能會失敗，並出現下列錯誤：

$ ssh admin@EXAMPLE.COM@198.51.100

no such identity: /Users/username/.ssh/id_ed25519: No such file or directory

admin@EXAMPLE.COM@198.51.100's password:

Permission denied, please try again.

admin@EXAMPLE.COM@198.51.100's password:

如果您使用公有金鑰登入執行個體並查看 `/var/log/auth.log`，可能會看到下列有關無法找到使用者的錯誤：

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0 user=admin@EXAMPLE.COM

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): received for user admin@EXAMPLE.COM: 10 (User not known to the underlying authentication module)

May 12 01:02:14 ip-192-0-2-0 sshd[2251]: Failed password for invalid user admin@EXAMPLE.COM from 203.0.113.0 port 13344 ssh2

May 12 01:02:15 ip-192-0-2-0 sshd[2251]: Connection closed by 203.0.113.0 [preauth]

不過，`kinit` 對於使用者仍然有效。請看如下範例：

ubuntu@ip-192-0-2-0:~$ kinit admin@EXAMPLE.COM Password for admin@EXAMPLE.COM: ubuntu@ip-192-0-2-0:~$ klist Ticket cache: FILE:/tmp/krb5cc_1000 Default principal: admin@EXAMPLE.COM

解決方法

目前對於這兩種情況的建議解決方法是停用 `/etc/krb5.conf` 中 [libdefaults] 區段的反向 DNS，如下所示：

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

無縫域加入的單向信任身分驗證問題

如果您在 AWS Managed Microsoft AD 和內部部署 Active Directory 之間建立了單向傳出信任，則嘗試使用 Winbind 的信任 Active Directory 登入資料對加入 Linux 執行個體的網域進行身分驗證時，可能會遇到身分驗證問題。

錯誤

Jul 31 00:00:00 EC2AMAZ-LSMWqT sshd[23832]: Failed password for user@corp.example.com from xxx.xxx.xxx.xxx port 18309 ssh2

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): getting password (0x00000390)

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): pam_get_item returned a password

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): request wbcLogonUser failed: WBC_ERR_AUTH_ERROR, PAM error: PAM_SYSTEM_ERR (4), NTSTATUS: **NT_STATUS_OBJECT_NAME_NOT_FOUND**, Error message was: The object name is not found.

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): internal module error (retval = PAM_SYSTEM_ERR(4), user = 'CORP\user')

解決方法

若要解決此問題，您需要執行下列步驟以註解或移除 PAM 模組組態檔 (`/etc/security/pam_winbind.conf`) 中的指令。

1. 在文字編輯器中開啟 `/etc/security/pam_winbind.conf` 檔案。

   ```
   sudo vim /etc/security/pam_winbind.conf
   ```

2. 註解或移除以下指令 krb5_auth = yes。

```
[global]

cached_login = yes
krb5_ccache_type = FILE
#krb5_auth = yes
```

3. 停止 Winbind 服務，然後重新啟動它。

```
service winbind stop or systemctl stop winbind
net cache flush
service winbind start or systemctl start winbind
```

AWS Managed Microsoft AD 低可用儲存空間

當您的 AWS Managed Microsoft AD 由於可用儲存空間Active Directory不足而受損時，需要立即採取動作，才能將目錄返回作用中狀態。以下章節涵蓋造成這種損害最常見的兩個原因：

1. SYSVOL 資料夾正在存放超過必要的群組政策物件
2. Active Directory 資料庫已填滿磁碟區

如需 AWS Managed Microsoft AD 儲存體的定價資訊，請參閱 AWS Directory Service 定價。

SYSVOL 資料夾正在存放超過必要的群組政策物件

這種損害的常見原因是在 SYSVOL 資料夾中存放了非必要的群組原則處理檔案。這些非必要的檔案可能是 EXE、MSI 或任何其他並非群組原則應處理的必要檔案。群組原則應處理的必要物件是群組政策物件、登入/登出指令碼，以及群組原則物件的中央存放區。任何非必要檔案都應存放在 Managed Microsoft AD 網域控制站 (AWS Managed Microsoft AD) 以外的檔案伺服器上。

如果需要群組原則軟體安裝的檔案，建議您使用檔案伺服器來存放這些安裝檔案。如果您不想自行管理檔案伺服器， AWS 會提供受管檔案伺服器選項 Amazon FSx。

若要移除任何不必要的檔案，您可以透過通用命名慣例 (UNC) 路徑存取 SYSVOL 共用。例如，如果您網域的完整網域名稱 (FQDN) 是 example.com，SYSVOL 的 UNC 路徑會是 "\\example.local\SYSVOL\example.local\"。一旦您找到並移除群組原則處理目錄時不需要的物件，其應該就會在 30 分鐘內回到作用中狀態。如果 30 分鐘後目錄未處於作用中狀態，請聯絡 AWS Support。

只將必要的群組原則檔案存放在您的 SYSVOL 共享中，可以確保您不會因為 SYSVOL 膨脹而損害您的目錄。

Active Directory 資料庫已填滿磁碟區

造成這種損害的常見原因是 Active Directory 資料庫填滿了磁碟區。如要驗證是否是這種情況，您可以檢閱您目錄中物件的 total (總) 計數。我們將 total (總) 這個字以粗體表示，是為了讓您了解 deleted (已刪除) 的物件仍然會計入目錄中的物件總數。

根據預設， AWS Managed Microsoft AD 會將 AD Recycling Bin 中的項目保留 180 天，之後才會成為 Recycled-Object。一旦物件成為 Recycled-Object (已標記)，便會另外再保留 180 天，最後才會從目錄清除。所以當物件遭到刪除時，物件仍會存在目錄資料庫中達 360 天，之後才會遭到清除。這就是為什麼必須評估物件的總數。

如需 AWS Managed Microsoft AD 支援物件計數的詳細資訊，請參閱 AWS Directory Service 定價。

如要取得目錄中包含已刪除物件的物件總數，您可以從加入網域的 Windows 執行個體執行以下 PowerShell 命令。如需如何設定管理執行個體的步驟，請參閱 AWS Managed Microsoft AD 中的使用者和群組管理。

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' |
 Select-Object -Property 'Count'
```

以下是以上命令的範例輸出：

```
Count
10000
```

如果總計數超過您上述備註中您目錄大小所支援的物件數，您便已超過您目錄的容量。

以下是解決這項損害的選項：

1. 清理 AD
   a. 刪除任何不需要的 AD 物件。
   b. 從 AD 資源回收筒移除任何不需要的物件。請注意，這是一項破壞性動作，且復原這些遭到刪除物件的唯一方法是執行目錄還原。
   c. 以下命令將會從 AD 資源回收筒移除任何遭到刪除的物件。

> **Important**
>
> 使用此命令時請特別小心，因為這是一項破壞性動作，且復原這些遭到刪除物件的唯一方法是執行目錄還原。

```
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
$NetBios = $DomainInfo.NetBIOSName
$ObjectsToRemove = Get-ADObject -Filter { isDeleted -eq $true } -
IncludeDeletedObjects -SearchBase "CN=Deleted Objects,$BaseDn" -Properties
 'LastKnownParent','DistinguishedName','msDS-LastKnownRDN' | Where-Object
 { ($_.LastKnownParent -Like "*OU=$NetBios,$BaseDn") -or ($_.LastKnownParent -Like
 '*\0ADEL:*') }
ForEach ($ObjectToRemove in $ObjectsToRemove) { Remove-ADObject -Identity
 $ObjectToRemove.DistinguishedName -IncludeDeletedObjects }
```

d. 向 AWS Support 開啟案例，請求 AWS Directory Service 回收可用空間。

2. 如果您的目錄類型是 Standard Edition 使用 AWS Support 開啟案例，請求將目錄升級至 Enterprise Edition。這也會增加您目錄的成本。如需定價資訊，請參閱 AWS Directory Service 定價。

在 AWS Managed Microsoft AD 中，AWS 委派的已刪除物件存留期管理員群組的成員能夠修改 屬性，該`msDS-DeletedObjectLifetime`屬性會設定已刪除物件在變成回收物件之前保留在 AD Recycling Bin 中的天數。

> **Note**
>
> 這是進階主題。如果設定不當，可能會導致資料遺失。我們強烈建議您先檢閱 The AD Recycle Bin: Understanding, Implementing, Best Practices, and Troubleshooting，以進一步了解這些程序。

將 `msDS-DeletedObjectLifetime` 屬性值變更為較低的數字，有助於確保您的物件數不會超過支援的層級。此屬性最低的有效值可以設為 2 天。一旦超過這個值，您將再也無法使用 AD 資源回收筒復原遭到刪除的物件。您將需要從快照還原目錄，才能復原這些物件。如需詳細資訊，請參閱使用快照還原 AWS Managed Microsoft AD。系統會從時間點進行還原，因此快照還原可能導致資料遺失。

如要變更您目錄的刪除物件生命週期，請執行以下命令：

> **Note**
>
> 如果您照原樣執行命令，該命令會將刪除物件生命週期屬性值設為 30 天。如果您想要讓它更長或更短，請以您偏好的數字取代 "30"。但是，我們建議您不要超過預設值 180。

```
$DeletedObjectLifetime = 30
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
Set-ADObject -Identity "CN=Directory Service,CN=Windows
 NT,CN=Services,CN=Configuration,$BaseDn" -Partition "CN=Configuration,$BaseDn" -
Replace:@{"msDS-DeletedObjectLifetime" = $DeletedObjectLifetime}
```

結構描述延伸錯誤

以下可協助您針對延伸 AWS Managed Microsoft AD 目錄的結構描述時可能遇到的一些錯誤訊息進行疑難排解。

參考項目

錯誤

Add error on entry starting on line 1: Referral The server side error is: 0x202b A referral was returned from the server. 延伸伺服器錯誤為：0000202B：RefErr：DSID-0310082F，資料 0、1 個存取點 \tref 1：'example.com' 修改的物件數量：0

故障診斷

請確定所有辨別名稱欄位包含正確的網域名稱。在上述範例中，`DC=example,dc=com` 應該取代成 Cmdlet `Get-ADDomain` 所示的 `DistinguishedName`。

無法讀取匯入檔案

錯誤

Unable to read the import file. Number of Objects Modified: 0

故障診斷

匯入的 LDIF 檔案是空的 (0 個位元組)。請確定所上傳的是正確檔案。

語法錯誤

錯誤

There is a syntax error in the input file Failed on line 21 The last token starts with 'q'. Number of Objects Modified: 0

故障診斷

第 21 行的文字格式不正確。無效文字的第一個字母是 A。請使用有效的 LDIF 語法更新第 21 行。如需如何格式化 LDIF 檔案的詳細資訊，請參閱「步驟 1：建立您的 LDIF 檔案」。

屬性或值已存在

錯誤

Add error on entry starting on line 1: Attribute Or Value Exists The server side error is: 0x2083 The specified value already exists. The extended server error is: 00002083: AtrErr: DSID-03151830, #1: \t0: 00002083: DSID-03151830, problem 1,006 (ATT_OR_VALUE_EXISTS), data 0, Att 20,019 (mayContain):len 4 Number of Objects Modified: 0

故障診斷

已套用結構描述變更。

沒有這類屬性

錯誤

Add error on entry starting on line 1: No Such Attribute The server side error is: 0x2085 The attribute value cannot be removed because it is not present on the object. The extended server error is: 00002085: AtrErr: DSID-03152367, #1: \t0: 00002085: DSID-03152367, problem 1,001 (NO_ATTRIBUTE_OR_VAL), data 0, Att 20,019 (mayContain):len 4 Number of Objects Modified: 0

故障診斷

LDIF 檔案嘗試從類別移除屬性，但該屬性目前未連接到這個類別。可能已套用結構描述變更。

錯誤

Add error on entry starting on line 41: No Such Attribute 0x57 The parameter is incorrect. The extended server error is: 0x208d Directory object not found. The extended server error is:

"00000057: LdapErr: DSID-0C090D8A, comment: Error in attribute conversion operation, data 0, v2580" Number of Objects Modified: 0

故障診斷

第 41 行所列的屬性不正確。請再次檢查拼法。

沒有這類物件

錯誤

Add error on entry starting on line 1: No Such Object The server side error is: 0x208d Directory object not found. 延伸伺服器錯誤為：0000208D：NameErr：DSID-03100238、問題 2001 (NO_OBJECT)、資料 0、最佳相符：'CN=結構描述、CN=組態、DC=example、DC=com' 修改的物件數量：0

故障診斷

辨別名稱 (DN) 所參考的物件不存在。

信任建立狀態原因

當 AWS Managed Microsoft AD 的信任建立失敗時，狀態訊息會包含其他資訊。以下可協助您了解這些訊息的意義。

存取遭拒

嘗試建立信任時存取遭拒。信任密碼不正確或遠端網域的安全設定不允許設定信任。如需信任的詳細資訊，請參閱 使用網站名稱和 DCLocator 提高信任效率。為解決此問題，請嘗試以下操作：

- 確認您使用的是您在遠端網域上建立對應信任時，所使用的相同信任密碼。
- 確認您的網域安全設定允許建立信任。
- 確認您的本機安全政策已正確設定。特別是檢查 `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` 並確保其中包含至少下列三個具名管道：
  - netlogon
  - samr
  - lsarpc

- 確認上述具名管道是否以 NullSessionPipes 登錄機碼上的值存在，該登錄機碼位於登錄路徑 HKLM\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters 中。這些值必須插入到單獨的列中。

> **Note**
>
> 根據預設，`Network access: Named Pipes that can be accessed anonymously` 並未設定且會顯示 `Not Defined`。這是正常的，因為網域控制站之 `Network access: Named Pipes that can be accessed anonymously` 的有效預設設定為 `netlogon、samr、lsarpc`。

- 在預設網域控制器政策中驗證下列伺服器訊息區塊 (SMB) 簽署設定。您可以在電腦組態 > Windows 設定 > 安全設定 > 本機政策/安全選項中找到這些設定。它們應該符合下列設定：
  - Microsoft 網路用戶端：數位簽署通訊（一律）：預設：已啟用
  - Microsoft 網路用戶端：數位簽署通訊（如果伺服器同意）：預設：已啟用
  - Microsoft 網路伺服器：數位簽署通訊（一律）：已啟用
  - Microsoft 網路伺服器：數位簽署通訊（如果用戶端同意）：預設：已啟用

使用網站名稱和 DCLocator 提高信任效率

Default-First-Site-Name 等第一個站台名稱不需要在網域之間建立信任關係。不過，在網域之間對齊網站名稱可以大幅改善網域控制站定位器 (DCLocator) 程序的效率。此對齊可改善預測和控制跨樹系信任的網域控制站選擇。

DCLocator 程序對於尋找不同網域和樹系的網域控制站至關重要。如需 DCLocator 程序的詳細資訊，請參閱 Microsoft 文件。高效率的網站組態可讓網域控制站位置更快且更準確，進而在跨樹系操作中提升效能和可靠性。

如需網站名稱和 DCLocator 程序如何互動的詳細資訊，請參閱下列Microsoft文章：

- 如何跨信任找到網域控制站
- 跨樹系的網域定位器

指定的網域名稱不存在或無法聯絡

若要解決此問題，請確定網域的安全群組設定和 VPC 的存取控制清單 (ACL) 正確無誤，而且您已正確輸入條件式轉寄站的資訊。 AWS 設定安全群組只開啟 Active Directory 通訊所需的連接埠。在預設設

定中，安全群組接受從任何 IP 地址到這些連接埠的流量。傳出流量僅限於安全群組。您將需要更新安全群組的傳出規則，以允許流量傳出到內部部署網路。如需安全需求的詳細資訊，請參閱「步驟 2：準備您的 AWS Managed Microsoft AD 」。

如果其他目錄網路的 DNS 伺服器使用公有 (非 RFC 1918) IP 地址，您將需要在目錄上新增從 Directory Services 主控台到 DNS 伺服器的 IP 路由。如需詳細資訊，請參閱建立、驗證或刪除信任關係及先決條件。

網際網路號碼分配局 (IANA) 為私有網際網路保留了以下三個 IP 地址空間區塊：

- 10.0.0.0 – 10.255.255.255 (10/8 字首)
- 172.16.0.0 – 172.31.255.255 (172.16/12 字首)
- 192.168.0.0 – 192.168.255.255 (192.168/16 字首)

如需詳細資訊，請參閱 https：//https://tools.ietf.org/html/rfc1918。

確認 AWS Managed Microsoft AD 的預設 AD 站點名稱與內部部署基礎設施中的預設 AD 站點名稱相符。電腦會使用其所屬的域 (而非使用者的域) 來決定網站名稱。重新命名網站以符合最近的內部部署部署可確保 DC 定位器使用最近網站的域控制站。如果這樣還是無法解決問題，可能因已快取之前建立的條件式轉寄站資訊，而阻礙新信任的建立。請稍候幾分鐘，然後重試建立信任和條件式轉寄站。

如需如何運作的詳細資訊，請參閱 Microsoft 網站上的跨樹系信任的網域定位器。

無法在此域上執行該操作

若要解決此問題，請確保兩個域的 / 目錄沒有重疊的 NETBIOS 名稱。如果域的 / 目錄確實具有重疊的 NETBIOS 名稱，請使用不同的 NETBIOS 名稱重新建立其中一個域，然後重試。

錯誤 "Required and valid domain name" 導致信任建立失敗

DNS 名稱只能包含字母字元 (A-Z)、數字字元 (0-9)、減號 (-) 和句點 (.)。僅當用於分隔域樣式名稱的組成部分時才允許使用句點字元。另外，請考量：

- AWS Managed Microsoft AD 不支援單一標籤網域的信任。如需詳細資訊，請參閱Microsoft支援單一標籤網域。
- 根據 RFC 1123 (https://tools.ietf.org/html/rfc1123)，DNS 標籤中只能使用 A 到 Z、a 到 z、0 到 9 以及連字號 (-)。DNS 名稱中也使用句點 (.)，但僅用於 DNS 標籤之間和 FQDN 末尾。

- 根據 RFC 952 (https://tools.ietf.org/html/rfc952)，名稱 (網路、主機、閘道或域) 是最多 24 個字元的文字字串，由字母 (A-Z)、數位 (0-9)、減號 (-) 和句點 (.) 組成。請注意，僅當用於分隔「域樣式名稱」的組成部分時才允許使用句點。

如需詳細資訊，請參閱Microsoft網站上的遵守主機和網域的名稱限制。

測試信任的一般工具

以下是可用於解決各種信任相關問題的工具。

AWS Systems Manager Automation 疑難排解工具

支援自動化工作流程 (SAW) 利用 AWS Systems Manager Automation 為您提供預先定義的 Runbook AWS Directory Service。AWSSupport-TroubleshootDirectoryTrust Runbook 工具可協助您診斷 AWS Managed Microsoft AD 與內部部署 Microsoft 之間的常見信任建立問題Active Directory。

DirectoryServicePortTest 工具

DirectoryServicePortTest 測試工具在針對 AWS Managed Microsoft AD 與內部部署 Active Directory 之間的信任建立問題進行疑難排解時很有幫助。如需使用工具的方法範例，請參閱「測試您的 AD Connector」。

NETDOM 和 NLTEST 工具

管理員可以使用 Netdom 和 Nltest 命令列工具來尋找、顯示、建立、移除和管理信任。這些工具直接與域控制站上的 LSA 機構通訊。如需如何使用這些工具的範例，請參閱Microsoft網站上的 Netdom 和 NLTEST。

封包擷取工具

您可以使用內建的 Windows 套件擷取公用程式，對潛在的網路問題進行調查和疑難排解。如需詳細資訊，請參閱 Capture a Network Trace without installing anything 一文。

AD Connector

AD Connector 是一種目錄閘道，您可以將目錄請求重新導向至內部部署，Microsoft Active Directory而無需快取雲端中的任何資訊。AD Connector 的大小分為兩種：小型和大型。小型 AD Connector 是專為小型組織所設計，專門用來處理每秒的小量作業。大型 AD Connector 是專為大型組織所設計，專門用來處理每秒的中等至大量作業。您可以將應用程式負載分散到多個 AD Connector 以擴展到您的效能需求。沒有強制執行的使用者或連線限制。

AD Connector 不支援 Active Directory 暫時性信任。AD Connector 和您的內部部署 Active Directory 網域具有 1：1 的關係。也就是說，對於每個內部部署網域，包括您要驗證的 Active Directory 樹系中的子網域，您必須建立唯一的 AD Connector。

> **Note**
>
> AD Connector 無法與其他 AWS 帳戶共用。如果這是必要項目，請考慮使用 AWS Managed Microsoft AD 來 共用您的 AWS Managed Microsoft AD。AD Connector 也不知道多 VPC，這表示像 WorkSpaces 這樣的 AWS 應用程式需要佈建到與 AD Connector 相同的 VPC 中。

設定 AD Connector 後，能為您提供下列優點：

- 您的最終使用者和 IT 管理員可以使用其現有的公司登入資料來登入 AWS 應用程式，例如 WorkSpaces、WorkDocs 或 Amazon WorkMail。
- 您可以透過 IAM 角色型存取 來管理 AWS 資源，例如 Amazon EC2 執行個體或 Amazon S3 儲存貯體 AWS Management Console。 Amazon EC2
- 無論使用者或 IT 管理員正在存取內部部署基礎設施或 AWS 雲端中的資源，您都可以持續強制執行現有的安全政策（例如密碼過期、密碼歷史記錄和帳戶鎖定）。
- 您可以使用 AD Connector 與現有的 RADIUS 型 MFA 基礎設施整合，以在使用者存取 AWS 應用程式時提供額外的安全層，以啟用多重驗證。

繼續閱讀本節主題，了解如何連線到目錄，並充分利用 AD Connector 功能。

主題

- AD Connector 入門
- AD Connector 的最佳實務
- 維護您的 AD Connector 目錄

- 保護您的 AD Connector 目錄
- 監控您的 AD Connector 目錄
- 從 AD Connector 存取 AWS 應用程式和服務
- 將 Amazon EC2 執行個體加入 的方法 Active Directory
- AD Connector 配額
- AD Connector 疑難排解

AD Connector 入門

使用 AD Connector，您可以 AWS Directory Service 連線到現有的企業 Active Directory。連線到您的現有目錄時，您所有的目錄資料皆會保留在您的網域控制站。 AWS Directory Service 不會複寫您任何目錄資料。

主題

- AD Connector 事前準備
- 建立 AD Connector
- 使用 AD Connector 建立的內容

AD Connector 事前準備

若要使用 AD Connector 連線到現有目錄，您需要準備下列項目：

Amazon VPC

進行下列 VPC 設定：

- 至少兩個子網路。每個子網路皆必須位於不同的可用區域。
- VPC 必須透過虛擬私有網路 (VPN) 連線或 AWS Direct Connect連線到您的現有網路。
- VPC 必須具有預設硬體租用。

AWS Directory Service 使用兩個 VPC 結構。組成目錄的 EC2 執行個體會在您的 AWS 帳戶之外執行，並由 管理 AWS。其使用兩種網路轉接器，ETH0 和 ETH1。ETH0 是管理轉接器，而且位於您的帳戶外部。ETH1 則是建立於您的帳戶內部。

目錄的 ETH0 網路的管理 IP 範圍以程式設計方式選擇，以確保它不會與部署目錄的 VPC 發生衝突。此 IP 範圍可以是以下任一對 (因為目錄在兩個子網路中運作)：

- 10.0.1.0/24 & 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 & 192.168.2.0/24

我們透過檢查 ETH1 CIDR 的第一個八位元組來避免衝突。如果以 10 開頭，則我們選擇具有 192.168.1.0/24 和 192.168.2.0/24 子網路並且地址為 192.168.0.0/16 的 VPC。如果第一個八位元位元組不是 10，我們會選擇具有 10.0.1.0/24 和 10.0.2.0/24 子網路並且地址為 10.0.0.0/16 的 VPC。

選取演算法不包含 VPC 上的路由。因此，這種情況可能會導致 IP 路由衝突。

如需詳細資訊，請參閱 Amazon VPC 使用者指南 中的下列主題：

- 「什麼是 Amazon VPC？」
- 「您 VPC 中的子網路」
- 「將硬體虛擬私有閘道新增到您的 VPC」

如需 的詳細資訊 AWS Direct Connect，請參閱 AWS Direct Connect 使用者指南。

現有 Active Directory

您將需要使用 Active Directory網域連線到現有的網路。

> **Note**
>
> AD Connector 不支援單一標籤域。

此Active Directory網域的功能層級必須`Windows Server 2003`或更高。AD Connector 也支援連線到託管於 Amazon EC2 執行個體上的域。

> **Note**
>
> 當 AD Connector 與 Amazon EC2 加入域功能結合使用時，不支援唯讀域控制站 (RODC)。

服務帳戶

您必須具備在現有目錄中，已委派下列權限之服務帳戶的登入資料：

- 讀取使用者和群組 – 必要

- 將電腦加入域 – 只有在使用無縫域加入和 WorkSpaces 時必要
- 建立電腦物件 – 只有在使用無縫域加入和 WorkSpaces 時必要
- 服務帳戶密碼應符合 AWS 密碼要求。 AWS 密碼應：
  - 長度介於 8 到 128 個字元之間。
  - 至少包含以下四個類別中的三個字元：
    - 小寫字母 (a-z)
    - 大寫字母 (A-Z)
    - 數字 (0-9)
    - 非英數字元 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

如需詳細資訊，請參閱委派權限給您的服務帳戶。

> **Note**
>
> AD Connector 使用 Kerberos 對 AWS 應用程式進行身分驗證和授權。LDAP 僅用於使用者和群組物件查詢 (讀取操作)。對於 LDAP 交易，任何內容都不可變，並且憑證不會以明文形式傳遞。身分驗證由 AWS 內部服務處理，該服務使用 Kerberos 票證以使用者身分執行 LDAP 操作。

使用者權限

所有 Active Directory 使用者必須具有讀取自己屬性的許可。特別是下列屬性：

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName
- UserAccountControl
- MemberOf

在預設情況下，Active Directory 使用者具有讀取這些屬性的許可。不過，管理員可能隨時間變更這些許可，所以您在首次設定 AD Connector 前，可能需先確認您的使用者擁有這些讀取許可。

IP 地址

取得您現有目錄中兩個 DNS 伺服器或網域控制器的 IP 地址。

當 AD Connector 連線到您的目錄時，要從這些伺服器取得 `_ldap._tcp.<DnsDomainName>` 和 `_kerberos._tcp.<DnsDomainName>` SRV 記錄，所以這些伺服器必須含有這些 SRV 記錄。AD Connector 會嘗試找到同時提供 LDAP 和 Kerberos 服務的常見域控制站，因此這些 SRV 記錄必須至少包含一個常見域控制站。如需 SRV 記錄的詳細資訊，請前往 Microsoft TechNet 上的 SRV Resource Records。

子網路的連接埠

若要讓 AD Connector 將目錄請求重新導向至現有的Active Directory網域控制站，現有網路的防火牆必須開放下列連接埠給 Amazon VPC 中兩個子網路CIDRs。

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 身分驗證
- TCP/UDP 389 - LDAP

您至少需要這些連接埠，AD Connector 才可連線到您的目錄。您特定的組態可能需要開啟其他連接埠。

如果您想要使用 AD Connector 和 Amazon WorkSpaces，您的網域控制站的 DisableVLVSupportLDAP 屬性必須設定為 0。這是網域控制站的預設設定。如果啟用 DisableVLVSupportLDAP 屬性，AD Connector 將無法查詢 目錄中的使用者。這可防止 AD Connector 使用 Amazon WorkSpaces。

> **Note**
>
> 如果您現有Active Directory網域的 DNS 伺服器或網域控制站伺服器位於 VPC 內，則與這些伺服器相關聯的安全群組必須對 VPC 中兩個子網路CIDRs 開放上述連接埠。

如需其他連接埠需求，請參閱 Microsoft 文件上的 AD 和 AD DS 連接埠需求。

Kerberos 預先驗證

您的使用者帳戶必須啟用 Kerberos 預先驗證。如需詳細的說明了解如何啟用此設定，請參閱 確定已啟用 Kerberos 預先驗證。如需此設定的一般資訊，請前往 Microsoft TechNet 上的預先驗證。

加密類型

AD Connector 在透過 Kerberos 對您的 Active Directory 網域控制站進行身分驗證時，支援下列加密類型：

- AES-256-HMAC

- AES-128-HMAC
- RC4-HMAC

AWS IAM Identity Center 先決條件

如果您打算將 IAM Identity Center 與 AD Connector 搭配使用，您需要確保符合下列條件：

- AD Connector 是在 AWS 組織的管理帳戶中設定。
- 您的 IAM Identity Center 執行個體與 AD Connector 是在相同區域中設定。

如需詳細資訊，請參閱《 AWS IAM Identity Center 使用者指南》中的 IAM Identity Center 先決條件。

多重要素驗證先決條件

若要使用 AD Connector 目錄支援多重驗證，您需要準備下列項目：

- 您現有網路中具有兩個用戶端端點的遠端驗證撥號使用者服務 (RADIUS) 伺服器。RADIUS 用戶端端點的要求如下：
  - 若要建立端點，您需要 AWS Directory Service 伺服器的 IP 地址。這些 IP 地址可從您目錄詳細資訊的 Directory IP Address (目錄 IP 地址) 欄位取得。
  - 這兩個 RADIUS 端點必須使用同一個共享秘密代碼。
- 您現有的網路必須允許來自 AWS Directory Service 伺服器的預設 RADIUS 伺服器連接埠 (1812) 的傳入流量。
- RADIUS 伺服器與現有目錄之間的使用者名稱必須相同。

如需搭配 MFA 使用 AD Connector 的詳細資訊，請參閱 啟用 AD Connector 的多重要素身分驗證。

委派權限給您的服務帳戶

若要連線到現有目錄，您必須具備在現有目錄中，已委派特定權限之 AD Connector 服務帳戶的登入資料。雖然 Domain Admins (網域管理員) 群組的成員具有連線到目錄的足夠權限，但最佳實務應該使用只具有連線到目錄所需之最低權限的服務帳戶。下列程序示範如何建立名為 的新群組`Connectors`、委派 AWS Directory Service 連線至此群組所需的必要權限，然後將新的服務帳戶新增至此群組。

此程序必須在已加入您目錄且已安裝 Active Directory User and Computers (Active Directory 使用者和電腦) MMC 嵌入的電腦上執行。您也必須以網域管理員的身分登入。

委派權限給您的服務帳戶

1. 開啟 Active Directory User and Computers (Active Directory 使用者和電腦)，並在導覽樹狀目錄中選取您的根網域。
2. 在左側窗格的清單中，對 Users (使用者) 按一下滑鼠右鍵，選取 New (新增)，再選取 Group (群組)。
3. 在 New Object - Group (新增物件 - 群組) 對話方塊中，輸入下列內容並按一下 OK (確定)。

欄位	值/選項
Group name (群組名稱)	`Connectors`
Group scope (群組範圍)	全域
Group type (群組類型)	安全性

4. 在 Active Directory 使用者和電腦導覽樹狀目錄中，選取識別要建立電腦帳戶的組織單位 (OU)。在選單中，選取 Action (動作)，再選取 Delegate Control (委派控制)。您可以選取網域的父 OU 做為許可傳播到子 OUs。如果您的 AD Connector 連線至 AWS Managed Microsoft AD，您將無法存取在網域根層級委派控制權。在這種情況下，要委派控制，請選取將在其中建立電腦物件的目錄 OU 下的 OU。
5. 在 Delegation of Control Wizard (委派控制精靈) 頁面上，按一下 Next (下一步)，然後按一下 Add (新增)。
6. 在 Select Users, Computers, or Groups (選取使用者、電腦或群組) 對話方塊中，輸入 `Connectors`，並按一下 OK (確定)。如果找到多個物件，請選取在上述步驟中建立的 `Connectors` 群組。按一下 Next (下一步)。
7. 在 Tasks to Delegate (要委派的任務) 頁面上，選取 Create a custom task to delegate (建立要委派的自訂任務)，然後選擇 Next (下一步)。
8. 選取 Only the following objects in the folder (僅限資料夾中的下列物件)，再選取 Computer objects (電腦物件) 和 User objects (使用者物件)。
9. 選取 Create selected objects in this folder (在此資料夾中建立選取的物件) 和 Delete selected objects in this folder (在此資料夾中刪除選取的物件)。然後選擇下一步。
10. 選取 Read (讀取)，然後選擇 Next (下一步)。

> **Note**
>
> 如果您將使用無縫域加入或 WorkSpaces，您也必須啟用寫入權限，以讓 Active Directory 建立電腦物件。

11. 驗證 Completing the Delegation of Control Wizard (完成委派控制精靈) 頁面中的資訊，然後按一下 Finish (完成)。
12. 建立使用高強度密碼的使用者帳戶，並將此使用者新增至 `Connectors` 群組。此使用者將稱為 AD Connector 服務帳戶，由於現在是 `Connectors`群組的成員，因此現在有足夠的權限 AWS Directory Service 可連線至 目錄。

測試您的 AD Connector

若要讓 AD Connector 連線至您的現有目錄，現有網路的防火牆必須向 VPC 中兩個子網路的 CIDR 開放特定連接埠。若要測試是否符合這些條件，請執行下列步驟：

測試連線

1. 在 VPC 中啟動 Windows 執行個體，並透過 RDP 與其連線。該執行個體必須為您現有網域的成員。其餘步驟皆在此 VPC 執行個體上執行。
2. 下載並解壓縮 DirectoryServicePortTest 測試應用程式。其中已包含來源碼與 Visual Studio 專案檔案，您可視需要修改測試應用程式。

> **Note**
>
> Windows Server 2003 或較舊的作業系統不支援此指令碼。

3. 在 Windows 命令提示下，運用下列選項執行 DirectoryServicePortTest 測試應用程式：

> **Note**
>
> 只在網域和樹系功能層級設定為 Windows Server 2012 R2 和以下時，才能使用 DirectoryServicePortTest 測試應用程式。

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp
 "53,88,389" -udp "53,88,389"
```

<domain_name>

完全合格的網域名稱。這用於測試森林和網域功能層級。如果您排除網域名稱，就不會測試功能層級。

<server_IP_address>

現有網域中網域控制器的 IP 地址。將針對此 IP 地址測試連接埠。如果您排除 IP 地址，就不會測試連接埠。

此測試應用程式會判斷 VPC 連線至您網域的必要連接埠是否開放，以及驗證最低的森林和網域功能層級。

輸出會類似下列內容：

```
Testing forest functional level.
Forest Functional Level = Windows2008R2Forest : PASSED

Testing domain functional level.
Domain Functional Level = Windows2008R2Domain : PASSED

Testing required TCP ports to <server_IP_address>:
Checking TCP port 53: PASSED
Checking TCP port 88: PASSED
Checking TCP port 389: PASSED

Testing required UDP ports to <server_IP_address>:
Checking UDP port 53: PASSED
Checking UDP port 88: PASSED
Checking UDP port 389: PASSED
```

下列是 DirectoryServicePortTest 應用程式的來源碼。

```
using System;
using System.Collections.Generic;
using System.IO;
```

```
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;
using System.DirectoryServices.ActiveDirectory;
using System.Threading;
using System.DirectoryServices.AccountManagement;
using System.DirectoryServices;
using System.Security.Authentication;
using System.Security.AccessControl;
using System.Security.Principal;

namespace DirectoryServicePortTest
{
    class Program
    {
        private static List<int> _tcpPorts;
        private static List<int> _udpPorts;

        private static string _domain = "";
        private static IPAddress _ipAddr = null;

        static void Main(string[] args)
        {
            if (ParseArgs(args))
            {
                try
                {
                    if (_domain.Length > 0)
                    {
                        try
                        {
                            TestForestFunctionalLevel();

                            TestDomainFunctionalLevel();
                        }
                        catch (ActiveDirectoryObjectNotFoundException)
                        {
                            Console.WriteLine("The domain {0} could not be found.\n",
 _domain);
                        }
                    }
```

```
                    if (null != _ipAddr)
                    {
                        if (_tcpPorts.Count > 0)
                        {
                            TestTcpPorts(_tcpPorts);
                        }

                        if (_udpPorts.Count > 0)
                        {
                            TestUdpPorts(_udpPorts);
                        }
                    }
                }
                catch (AuthenticationException ex)
                {
                    Console.WriteLine(ex.Message);
                }
            }
            else
            {
                PrintUsage();
            }

            Console.Write("Press <enter> to continue.");
            Console.ReadLine();
        }

        static void PrintUsage()
        {
            string currentApp =
Path.GetFileName(System.Reflection.Assembly.GetExecutingAssembly().Location);
            Console.WriteLine("Usage: {0} \n-d <domain> \n-ip \"<server IP address>\"
\n[-tcp \"<tcp_port1>,<tcp_port2>,etc\"] \n[-udp \"<udp_port1>,<udp_port2>,etc\"]",
currentApp);
        }

        static bool ParseArgs(string[] args)
        {
            bool fReturn = false;
            string ipAddress = "";

            try
            {
                _tcpPorts = new List<int>();
```

```
            _udpPorts = new List<int>();

            for (int i = 0; i < args.Length; i++)
            {
                string arg = args[i];

                if ("-tcp" == arg | "/tcp" == arg)
                {
                    i++;
                    string portList = args[i];
                    _tcpPorts = ParsePortList(portList);
                }

                if ("-udp" == arg | "/udp" == arg)
                {
                    i++;
                    string portList = args[i];
                    _udpPorts = ParsePortList(portList);
                }

                if ("-d" == arg | "/d" == arg)
                {
                    i++;
                    _domain = args[i];
                }

                if ("-ip" == arg | "/ip" == arg)
                {
                    i++;
                    ipAddress = args[i];
                }
            }
        }
        catch (ArgumentOutOfRangeException)
        {
            return false;
        }

        if (_domain.Length > 0 || ipAddress.Length > 0)
        {
            fReturn = true;
        }

        if (ipAddress.Length > 0)
```

```
            {
                _ipAddr = IPAddress.Parse(ipAddress);
            }

            return fReturn;
        }

        static List<int> ParsePortList(string portList)
        {
            List<int> ports = new List<int>();

            char[] separators = {',', ';', ':'};

            string[] portStrings = portList.Split(separators);
            foreach (string portString in portStrings)
            {
                try
                {
                    ports.Add(Convert.ToInt32(portString));
                }
                catch (FormatException)
                {
                }
            }

            return ports;
        }

        static void TestForestFunctionalLevel()
        {
            Console.WriteLine("Testing forest functional level.");

            DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Forest, _domain, null, null);
            Forest forestContext = Forest.GetForest(dirContext);

            Console.Write("Forest Functional Level = {0} : ",
forestContext.ForestMode);

            if (forestContext.ForestMode >= ForestMode.Windows2003Forest)
            {
                Console.WriteLine("PASSED");
            }
            else
```

```
            {
                Console.WriteLine("FAILED");
            }

            Console.WriteLine();
        }

        static void TestDomainFunctionalLevel()
        {
            Console.WriteLine("Testing domain functional level.");

            DirectoryContext dirContext = new
 DirectoryContext(DirectoryContextType.Domain, _domain, null, null);
            Domain domainObject = Domain.GetDomain(dirContext);

            Console.Write("Domain Functional Level = {0} : ", domainObject.DomainMode);

            if (domainObject.DomainMode >= DomainMode.Windows2003Domain)
            {
                Console.WriteLine("PASSED");
            }
            else
            {
                Console.WriteLine("FAILED");
            }

            Console.WriteLine();
        }

        static List<int> TestTcpPorts(List<int> portList)
        {
            Console.WriteLine("Testing TCP ports to {0}:", _ipAddr.ToString());

            List<int> failedPorts = new List<int>();

            foreach (int port in portList)
            {
                Console.Write("Checking TCP port {0}: ", port);

                TcpClient tcpClient = new TcpClient();

                try
                {
                    tcpClient.Connect(_ipAddr, port);
```

```
                tcpClient.Close();
                Console.WriteLine("PASSED");
            }
            catch (SocketException)
            {
                failedPorts.Add(port);
                Console.WriteLine("FAILED");
            }
        }

        Console.WriteLine();

        return failedPorts;
    }

    static List<int> TestUdpPorts(List<int> portList)
    {
        Console.WriteLine("Testing UDP ports to {0}:", _ipAddr.ToString());

        List<int> failedPorts = new List<int>();

        foreach (int port in portList)
        {
            Console.Write("Checking UDP port {0}: ", port);

            UdpClient udpClient = new UdpClient();

            try
            {
                udpClient.Connect(_ipAddr, port);
                udpClient.Close();
                Console.WriteLine("PASSED");
            }
            catch (SocketException)
            {
                failedPorts.Add(port);
                Console.WriteLine("FAILED");
            }
        }

        Console.WriteLine();

        return failedPorts;
```

```
        }
    }
}
```

建立 AD Connector

若要使用 AD Connector 連線到您的現有目錄，請執行下列步驟。開始此程序之前，請確定您已完成 AD Connector 事前準備 中所示的必要條件。

> **Note**
>
> 您無法使用 Cloud Formation 範本建立 AD Connector。

使用 AD Connector 連線

1. 在 AWS Directory Service 主控台中，選擇目錄，然後選擇設定目錄。
2. 在選取目錄類型 頁面上，選擇 AD Connector，然後選擇下一步。
3. 在 Enter AD Connector information (輸入 AD Connector 資訊) 頁面上，提供下列資訊：

   Directory size (目錄大小)

   選擇 Small (小型) 或 Large (大型) 尺寸選項。如需尺寸的詳細資訊，請參閱 AD Connector。

   目錄描述

   選擇填寫其他目錄說明。
4. 在 Choose VPC and subnets (選擇 VPC 和子網路) 頁面上，提供下列資訊，然後選擇 Next (下一步)。

   VPC

   目錄的 VPC。

   子網路

   選擇網域控制站的子網路。這兩個子網路必須位於不同的可用區域。
5. 在 Connect to AD (連結到 AD) 頁面上，提供下列資訊：

   目錄 DNS 名稱

   現有目錄的完整名稱，例如 `corp.example.com`。

目錄 NetBIOS 名稱

您現有目錄的簡稱，例如 CORP。

DNS IP 地址

您現有目錄中至少一個 DNS 伺服器的 IP 地址。這些伺服器皆必須可從步驟 4 指定的各子網路存取。只要指定的子網路和 DNS 伺服器 IP 地址之間有網路連線 AWS，這些伺服器就可以位於 外部。

服務帳戶使用名稱

現有目錄中使用者的使用者名稱。如需此帳戶的詳細資訊，請參閱「AD Connector 事前準備」。

服務帳戶密碼

現有使用者帳戶的密碼。密碼區分大小寫，長度須介於 8 至 128 個字元 (含) 之間。至少須有一位字元屬於以下四種類型中的三類：

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

Confirm password (確認密碼)

重新輸入現有使用者帳戶的密碼。

6. 在 Review & create (檢閱和建立) 頁面上檢閱目錄資訊，並進行必要的變更。若資訊無誤，請選擇 Create directory (建立目錄)。建立目錄需要幾分鐘的時間。建立後，Status (狀態) 值會變更為 Active (作用中)。

如需使用 AD Connector 建立之項目的詳細資訊，請參閱 使用 AD Connector 建立的內容。

使用 AD Connector 建立的內容

當您建立 AD Connector 時， AWS Directory Service 會自動建立彈性網路界面 (ENI) 並與您的每個 AD Connector 執行個體建立關聯。每個 ENIs對 VPC 和 AWS Directory Service AD Connector 之間的連線至關重要，不應刪除。您可以透過 AWS Directory Service 描述識別保留給 使用的所有網路介面：「為 directory-idAWS 建立網路介面」。如需詳細，請參閱《Amazon EC2 使用者指南》中的彈性網路界面。

> **Note**
>
> 依預設，AD Connector 執行個體會跨區域中的兩個可用區域部署，並連線至您的 Amazon Virtual Private Cloud (VPC)。出現故障的 AD Connector 執行個體將在同一可用區域中使用相同的 IP 地址自動替換。

當您登入與 AD Connector (AWS IAM Identity Center 包含） 整合的任何 AWS 應用程式或服務時，應用程式或服務會將您的身分驗證請求轉送至 AD Connector，然後將請求轉送至自我管理 Active Directory 中的網域控制站以進行身分驗證。如果您成功通過自我管理 Active Directory 的身分驗證，AD Connector 接著會將身分驗證字符傳回應用程式或服務 （類似 Kerberos 字符）。此時，您現在可以存取 AWS 應用程式或服務。

AD Connector 的最佳實務

以下是您應該考量的一些建議和準則，從而避免問題並充分運用 AD Connector。

設定：事前準備

建立目錄之前，請考量這些準則。

確認目錄類型是否正確

AWS Directory Service 提供多種方式可Microsoft Active Directory與其他 AWS 服務搭配使用。您可以依所需功能及成本預算，選擇目錄服務：

- AWS Directory Service for Microsoft Active Directory 是在 AWS 雲端Microsoft Active Directory上託管的豐富功能受管 Microsoft AD。如果您有超過 5，000 名使用者，而且需要在託管目錄和內部部署目錄之間 AWS 設定信任關係，則 AWS 受管 Microsoft AD 是您的最佳選擇。
- AD Connector 只會將您現有的現場部署連線到 Active Directory AWS。如果您想要將現有的內部部署目錄用於 AWS 服務，AD Connector 會是您的最佳選擇。
- Simple AD 是具有基本Active Directory相容性的低規模、低成本目錄。它支援最多 5,000 名使用者、Samba 4 相容應用程式，以及 LDAP 感知應用程式的 LDAP 相容性。

如需 AWS Directory Service 選項的更詳細比較，請參閱 該選擇哪種。

確認已正確設定您的 VPC 和執行個體

為了連線、管理及使用您的目錄，您必須正確設定與目錄相關聯的 VPC。如需 VPC 安全與聯網需求的資訊，請參閱「建立 AWS Managed Microsoft AD 的先決條件」、「AD Connector 事前準備」或「Simple AD 先決條件」。

如果您想要將執行個體新增至網域，請確定您具備連線能力並可遠端存取您的執行個體，如「將 Amazon EC2 執行個體加入 AWS Managed Microsoft AD 的方法」中所述。

留意您的限制

了解特定目錄類型的不同限制。您可以在目錄中儲存的物件數量僅受限於可用儲存空間和物件的彙總大小。有關所選目錄的詳細資訊，請參閱「AWS Managed Microsoft AD 配額」、「AD Connector 配額」或「Simple AD 配額」。

了解目錄 AWS 的安全群組組態和使用

AWS 會建立安全群組，並將其連接到您目錄的彈性網路介面，這些介面可從對等或調整大小VPCs 內存取。 AWS 會設定安全群組以封鎖對目錄不必要的流量，並允許必要的流量。

修改目錄安全群組

若要修改安全群組目錄的安全性，您可以這麼做。請只在您完全了解安全群組篩選的運作方式時才進行這類變更。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的適用於 Linux 執行個體的 Amazon EC2 安全群組一節。不當變更可能會導致與預期電腦和執行個體的通訊中斷。 AWS 建議您不要嘗試開啟目錄的其他連接埠，因為這會降低目錄的安全性。請仔細檢閱 AWS 共同的責任模型。

> **Warning**
>
> 在技術上，您可以將目錄的安全群組與您建立的其他 EC2 執行個體建立關聯。不過，針對此實務 AWS 建議 。 AWS 可能有理由在不通知的情況下修改安全群組，以解決受管目錄的功能或安全需求。這類變更會影響您要與目錄安全群組建立關聯的任何執行個體，而且可能會干擾具關聯執行個體的操作。此外，將目錄安全群組與您的 EC2 執行個體產生關聯可能會對 EC2 執行個體帶來安全風險。

使用 AD Connector 時正確設定內部部署站台和子網路

如果您的內部部署網路已定義 Active Directory 站台，您必須確定 AD Connector 所在之 VPC 中的子網路已於 Active Directory 站台中定義，而且 VPC 中的子網路與其他站台中的子網路之間沒有任何衝突。

為了探索域控制站，AD Connector 會使用與含有 AD Connector 之 VPC 的子網路 IP 地址範圍相近的 Active Directory 站台。如果您站台的子網路與 VPC 的子網路有相同 IP 地址範圍，AD Connector 會探索該站台中的域控制站，實際上有可能與您的區域不相近。

了解 AWS 應用程式的使用者名稱限制

AWS Directory Service 支援可用於建構使用者名稱的大多數字元格式。不過，在用於登入 AWS 應用程式的使用者名稱上會強制執行字元限制，例如 WorkSpaces、WorkDocs、Amazon WorkMail 或 QuickSight。這些限制要求不使用下列字元：

- 空格
- 多位元組字元
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> @ 符號只可位於 UPN 尾碼之前。

編寫程式設計自己的應用程式

編寫程式設計自己的應用程式之前，請考慮下列事項：

投入生產前先進行負載測試

請務必針對代表您生產工作負載的應用程式與請求執行實驗室測試，以確認目錄擴展至您的應用程式負載。如果您需要更多容量，將負載分散到多個 AD Connector 目錄。

使用您的目錄

以下是使用目錄時需謹記的一些建議。

定期輪換管理員憑證

請定期變更您的 AD Connector 服務帳戶管理員密碼，並確保密碼與您現有的 Active Directory 密碼政策保持一致。如需有關如何變更服務帳戶密碼的詳細資訊，請參閱在 中更新您的 AD Connector 服務帳戶登入資料 AWS Management Console。

針對每個域使用唯一的 AD Connector

AD Connector 與您的內部部署 AD 域具有一對一關係。也就是說，對於每個內部部署域 (包括您要驗證的 AD 樹系子域)，您皆必須建立唯一的 AD Connector。即使您建立的每個 AD Connector 都連線到同一個目錄，他們仍必須使用不同的服務帳戶。

檢查相容性

使用 AD Connector 時，您必須確保您的內部部署目錄與 保持相容 AWS Directory Service。如需您責任的詳細資訊，請參閱我們的「共同的責任模型」。

維護您的 AD Connector 目錄

您可以使用 AWS Management Console 來維護 AD Connector day-to-day管理任務。您可以維護目錄的方式包括：

- 檢視 AD Connector 的詳細資訊。
- 更新 AD Connector 指向的 DNS 地址。
- 在不再需要 AD Connector 時將其刪除。

檢視 AD Connector 目錄資訊

檢視詳細目錄資訊

1. 在AWS Directory Service 主控台導覽窗格中的 下Active Directory，選取目錄。
2. 選擇您目錄的目錄 ID 連結。目錄的相關資訊會顯示在目錄詳細資訊頁面。

如需 Status (狀態) 欄位的詳細資訊，請參閱「了解您的目錄狀態」。

更新 AD Connector 的 DNS 地址

使用下列步驟可更新您 AD Connector 指向的 DNS 地址。

> **Note**
>
> 如果您正在進行某項更新，必須等到此更新完成後，才能提交另一項更新。
> 如果您搭配 AD Connector 使用 WorkSpaces，請確定 WorkSpace 的 DNS 地址也已更新。如需詳細資訊，請參閱更新 WorkSpaces 的 DNS 伺服器。

更新 AD Connector 的 DNS 設定

1. 在 AWS Directory Service 主控台導覽窗格中的 Active Directory 下，選擇目錄。
2. 選擇您目錄的目錄 ID 連結。
3. 在目錄詳細資訊頁面上，選擇網路和安全索引標籤。
4. 向下捲動至現有 DNS 設定區段中，選擇更新。
5. 在 Update existing DNS addresses (更新現有的 DNS 地址) 對話方塊中，輸入更新的 DNS IP 地址，然後選擇 Update (更新)。

有關 AD Connector 疑難排解的詳細資訊，請參閱 AD Connector 疑難排解。

刪除 AD Connector

刪除 AD Connector 時，您的內部部署目錄會保持不變。所有加入目錄的執行個體也會保持不變，並保持在已加入您內部部署目錄的狀態。您仍然可以使用目錄登入資料來登入這些執行個體。

刪除 AD Connector

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。請確定您在 AD Connector 部署 AWS 區域 所在的 中。如需詳細資訊，請參閱選擇區域。
2. 請確定您要刪除的 AD Connector 未啟用 AWS 任何應用程式。啟用 AWS 的應用程式會阻止您刪除 AD Connector。

   a. 在 Directories (目錄) 頁面中，選擇目錄 ID。
   b. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。在AWS 應用程式和服務區段中，您會看到哪些 AWS 應用程式已啟用 AD Connector。

      - 停用 AWS Management Console 存取。如需詳細資訊，請參閱停用 AWS Management Console 存取。
      - 若要停用 Amazon WorkSpaces，您必須從 WorkSpaces 主控台的目錄中取消登錄該服務。如需詳細資訊，請參閱《Amazon WorkSpaces 管理指南》中的刪除目錄。
      - 若要停用 WorkDocs，您必須在 WorkDocs 主控台中刪除 WorkDocs 網站。如需詳細資訊，請參閱《Amazon WorkDocs 管理指南》中的刪除網站一節。
      - 若要停用 Amazon WorkMail，您必須在 Amazon WorkMail 主控台中移除 Amazon WorkMail 組織。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的移除組織一節。

- 若要停用 Amazon FSx for Windows File Server，您必須從域中移除 Amazon FSx 檔案系統。如需詳細資訊，請參閱《Amazon FSx for Windows File Server 使用者指南》中的Active Directory在 FSx for Windows File Server 中使用 。 FSx
- 若要停用 Amazon Relational Database Service，您必須從域中移除 Amazon RDS 執行個體。如需詳細資訊，請參閱《Amazon RDS 使用者指南》中的管理域中的資料庫執行個體一節。
- 若要停用 AWS Client VPN 服務，您必須從 Client VPN 端點移除目錄服務。如需詳細資訊，請參閱《 AWS Client VPN 管理員指南》中的使用 Client VPN。
- 若要停用 Amazon Connect，您必須刪除 Amazon Connect 執行個體。如需詳細資訊，請參閱《Amazon Connect 管理指南》中的刪除 Amazon Connect 執行個體。 Amazon Connect
- 若要停用 Amazon QuickSight，您必須取消訂閱 Amazon QuickSight。如需詳細資訊，請參閱《Amazon QuickSight 使用者指南》中的關閉 Amazon QuickSight 您的帳戶。

> **Note**
>
> 如果您使用 AWS IAM Identity Center 且先前已將其連線至您計劃刪除的 AWS Managed Microsoft AD 目錄，您必須先變更身分來源，才能將其刪除。如需詳細資訊，請參閱《IAM Identity Center 使用者指南》中的變更身分來源一節。

3. 在導覽窗格中，選擇目錄。
4. 只選取要刪除的 AD Connector，然後按一下刪除。刪除 AD Connector 需要幾分鐘的時間。刪除相應 AD Connector 之後，它會從您的目錄清單中移除。

保護您的 AD Connector 目錄

您可以使用多重要素驗證 (MFA)、透過 Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (LDAPS) 的用戶端輕量型目錄存取通訊協定，以及 等功能 AWS Private Certificate Authority 來保護 AD Connector。保護 AD Connector 的方式包括：

- 啟用 MFA 以增加 AD Connector 安全性。
- 透過 Secure Socket Layer (SSL)/Transport Layer Security (TLS) (LDAPS) 啟用用戶端輕量型目錄存取通訊協定，以便透過 LDAP 進行通訊加密並提高安全性。
- 使用智慧卡啟用以憑證為基礎的交互傳輸層安全 (mTLS) 身分驗證，允許使用者透過您的 Active Directory和 AD Connector 在 Amazon Web Services 中進行身分驗證。

- 更新您的 AD Connector 服務帳戶憑證。
- 設定 AWS Private CA Connector for AD，以便您可以發行和管理 AD Connector 的憑證。

保護 AD Connector 的任務

- 啟用 AD Connector 的多重要素身分驗證
- 使用 AD Connector 啟用用戶端 LDAPS
- 在 AD Connector 中啟用 mTLS 身分驗證，以搭配智慧卡使用
- 在 中更新您的 AD Connector 服務帳戶登入資料 AWS Management Console
- 設定適用於 AD 的 AWS Private CA Connector

啟用 AD Connector 的多重要素身分驗證

當您在內部部署或在 Amazon EC2 執行個體中Active Directory執行時，您可以啟用 AD Connector 的多重要素驗證。如需搭配 使用多重要素驗證的詳細資訊 AWS Directory Service，請參閱 AD Connector 事前準備。

> **Note**
>
> 多重要素驗證不可用於 Simple AD。不過，您可以為 AWS Managed Microsoft AD 目錄啟用 MFA。如需詳細資訊，請參閱啟用 AWS Managed Microsoft AD 的多重驗證。

為 AD Connector 啟用多重要素驗證

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 為您的 AD Connector 目錄選擇目錄 ID 連結。
3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Networking & security (聯網和安全) 索引標籤。
4. 在 Multi-factor authentication (多重因素認證) 區段中，選擇 Actions (動作)，然後選擇 Enable (啟用)。
5. 在 Enable multi-factor authentication (MFA) (啟用多重因素認證 (MFA)) 頁面上，提供下列值：

   Display label (顯示標籤)

   提供標籤名稱。

RADIUS server DNS name or IP addresses (RADIUS 伺服器 DNS 名稱或 IP 地址)

您的 RADIUS 伺服器端點的 IP 地址，或您的 RADIUS 伺服器負載平衡器的 IP 地址。您可以輸入多個 IP 地址，中間以英文逗號分隔 (例如 `192.0.0.0,192.0.0.12`)。

> **Note**
>
> RADIUS MFA 僅適用於驗證對 或 Amazon Enterprise 應用程式和服務的存取 AWS Management Console，例如 WorkSpaces、Amazon QuickSight 或 Amazon Chime。它不會將 MFA 提供給在 EC2 執行個體上執行的 Windows 工作負載，或用於登入 EC2 執行個體。 AWS Directory Service 不支援 RADIUS 挑戰/回應身分驗證。
> 使用者在輸入使用者名稱與密碼時，必須有自己的 MFA 碼。或者，您必須使用頻外執行 MFA 的解決方案，例如使用者簡訊驗證。在頻外 MFA 解決方案中，務必為您的解決方案適當地設定 RADIUS 逾時值。使用頻外 MFA 解決方案時，登入頁面會提示使用者輸入 MFA 代碼。在此情況下，最佳實務是讓使用者在密碼欄位和 MFA 欄位中輸入其密碼。

連接埠

RADIUS 伺服器用於通訊的連接埠。您的內部部署網路必須允許從 AWS Directory Service 伺服器透過預設 RADIUS 伺服器連接埠 (UDP：1812) 的傳入流量。

共用秘密代碼

您的 RADIUS 端點建立時所指定的共用秘密代碼。

確認共用秘密代碼

確認您的 RADIUS 端點的共用秘密代碼。

通訊協定

選擇您的 RADIUS 端點建立時所指定的通訊協定。

Server timeout (in seconds) (伺服器逾時 (以秒為單位))

等待 RADIUS 伺服器回應的時間 (以秒為單位)。此值必須介於 1 到 50。

Max RADIUS request retries (RADIUS 請求重試次數上限)

嘗試與 RADIUS 伺服器進行通訊的次數。此值必須介於 0 到 10。

當 RADIUS Status (RADIUS 狀態) 變更為 Enabled (啟用) 時，即可使用 Multi-Factor Authentication。

6. 選擇 啟用 。

使用 AD Connector 啟用用戶端 LDAPS

AD Connector 中的用戶端 LDAPS 支援會加密 MicrosoftActive Directory(AD) 和 AWS 應用程式之間的通訊。這類應用程式的範例包括 WorkSpaces AWS IAM Identity Center、QuickSight 和 Amazon Chime。此加密可協助您更完善地保護組織的身分資料，並滿足您的安全需求。

您也可以取消註冊和停用用戶端 LDAPS。

主題

- 先決條件
- 啟用用戶端 LDAPS
- 管理用戶端 LDAPS

先決條件

啟用用戶端 LDAPS 前，您必須符合以下要求。

事前準備：

- 在 Active Directory 中部署伺服器憑證
- CA 憑證要求
- 網路要求

在 Active Directory 中部署伺服器憑證

若要啟用用戶端 LDAPS，您需要為 Active Directory 中的每個網域控制站取得並安裝伺服器憑證。LDAP 服務將使用這些憑證接聽並自動接受來自 LDAP 用戶端的 SSL 連線。您可以使用內部 Active Directory Certificate Services (ADCS) 部署發行或從商業發行者購買的 SSL 憑證。如需 Active Directory 伺服器憑證要求的詳細資訊，請參閱 Microsoft 網站上透過 SSL 的 LDAP (LDAPS) 憑證。

CA 憑證要求

用戶端 LDAPS 操作須使用憑證授權機構 (CA) 的憑證 (代表您伺服器憑證的發行者)。憑證授權機構憑證會以 Active Directory 網域控制站出示的伺服器憑證進行比對，以加密 LDAP 通訊。請注意下列 CA 憑證要求：

- 若要登錄憑證，憑證的過期日期必須在 90 天以上。
- 憑證必須是隱私權增強式郵件 (PEM) 格式。如果從 Active Directory 內部匯出 CA 憑證，選擇 base64 編碼的 X.509 (.CER) 做為匯出檔案格式。
- 每個 AD Connector 目錄最多可以儲存五 (5) 個憑證授權機構憑證。
- 不支援使用 RSASSA-PSS 簽章演算法的憑證。

網路要求

AWS 應用程式 LDAP 流量只會在 TCP 連接埠 636 上執行，不會回復至 LDAP 連接埠 389。不過，支援複寫、信任等等的 Windows LDAP 通訊將繼續使用具備 Windows 原生安全性的 LDAP 連接埠 389。設定 AWS 安全群組和網路防火牆，以允許 AD Connector （傳出） 和自我管理 Active Directory （傳入） 中連接埠 636 上的 TCP 通訊。

啟用用戶端 LDAPS

若要啟用用戶端 LDAPS，您只需將憑證授權機構 (CA) 憑證匯入 AD Connector，然後在目錄上啟用 LDAPS。啟用時， AWS 應用程式與自我管理 Active Directory 之間的所有 LDAP 流量都會使用 Secure Sockets Layer (SSL) 頻道加密。

您可以使用兩種不同的方法，為您的目錄啟用用戶端 LDAPS。您可以使用 AWS Management Console 方法或 AWS CLI 方法。

在 中註冊憑證 AWS Directory Service

使用下列其中一種方法來註冊憑證 AWS Directory Service。

方法 1：在 AWS Directory Service (AWS Management Console) 中註冊您的憑證

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 選擇您目錄的目錄 ID 連結。
3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Networking & security (聯網和安全) 索引標籤。
4. 在 Client-side LDAPS (用戶端 LDAPS) 畫面中，選取 Actions (動作) 功能表，然後選取 Register certificate (登錄憑證)。

5. 在 Register a CA certificate (登錄憑證授權機構憑證) 對話方塊中，選取 Browse (瀏覽)，然後選取憑證並選擇 Open (開啟)。
6. 選擇 Register certificate (登錄憑證)。

方法 2：在 AWS Directory Service (AWS CLI) 中註冊您的憑證

- 執行下列命令。對於憑證資料，請指向您 CA 憑證檔案的位置。憑證 ID 會在回應中提供。

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

檢查註冊狀態

若要查看憑證登錄狀態或登錄的憑證清單，請使用以下任一方法。

方法 1：檢查 AWS Directory Service (AWS Management Console) 中的憑證註冊狀態

1. 前往目錄詳細資訊頁面上的用戶端 LDAPS 區段。
2. 檢閱 Registration status (登錄狀態) 欄下方顯示的目前憑證登錄狀態。當登錄狀態值變更為 Registered (已登錄)，表示您的憑證已成功登錄。

方法 2：檢查 AWS Directory Service (AWS CLI) 中的憑證註冊狀態

- 執行下列命令。如果狀態值傳回 `Registered`，表示您的憑證已成功登錄。

```
aws ds list-certificates --directory-id your_directory_id
```

啟用用戶端 LDAPS

使用下列其中一種方法在 中啟用用戶端 LDAPS AWS Directory Service。

> **Note**
>
> 您必須先成功登錄至少一個憑證，才能啟用用戶端 LDAPS。

方法 1：在 AWS Directory Service (AWS Management Console) 中啟用用戶端 LDAPS

1. 前往目錄詳細資訊頁面上的用戶端 LDAPS 區段。
2. 選擇 啟用 。如果無法使用此選項，請確認已成功登錄有效憑證，然後再試一次。
3. 在 Enable client-side LDAPS (啟用用戶端 LDAPS) 對話方塊中，選擇 Enable (啟用)。

方法 2：在 AWS Directory Service (AWS CLI) 中啟用用戶端 LDAPS

- 執行下列命令。

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

檢查 LDAPS 狀態

使用下列其中一種方法來檢查 中的 LDAPS 狀態 AWS Directory Service。

方法 1：在 AWS Directory Service (AWS Management Console) 中檢查 LDAPS 狀態

1. 前往目錄詳細資訊頁面上的用戶端 LDAPS 區段。
2. 如果狀態值顯示為 Enabled (已啟用)，表示 LDAPS 已成功設定。

方法 2：在 AWS Directory Service (AWS CLI) 中檢查 LDAPS 狀態

- 執行下列命令。如果狀態值傳回 `Enabled`，表示 LDAPS 已成功設定。

```
aws ds describe-ldaps-settings -directory-id your_directory_id
```

如需檢視用戶端 LDAPS 憑證、取消註冊或停用 LDAPS 憑證的詳細資訊，請參閱 管理用戶端 LDAPS。

管理用戶端 LDAPS

使用這些命令來管理您的 LDAPS 組態。

您可以使用兩種不同的方法來管理用戶端 LDAPS 設定。您可以使用 AWS Management Console 方法或 AWS CLI 方法。

檢視憑證詳細資訊

使用下列其中一種方法來查看憑證設為過期的時間。

方法 1：在 AWS Directory Service (AWS Management Console) 中檢視憑證詳細資訊

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 選擇您目錄的目錄 ID 連結。
3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Networking & security (聯網和安全) 索引標籤。
4. 在 Client-side LDAPS (用戶端 LDAPS) 區段中，在 CA certificates (憑證授權機構憑證) 下方，將顯示憑證相關資訊。

方法 2：在 AWS Directory Service (AWS CLI) 中檢視憑證詳細資訊

- 執行下列命令。對於憑證 ID，使用 `register-certificate` 或 `list-certificates` 傳回的識別符。

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

取消登錄憑證

使用下列其中一種方法來取消登錄憑證。

> **Note**
>
> 如果只登錄一個憑證，必須先停用 LDAPS，才能取消登錄憑證。

方法 1：在 AWS Directory Service (AWS Management Console) 中取消註冊憑證

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 選擇您目錄的目錄 ID 連結。
3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Networking & security (聯網和安全) 索引標籤。
4. 在 Client-side LDAPS (用戶端 LDAPS) 區段中，選擇 Actions (動作)，然後選擇 Deregister certificate (取消登錄憑證)。

5. 在 Deregister a CA certificate (取消登錄憑證授權機構憑證) 對話方塊中，選擇 Deregister (取消登錄)。

方法 2：在 AWS Directory Service (AWS CLI) 中取消註冊憑證

- 執行下列命令。對於憑證 ID，使用 `register-certificate` 或 `list-certificates` 傳回的識別符。

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

停用用戶端 LDAPS

使用以下其中一個方法來停用用戶端 LDAPS。

方法 1：在 AWS Directory Service (AWS Management Console) 中停用用戶端 LDAPS

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 選擇您目錄的目錄 ID 連結。
3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Networking & security (聯網和安全) 索引標籤。
4. 在 Client-side LDAPS (用戶端 LDAPS) 區段中，選擇 Disable (停用)。
5. 在 Disable client-side LDAPS (停用用戶端 LDAPS) 對話方塊中，選擇 Disable (停用)。

方法 2：在 AWS Directory Service (AWS CLI) 中停用用戶端 LDAPS

- 執行下列命令。

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

在 AD Connector 中啟用 mTLS 身分驗證，以搭配智慧卡使用

您可以將以憑證為基礎的交互式 Transport Layer Security (mTLS) 身分驗證與智慧卡結合使用，透過自我管理的 Active Directory (AD) 和 AD Connector 對使用者進行身分驗證，讓使用者存取 Amazon WorkSpaces。啟用後，使用者在 WorkSpaces 登入畫面上選取智慧卡並輸入 PIN 碼進行身分驗證，而不是使用使用者名稱和密碼。之後，Windows 或 Linux 虛擬桌面便可以使用智慧卡從原生桌面作業系統進行 AD 身分驗證。

> **Note**
>
> AD Connector 中的智慧卡身分驗證功能僅在以下 AWS 區域提供，並且僅適用於 WorkSpaces。目前不支援其他 AWS 應用程式。
>
> - 美國東部 (維吉尼亞北部)
> - 美國西部 (奧勒岡)
> - 亞太區域 (悉尼)
> - 亞太區域 (東京)
> - 歐洲 (愛爾蘭)
> - AWS GovCloud （美國西部）
> - AWS GovCloud （美國東部）

您也可以取消註冊和停用憑證。

主題

- 先決條件
- 啟用智慧卡身分驗證
- 管理智慧卡身分驗證設定

先決條件

若要使用智慧卡為 Amazon WorkSpaces 用戶端啟用憑證型交互 Transport Layer Security (mTLS) 身分驗證，您需要與自我管理的 整合的操作智慧卡基礎設施Active Directory。如需如何使用 Amazon WorkSpaces 和 設定智慧卡身分驗證的詳細資訊Active Directory，請參閱 Amazon WorkSpaces 管理指南。

為 WorkSpaces 啟用智慧卡身分驗證之前，請檢閱下列先決條件：

- CA 憑證要求
- 使用者憑證要求
- 憑證撤銷檢查流程
- 考量事項

CA 憑證要求

AD Connector 需要憑證授權機構 (CA) 憑證 (代表使用者憑證的發行者) 進行智慧卡身分驗證。AD Connector 將 CA 憑證與使用者透過其智慧卡提供的憑證進行比對。請注意下列 CA 憑證要求：

- 若要登錄 CA 憑證，憑證距離過期日期必須在 90 天以上。
- CA 憑證必須是隱私權增強式郵件 (PEM) 格式。如果從 Active Directory 內部匯出 CA 憑證，選擇 Base64 編碼的 X.509 (.CER) 做為匯出檔案格式。
- 必須上傳從發行 CA 連結到使用者憑證的所有根 CA 憑證和中間 CA 憑證，智慧卡身分驗證才能成功。
- 每個 AD Connector 目錄最多可以儲存 100 個 CA 憑證
- AD Connector 不支援 CA 憑證的 RSASSA–PSS 簽章演算法。
- 確認憑證傳播服務設定為自動並執行中。

使用者憑證要求

以下是使用者憑證的一些需求：

- 使用者的智慧卡憑證具有使用者 userPrincipalName (UPN) 的主體別名 (SAN)。
- 使用者的智慧卡憑證具有增強型金鑰用量作為智慧卡登入 (1.3.6.1.4.1.311.20.2.2) 用戶端身分驗證 (1.3.6.1.5.5.7.3.2)。
- 使用者智慧卡憑證的線上憑證狀態協定 (OCSP) 資訊應該是授權資訊存取中的存取方法=線上憑證狀態協定 (1.3.6.1.5.5.7.48.1)。

如需 AD Connector 和智慧卡身分驗證需求的詳細資訊，請參閱《Amazon WorkSpaces 管理指南》中的需求。如需疑難排解 Amazon WorkSpaces 問題的說明，例如登入 WorkSpaces、重設密碼或連線至 WorkSpaces，請參閱《Amazon WorkSpaces 使用者指南》中的疑難排解 WorkSpaces 用戶端問題。 Amazon WorkSpaces

憑證撤銷檢查流程

為了執行智慧卡身分驗證，AD Connector 必須使用線上憑證狀態協定 (OCSP) 檢查使用者憑證的撤銷狀態。若要執行憑證撤銷檢查，OCSP 回應程式 URL 必須可透過網際網路存取。如果使用 DNS 名稱，OCSP 回應程式 URL 必須使用在網際網路號碼分配局 (IANA) 根區域資料庫中的頂層域。

AD Connector 憑證撤銷檢查流程如下：

- AD Connector 必須檢查使用者憑證中的 Authority Information Access (AIA) 擴充欄位以取得 OCSP 回應程式 URL，然後 AD Connector 使用該 URL 檢查是否已撤銷。
- 如果 AD Connector 無法解析使用者憑證 AIA 擴充欄位中找到的 URL，或無法在使用者憑證中找到 OCSP 回應程式 URL，則 AD Connector 將使用在根 CA 憑證登錄期間提供的選用 OCSP URL。

  如果使用者憑證 AIA 擴充欄位中的 URL 可以解析但沒有回應，則使用者身分驗證失敗。
- 如果在根 CA 憑證登錄期間提供的 OCSP 回應程式 URL 無法解析、無回應或未提供 OCSP 回應程式 URL，則使用者身分驗證將會失敗。
- OCSP 伺服器必須符合 RFC 6960。此外，對於總數小於或等於 255 個位元組的請求，OCSP 伺服器必須使用 GET 方法支援請求。

> **Note**
>
> AD Connector 要求 OCSP 回應程式 URL 為 HTTP URL。

考量事項

在 AD Connector 中啟用智慧卡身分驗證之前，請考慮以下事項：

- AD Connector 使用以憑證為基礎的交互式 Transport Layer Security (交互式 TLS) 身分驗證，透過硬體或軟體智慧卡憑證對 Active Directory 的使用者進行身分驗證。目前僅支援通用門禁卡 (CAC) 和個人身分驗證 (PIV) 卡。其他類型的硬體或軟體智慧卡可能也可以使用，但尚未經過使用 WorkSpaces 串流協定的測試。
- 在驗證 WorkSpaces 使用者的身分時，智慧卡身分驗證可取代使用者名稱和密碼身分驗證。

  如果您在啟用智慧卡身分驗證的 AD Connector 目錄中設定了其他 AWS 應用程式，這些應用程式仍會顯示使用者名稱和密碼輸入畫面。
- 啟用智慧卡身分驗證會將使用者工作階段長度限制為 Kerberos 服務票證的最大生命週期。您可以使用群組政策設定此設定 (預設為 10 小時)。如需此設定的詳細資訊，請參閱 Microsoft 文件。
- AD Connector 服務帳戶支援的 Kerberos 加密類型應與每個域控制站支援的 Kerberos 加密類型相符。

啟用智慧卡身分驗證

若要在 AD Connector 上為 WorkSpaces 啟用智慧卡身分驗證，首先需要將憑證授權機構 (CA) 憑證匯入 AD Connector。您可以使用 AWS Directory Service 主控台、API 或 CLI 將 CA 憑證匯入 AD Connector。使用下列步驟匯入 CA 憑證然後啟用智慧卡身分驗證。

步驟

- 啟用 AD Connector 服務帳戶的 Kerberos 限制委派
- 在 AD Connector 中註冊 CA 憑證
- 為支援 AWS 的應用程式和服務啟用智慧卡身分驗證

啟用 AD Connector 服務帳戶的 Kerberos 限制委派

若要透過 AD Connector 使用智慧卡身分驗證，您必須為自我管理 AD 目錄中的 LDAP 服務的 AD Connector 服務帳戶啟用 Kerberos 限制委派 (KCD)。

Kerberos 限制委派是 Windows Server 功能。此功能可讓管理員透過限制應用程式服務可代表使用者採取行動的範圍，來指定和強制執行應用程式信任界限。如需更多詳細資訊，請參閱 Kerberos 限制委派。

> **Note**
>
> Kerberos 限制委派 (KCD) 要求 AD Connector 服務帳戶的使用者名稱部分與相應使用者的 sAMAccountName 相符。sAMAccountName 不可超過 20 個字元。sAMAccountName 是 Microsoft Active Directory 屬性，用作早期版本的 Windows 用戶端和伺服器的登入名稱。

1. 使用 `SetSpn` 指令為自我管理 AD 中的 AD Connector 服務帳戶設定服務主體名稱 (SPN)。這將為服務帳戶啟用委派組態。

   SPN 可以是任何服務或名稱組合，但不能與現有 SPN 重複。`-s` 會檢查重複項。

   ```
   setspn -s my/spn service_account
   ```

2. 在 AD 使用者和電腦中，開啟內容 (右鍵) 選單並選擇 AD Connector 服務帳戶，然後選擇屬性。
3. 選擇委派索引標籤。
4. 選擇僅信任此使用者對指定服務的委派和使用任何身分驗證協定選項。
5. 選擇新增，然後選擇使用者或電腦以找到域控制站。

6. 選擇確定顯示用於委派的可用服務清單。
7. 選擇 ldap 服務類型，然後選擇確定。
8. 再次選擇確定以儲存組態。
9. 針對 Active Directory 中的其他網域控制站重複此程序。您也可以使用 PowerShell 自動化此流程。

在 AD Connector 中註冊 CA 憑證

使用下列方法之一為 AD Connector 目錄登錄 CA 憑證。

方法 1：將您的 CA 憑證登錄於 AD Connector (AWS Management Console)

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 選擇您目錄的目錄 ID 連結。
3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Networking & security (聯網和安全) 索引標籤。
4. 在智慧卡身分驗證區段，選擇動作，然後選擇登錄憑證。
5. 在登錄憑證對話方塊中，選取選擇檔案，然後選擇憑證，再選擇開啟。您可以選擇透過提供線上憑證狀態協定 (OCSP) 回應程式 URL，來對此憑證執行撤銷檢查。如需有關 OCSP 的詳細資訊，請參閱 憑證撤銷檢查流程。
6. 選擇 Register certificate (登錄憑證)。當您看到憑證狀態變更為已註冊 時，表示登錄程序已成功完成。

方法 2：將您的 CA 憑證登錄於 AD Connector (AWS CLI)

- 執行下列命令。對於憑證資料，請指向您 CA 憑證檔案的位置。若要提供輔助 OCSP 回應程式地址，請使用選用的 `ClientCertAuthSettings` 物件。

```
aws ds register-certificate --directory-id your_directory_id --certificate-
data file://your_file_path --type ClientCertAuth --client-cert-auth-settings
 OCSPUrl=http://your_OCSP_address
```

如果成功，回應會提供憑證 ID。您也可以透過執行以下 CLI 命令來驗證 CA 憑證是否登錄成功：

```
aws ds list-certificates --directory-id your_directory_id
```

如果狀態值傳回 `Registered`，表示您的憑證已成功登錄。

為支援 AWS 的應用程式和服務啟用智慧卡身分驗證

使用下列方法之一為 AD Connector 目錄登錄 CA 憑證。

方法 1：在 AD Connector 中啟用智慧卡身分驗證 (AWS Management Console)

1. 導覽至目錄詳細資訊頁面上的智慧卡身分驗證區段，然後選擇啟用。如果無法使用此選項，請確認已成功登錄有效憑證，然後再試一次。
2. 在啟用智慧卡身分驗證對話方塊中，選取啟用。

方法 2：在 AD Connector 中啟用智慧卡身分驗證 (AWS CLI)

- 執行下列命令。

```
aws ds enable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

如果成功，AD Connector 將傳回帶有空白 HTTP 正文的 HTTP 200 回應。

如需檢視憑證、取消註冊或停用憑證的詳細資訊，請參閱 管理智慧卡身分驗證設定。

管理智慧卡身分驗證設定

您可以使用兩種不同的方法來管理智慧卡設定。您可以使用 AWS Management Console 方法或 AWS CLI 方法。

主題

- 檢視憑證詳細資訊
- 取消登錄憑證
- 停用智慧卡身分驗證

檢視憑證詳細資訊

使用下列其中一種方法來查看憑證設為過期的時間。

方法 1：在 AWS Directory Service (AWS Management Console) 中檢視憑證詳細資訊

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。

2. 為您的 AD Connector 目錄選擇目錄 ID 連結。
3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Networking & security (聯網和安全) 索引標籤。
4. 在智慧卡身分驗證區段中的 CA 憑證下，選擇憑證 ID 以顯示相應憑證的詳細資訊。

方法 2：在 AWS Directory Service (AWS CLI) 中檢視憑證詳細資訊

- 執行下列命令。對於憑證 ID，使用 `register-certificate` 或 `list-certificates` 傳回的識別符。

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

取消登錄憑證

使用下列其中一種方法來取消登錄憑證。

> **Note**
> 如果只登錄一個憑證，必須先停用智慧卡身分驗證，才能取消登錄憑證。

方法 1：在 AWS Directory Service (AWS Management Console) 中取消註冊憑證

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 為您的 AD Connector 目錄選擇目錄 ID 連結。
3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Networking & security (聯網和安全) 索引標籤。
4. 在智慧卡身分驗證區段的 CA 憑證下，選取要取消登錄的憑證，選擇動作，然後取消登錄憑證。

> **Important**
> 確保您要取消登錄的憑證未處於作用中狀態或目前未用作智慧卡身分驗證的 CA 憑證鏈的一部分。

5. 在 Deregister a CA certificate (取消登錄憑證授權機構憑證) 對話方塊中，選擇 Deregister (取消登錄)。

方法 2：在 AWS Directory Service (AWS CLI) 中取消註冊憑證

- 執行下列命令。對於憑證 ID，使用 `register-certificate` 或 `list-certificates` 傳回的識別符。

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

停用智慧卡身分驗證

使用下列任一方法停用智慧卡身分驗證。

方法 1：在 AWS Directory Service (AWS Management Console) 中停用智慧卡身分驗證

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 為您的 AD Connector 目錄選擇目錄 ID 連結。
3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Networking & security (聯網和安全) 索引標籤。
4. 在智慧卡身分驗證區段中，選擇停用。
5. 在停用智慧卡身分驗證對話方塊中，選擇停用。

方法 2：在 AWS Directory Service (AWS CLI) 中停用智慧卡身分驗證

- 執行下列命令。

```
aws ds disable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

在 中更新您的 AD Connector 服務帳戶登入資料 AWS Management Console

您在 中提供的 AD Connector 登入資料 AWS Directory Service 代表用來存取現有內部部署目錄的服務帳戶。您可以執行下列步驟，在 中修改服務帳戶登入 AWS Directory Service 資料。

> **Note**
>
> 如果 目錄 AWS IAM Identity Center 已啟用 ， AWS Directory Service 則必須將服務主體名稱 (SPN) 從目前的服務帳戶轉移到新的服務帳戶。如果目前的服務帳戶不具刪除 SPN 的許可，

或新的服務帳戶無權新增 SPN，系統會提示您輸入具有執行這兩個動作之目錄帳戶許可的登入資料。這些登入資料只會用來轉移 SPN，服務不會存放此資料。

在 中更新您的 AD Connector 服務帳戶登入資料 AWS Directory Service

1. 在 AWS Directory Service 主控台導覽窗格中的 Active Directory 下，選擇目錄。
2. 選擇您目錄的目錄 ID 連結。
3. 在目錄詳細資訊頁面上，向下捲動至服務帳戶憑證區段。
4. 在 Service account credentials (服務帳戶認證) 區段中，選擇 Update (更新)。
5. 在更新服務帳戶憑證對話方塊中，鍵入服務帳戶使用者名稱和密碼。重新鍵入密碼進行確認，然後選擇更新。

設定適用於 AD 的 AWS Private CA Connector

您可以使用 AWS Private Certificate Authority AD Connector 整合自我管理Active Directory與 ，為加入 AD 網域的使用者、群組和機器發行和管理憑證。 AWS Private CA Connector for AD 提供全受管 AWS Private CA 做為自我管理企業 CAs 的下拉式選單，而不需要您部署、修補或更新本機代理程式或代理伺服器。

您可以透過 主控台、 AWS Private CA Connector for AD 主控台或呼叫 `CreateTemplate` API 來設定此整合 AWS Directory Service 。若要使用 AWS Private CA Connector for Active Directory主控台，請參閱 AWS Private CA Connector for Active Directory。下列各節說明如何從 AWS Directory Service 主控台設定此整合。

先決條件

如需設定說明，請參閱《 Connector for AD 使用者指南》中的設定 AWS Private CA Connector for AD。

設定 AWS Private CA Connector for AD

1. 登入 AWS Management Console ，並在 開啟 AWS Directory Service 主控台https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。

3. 在應用程式管理索引標籤和AWS 應用程式與服務區段下，選擇 AWS Private CA Connector for AD。隨即顯示為 建立私有 CA 憑證Active Directory頁面。遵循主控台上的步驟，為Active Directory連接器建立私有 CA，以註冊私有 CA。如需詳細資訊，請參閱建立連接器。
4. 建立連接器後，下列步驟會逐步引導您檢視 AWS Private CA Connector for AD 的詳細資訊，包括連接器的狀態和相關聯的 Private CA 狀態。

檢視您的 AWS Private CA Connector for AD

1. 登入 AWS Management Console ，並在 開啟 AWS Directory Service 主控台https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在應用程式管理索引標籤和AWS 應用程式與服務區段下，您可以檢視私有 CA 連接器和相關聯的私有 CA。依預設，您會看到下列欄位：
   a. AWS Private CA 連接器 ID — AWS Private CA 連接器的唯一識別符。選取它會導致該 AWS Private CA 連接器的詳細資訊頁面。
   b. AWS Private CA subject — CA 辨別名稱的相關資訊。按一下它會進入相應 AWS Private CA 的詳細資訊頁面。
   c. 狀態 — 根據 AWS Private CA Connector 和 的狀態檢查 AWS Private CA。如果兩項檢查均透過，則會顯示作用中。如果其中一項檢查失敗，則會顯示 1/2 檢查失敗。如果兩項檢查均失敗，則會顯示失敗。如需失敗狀態的更多資訊，請將滑鼠懸停在超連結上以了解哪個檢查失敗。然後按照主控台中的說明進行修復。
   d. 建立日期 — AWS Private CA 連接器建立的日期。

如需詳細資訊，請參閱檢視連接器詳細資訊。

驗證 AD 使用者的憑證發行

完成下列步驟，以確認 AWS Private CA 正在向您的自我管理 發行憑證Active Directory：

- 重新啟動您的內部部署網域控制站。
- 使用 檢視您的憑證Microsoft Management Console。如需詳細資訊，請參閱 Microsoft 文件。

監控您的 AD Connector 目錄

您可以透過進一步了解不同的 AD Connector 狀態，以及其對 AD Connector 的意義，充分利用 AD Connector。您也可以使用 Amazon Simple Notification Service 接收 AD Connector 狀態的通知。

監控 AD Connector 的任務：

- 了解您的目錄狀態
- 使用 Amazon SNS 啟用 AD Connector 目錄狀態通知

了解您的目錄狀態

下列是各種目錄狀態。

Active (作用中)

此目錄運作正常。 AWS Directory Service 未在目錄中偵測到任何問題。

正在建立

目前正在建立目錄。建立目錄通常需要 20 到 45 分鐘，但所需時間可能因系統負載而不同。

Deleted (已刪除)

目錄已刪除。目錄的所有資源皆已釋出。一旦目錄進入此狀態，便無法復原。

正在刪除

目前正在刪除目錄。目錄會保持這個狀態，直到完全刪除為止。一旦目錄進入此狀態，將無法取消刪除操作，且目錄無法復原。

失敗

無法建立目錄。請刪除此目錄。如果此問題仍存在，請聯絡 AWS 支援 中心 。

Impaired (受損)

目錄正在降級狀態下執行。已偵測到一個或多個問題，且並非所有目錄操作都能以完整的操作容量運作；目前處於狀態有許多可能的原因。其中包括正常的運作維護活動 (例如修補或 EC2 執行個體輪換)、應用程式在您的其中一個網域控制站上的暫時作用區，或您對不慎中斷目錄通訊的網路所做的變更。如需詳細資訊，請參閱 Managed AWS Microsoft AD 故障診斷、AD Connector 疑難排解、Simple AD 疑難排解。對於正常維護相關問題， 會在 40 分鐘內 AWS 解決這些問題。在檢閱疑難排解主題之後，如果您的目錄處於「受損」 狀態超過 40 分鐘，建議您聯絡 AWS 支援 中心。

> **Important**
>
> 目錄處於 Impaired (受損) 狀態時，請勿還原快照。還原快照很難解決受損問題。如需詳細資訊，請參閱使用快照還原 AWS Managed Microsoft AD。

Inoperable (無法操作)

目錄無法運作。所有目錄端點均已回報問題。

Requested (已請求)

目錄的建立請求目前待定中。

使用 Amazon SNS 啟用 AD Connector 目錄狀態通知

使用 Amazon Simple Notification Service (Amazon SNS)，當目錄狀態有所變更時，您便可以收到電子郵件或文字 (SMS) 簡訊。如果您的目錄從 Active (作用中) 狀態變成「受損」或「無法操作」狀態，您便會收到通知。當目錄恢復到 Active (作用中) 狀態時，您也會收到通知。

運作方式

Amazon SNS 使用「主題」收集和分發訊息。每個主題都有一或多個訂閱者，接收發佈到該主題的訊息。您可以使用下列步驟，將 AWS Directory Service 做為發佈者新增至 Amazon SNS 主題。當 AWS Directory Service 偵測到目錄狀態變更時，它會發佈訊息至該主題，然後傳送給主題的訂閱者。

您可以將多個目錄當成發布者，建立它們與單一主題的關聯性。您也可以於您之前在 Amazon SNS 中建立的主題中新增目錄狀態訊息。您對可以發佈和訂閱主題的人有精細的控制權。如需 Amazon SNS 的完整資訊，請參閱「什麼是 Amazon SNS？」。

為您的目錄啟用 SNS 簡訊

1. 登入 AWS Management Console 並開啟 AWS Directory Service 主控台。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 選取維護索引標籤。
4. 在目錄監控區段中，選擇動作，然後選取建立通知。
5. 在建立通知頁面上，選取選擇通知類型，然後選擇建立新通知。或者，如果您已有現有的 SNS 主題，您可以選擇與現有的 SNS 主題建立關聯性從這個目錄傳送狀態訊息到該主題。

> **Note**
>
> 如果您選擇建立新的通知，但接著卻為已存在的 SNS 主題使用了相同的主題名稱，則 Amazon SNS 不會建立新的主題，只會在現有的主題中新增新的訂閱資訊。
> 如果您選擇與現有的 SNS 主題建立關聯性，您只能選擇和目錄同一個區域的 SNS 主題。

6. 選擇收件人類型，然後輸入收件人聯絡資訊。如果您輸入適用於 SMS 的電話號碼，請只使用數字。不要包含破折號、空格或括號。
7. (選用) 提供主題的名稱和 SNS 顯示名稱。顯示名稱為不超過 10 個字元的簡稱，包含在這個主題的所有 SMS 訊息中。當您使用 SMS 選項時，需要有顯示名稱。

> **Note**
>
> 如果您登入時使用的是只有 DirectoryServiceFullAccess 受管政策的 IAM 使用者或角色，則您的主題名稱必須以 “DirectoryMonitoring” 開頭。如果您想進一步自訂您的主題名稱，您會需要額外的 SNS 權限。

8. 選擇 Create (建立)。

如果您想要指定其他 SNS 訂閱者，例如額外的電子郵件地址、Amazon SQS 佇列或 AWS Lambda，您可以從 Amazon SNS 主控台執行此操作。

從主題中移除目錄狀態訊息

1. 登入 AWS Management Console 並開啟 AWS Directory Service 主控台。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 選取維護索引標籤。
4. 在目錄監控區段中，選取清單中的相應 SNS 主題名稱，選擇動作，然後選取移除。
5. 選擇移除。

這會移除您在選取的 SNS 主題中做為發布者的目錄。如果您想要刪除整個主題，您可以從 Amazon SNS 主控台執行此操作。

> **Note**
>
> 使用 SNS 主控台刪除 Amazon SNS 主題之前，您應該確保目錄不會向該主題傳送狀態訊息。

如果您使用 SNS 主控台刪除 Amazon SNS 主題，此變更不會立即反映在 Directory Services 主控台中。您只會在下次目錄發佈通知到已刪除的主題時收到通知；在這種情況下，您會在目錄的 Monitoring (監控) 標籤中看到指出找不到主題的更新狀態。
因此，為了避免遺失重要的目錄狀態訊息，在刪除接收訊息的任何主題之前 AWS Directory Service，請將您的目錄與不同的 Amazon SNS 主題建立關聯。

從 AD Connector 存取 AWS 應用程式和服務

您可以允許 AD Connector 存取已連線 AWS 的應用程式和服務Active Directory。部分支援 AWS 的應用程式和服務包括：

- Amazon Chime
- Amazon WorkSpaces
- IAM Identity Center
- AWS Management Console

沒有第三方應用程式能搭配 AD Connector 使用。

從 AD Connector 存取 AWS 應用程式和服務的任務

- AD Connector 應用程式相容性政策
- 啟用從 AD Connector 存取 AWS 應用程式和服務

AD Connector 應用程式相容性政策

作為 AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) 的替代方案，AD Connector 是僅適用於 AWS 已建立應用程式和服務的 Active Directory 代理。您需要使用指定的 Active Directory 網域來設定 Proxy。該應用程式必須在 Active Directory 查詢使用者或群組時，AD Connector 會將請求代理發送至目錄。同樣地，使用者登入該應用程式時，AD Connector 會將身分驗證請求代理發送至目錄。沒有第三方應用程式能搭配 AD Connector 使用。

以下是相容的 AWS 應用程式和服務清單：

- Amazon Chime – 如需詳細說明，請參閱連線到您的 Active Directory 相關文章。
- Amazon Connect – 如需詳細資訊，請參閱 Amazon Connect 如何運作相關文章。

- 適用於 Windows 或 Linux 的 Amazon EC2 – 您可以使用 Amazon EC2 Windows 或 Linux 的無縫 Active Directory 網域聯結功能，將執行個體加入自我管理的 Active Directory （內部部署）。加入後，執行個體會直接與您的 Active Directory 通訊，並略過 AD Connector。如需詳細資訊，請參閱將 Amazon EC2 執行個體加入 的方法 Active Directory。
- AWS Management Console – 您可以使用 AD Connector 透過其 Active Directory 登入資料來驗證 AWS Management Console 使用者，而無需設定 SAML 基礎設施。如需詳細資訊，請參閱使用 AWS Managed Microsoft AD 登入資料啟用 AWS Management Console 存取。
- QuickSight - 如需詳細資訊，請參閱在 QuickSight 企業版中管理使用者帳戶。
- AWS IAM Identity Center - 如需詳細說明，請參閱將 IAM Identity Center 連線至內部部署 Active Directory。
- AWS Transfer Family - 如需詳細說明，請參閱使用 AWS Directory Service for Microsoft Active Directory。
- AWS Client VPN - 如需詳細說明，請參閱用戶端身分驗證和授權。
- WorkDocs - 如需詳細說明，請參閱使用 AD Connector 連線至您的內部部署目錄。
- Amazon WorkMail – 如需詳細說明，請參閱將 Amazon WorkMail 與現有目錄 (標準設定) 整合。
- WorkSpaces – 如需詳細說明，請參閱使用 AD Connector 啟用工作空間相關文章。

> **Note**
>
> Amazon RDS 僅與 AWS Managed Microsoft AD 相容，與 AD Connector 不相容。如需詳細資訊，請參閱AWS Directory Service FAQs頁面中的 AWS Managed Microsoft AD 一節。

啟用從 AD Connector 存取 AWS 應用程式和服務

使用者可以授權 AD Connector 提供 AWS 應用程式和服務，例如 Amazon WorkSpaces 存取您的 Active Directory。您可以啟用或停用下列 AWS 應用程式和服務，以使用 AD Connector。

AWS 應用程式/服務	詳細資訊...
Amazon Chime	如需詳細資訊，請參閱連線至 Active Directory。
Amazon Connect	如需詳細資訊，請參閱《Amazon Connect 管理指南》。

AWS 應用程式/服務	詳細資訊...
Amazon WorkDocs	如需詳細資訊，請參閱 Amazon WorkDocs 入門。
Amazon WorkMail	如需詳細資訊，請參閱建立組織。
Amazon WorkSpaces	您可以直接從 WorkSpaces 建立 Simple AD、AWS Managed Microsoft AD 或 AD Connector。只要在建立工作空間時啟動 Advanced Setup (進階設定) 即可。 如需詳細資訊，請參閱《Amazon WorkSpaces 管理指南》。
AWS Client VPN	如需詳細資訊，請參閱《AWS Client VPN 使用者指南》https://docs.aws.amazon.com/vpn/latest/clientvpn-user/。
AWS IAM Identity Center	如需詳細資訊，請參閱《AWS IAM Identity Center 使用者指南》https://docs.aws.amazon.com/singlesignon/latest/userguide/。
AWS Management Console	如需詳細資訊，請參閱使用 AWS Managed Microsoft AD 登入資料啟用 AWS Management Console 存取。
AWS Transfer Family	如需詳細資訊，請參閱《AWS Transfer Family 使用者指南》https://docs.aws.amazon.com/transfer/latest/userguide/what-is-aws-transfer-family.html。

一旦啟用，您就可以在要授權存取目錄之應用程式或服務的主控台中，管理您目錄的存取。若要在 AWS Directory Service 主控台中尋找上述 AWS 應用程式和服務連結，請執行下列步驟。

顯示目錄的應用程式與服務

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。

2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。
4. 檢視 AWS 應用程式和服務區段下的清單。

如需如何使用 授權或取消授權 AWS 應用程式和服務的詳細資訊 AWS Directory Service，請參閱使用 AWS 的應用程式和服務授權 AWS Directory Service。

將 Amazon EC2 執行個體加入 的方法 Active Directory

AD Connector 是一種目錄閘道，您可以將目錄請求重新導向至內部部署，MicrosoftActive Directory而無需快取雲端中的任何資訊。以下是如何將 Amazon EC2 加入 Active Directory網域的詳細資訊：

- 您可以在執行個體啟動時，將 Amazon EC2 執行個體無縫加入您的Active Directory網域。如需將 EC2 Windows 執行個體加入 AWS Managed Microsoft AD 的詳細資訊，請參閱 將 Amazon EC2 Windows 執行個體加入您的 AWS Managed Microsoft AD Active Directory。
- 如果您需要手動將 EC2 執行個體加入Active Directory網域，您必須在適當的 AWS 區域 安全群組或子網路中啟動執行個體，然後將執行個體加入Active Directory網域。
- 若要從遠端連線到這些執行個體，您必須具備從來源網路連線到執行個體的 IP 連線能力。在大多數情況下，這需要將網際網路閘道連接到您的 Amazon VPC，而且執行個體必須具備公有 IP 地址。如需使用網際網路閘道連線至網際網路的詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用網際網路閘道連線至網際網路一節。

> **Note**
>
> 將執行個體加入自我管理 Active Directory（內部部署）後，執行個體會直接與您的 通訊，Active Directory並略過 AD Connector。

AD Connector 配額

以下是 AD Connector 的預設配額。除非另有說明，否則每項配額都是依區域規定。

AD Connector 配額

資源	預設配額
AD Connector 目錄	10
每個目錄的已登錄憑證授權機構 (CA) 憑證數目上限	5

AD Connector 疑難排解

以下可協助您疑難排解在建立或使用 AD Connector 時可能遇到的一些常見問題。

主題

- 建立問題
- 連線問題
- 身分驗證問題
- 維護問題
- 我無法刪除我的 AD Connector
- 調查 AD Connector 發行者的一般工具

建立問題

以下是 AD Connector 的常見建立問題

- 當我建立目錄時，收到「AZ 限制」錯誤
- 當我嘗試建立 AD Connector 時，收到「偵測到連線問題」錯誤

當我建立目錄時，收到「AZ 限制」錯誤

在 2012 年之前建立的某些 AWS 帳戶可能可以存取美國東部（維吉尼亞北部）、美國西部（加利佛尼亞北部）或亞太區域（東京）不支援 AWS Directory Service 目錄的可用區域。如果您在建立 時收到這類錯誤Active Directory，請選擇不同可用區域中的子網路，然後再次嘗試建立目錄。

當我嘗試建立 AD Connector 時，收到「偵測到連線問題」錯誤

如果您在嘗試建立 AD Connector 時收到「偵測到連線問題」錯誤，則錯誤可能是因為連接埠可用性或 AD Connector 密碼複雜性。您可以測試 AD Connector 的連線，以查看下列連接埠是否可用：

- 53 (DNS)
- 88 (Kerberos)
- 389 (LDAP)

若要測試您的連線，請參閱 測試您的 AD Connector。連線測試應在與 AD Connector 的 IP 地址相關聯的兩個子網路聯結的執行個體上執行。

如果連線測試成功且執行個體加入網域，請檢查 AD Connector 的密碼。AD Connector 必須符合 AWS 密碼複雜性要求。如需詳細資訊，請參閱 中的服務帳戶AD Connector 事前準備。

如果您的 AD Connector 不符合這些要求，請使用符合這些要求的密碼重新建立 AD Connector。

我收到「連線目錄時遇到內部服務錯誤。請重試操作。」 建立 AD Connector 時發生錯誤

當 AD Connector 無法建立且無法連線至自我管理網域的有效Active Directory網域控制器時，通常會發生此錯誤。

> **Note**
>
> 最佳實務是，如果您的自我管理網路已定義Active Directory網站，您必須確保下列事項：
>
> - AD Connector 所在的 VPC 子網路定義於 Active Directory 網站。
> - 您的 VPC 子網路與其他網站中的子網路之間不存在衝突。

AD Connector 使用其子網路 IP 地址範圍接近包含 AD Connector 之 VPC 的Active Directory站台來探索 AD 網域控制站。如果您有一個站點，其子網路的 IP 地址範圍與 VPC 中的 IP 地址範圍相同，AD Connector 將探索該站點中的網域控制站。網域控制站可能不是實際靠近 AD Connector 所在的區域。

- DNS SRV 記錄中的不一致（這些記錄使用以下在客戶受管Active Directory網域中建立的語法：`_ldap._tcp.<DnsDomainName>`和 `_kerberos._tcp.<DnsDomainName>`)。當 AD Connector 找不到並根據這些 SRV 記錄連線到有效的網域控制器時，可能會發生這種情況。
- AD Connector 與客戶受管 AD 之間的聯網問題，例如防火牆裝置。

您可以在網域控制站、DNS 伺服器和目錄網路介面的 VPC 流程日誌上使用網路封包擷取來調查此問題。如需進一步協助AWS 支援，請聯絡 。

連線問題

以下是 AD Connector 的常見連線問題

- 當我嘗試連線到內部部署目錄時，收到「偵測到連線問題」錯誤
- 當我嘗試連線到內部部署目錄時，收到「DNS 無法使用」錯誤
- 當我嘗試連線到內部部署目錄時，收到「SRV 記錄」錯誤

當我嘗試連線到內部部署目錄時，收到「偵測到連線問題」錯誤

連線至內部部署目錄時，您會收到類似以下的錯誤訊息：偵測到連線問題：IP 無法使用 LDAP (TCP 連接埠 389)：*<IP ###* Kerberos/身分驗證無法使用 (TCP 連接埠 88)：*<IP ###* 請確保列出的連接埠可用，然後重試操作。

AD Connector 必須能夠經由透過下列連接埠的 TCP 和 UDP 與您的內部部署域控制站通訊。確認您的安全群組和內部部署防火牆允許透過這些連接埠的 TCP 和 UDP 通訊。如需詳細資訊，請參閱AD Connector 事前準備。

- 88 (Kerberos)
- 389 (LDAP)

視您的需求而定，您可能需要額外的 TCP/UDP 連接埠。如需其中一些連接埠，請參閱下列清單。如需使用之連接埠的詳細資訊Active Directory，請參閱 Microsoft 文件中的如何設定Active Directory網域和信任的防火牆。

- 135 (RPC 端點映射器)
- 646 (LDAP SSL)
- 3268 (LDAP GC)
- 3269 (LDAP GC SSL)

當我嘗試連線到內部部署目錄時，收到「DNS 無法使用」錯誤

當您連線到內部部署目錄時，您會收到類似如下的錯誤訊息：

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

AD Connector 必須能夠經由透過連接埠 53 的 TCP 和 UDP 與您的內部部署 DNS 伺服器通訊。確認您的安全群組和內部部署防火牆允許透過此連接埠的 TCP 和 UDP 通訊。如需詳細資訊，請參閱AD Connector 事前準備。

當我嘗試連線到內部部署目錄時，收到「SRV 記錄」錯誤

當您連線到內部部署目錄時，您會收到類似下列一或多個錯誤訊息：

```
SRV record for LDAP does not exist for IP: <DNS IP address> SRV record for Kerberos
 does not exist for IP: <DNS IP address>
```

連線到您的目錄時，AD Connector 需要取得 _ldap._tcp.*<DnsDomainName>* 和 _kerberos._tcp.*<DnsDomainName>* SRV 記錄。如果此服務無法從您在連線到目錄時所指定的 DNS 伺服器取得這些記錄，您會收到此錯誤。如需這些 SRV 記錄的詳細資訊，請參閱「SRV record requirements」。

身分驗證問題

以下是 AD Connector 的一些常見身分驗證問題：

- 當我嘗試 Amazon WorkSpaces 使用智慧卡登入 時，收到「憑證驗證失敗」錯誤
- 當 AD Connector 所使用的服務帳戶嘗試進行身分驗證時，我收到「憑證無效」錯誤
- 使用 AWS 應用程式搜尋使用者或群組時，我收到「無法驗證」錯誤
- 當我嘗試更新 AD Connector 服務帳戶時，收到有關目錄登入資料的錯誤
- 我有一些使用者無法使用我的目錄進行身分驗證

當我嘗試 Amazon WorkSpaces 使用智慧卡登入 時，收到「憑證驗證失敗」錯誤

當您嘗試使用智慧卡登入 WorkSpaces 時，會收到類似以下的錯誤訊息：錯誤：憑證驗證失敗。請重新啟動瀏覽器或應用程式，並確定您選取正確的憑證，然後再試一次。如果智慧卡的憑證未正確存放在使用憑證的用戶端上，就會發生錯誤。如需 AD Connector 和智慧卡需求的詳細資訊，請參閱先決條件。

使用下列程序對智慧卡在使用者憑證存放區中存放憑證的能力進行疑難排解：

1. 在無法存取憑證的裝置上，存取 Microsoft Management Console(MMC)。

> **Important**
>
> 在繼續之前，請建立智慧卡憑證的副本。

2. 導覽至 MMC 中的憑證存放區。從憑證存放區刪除使用者的智慧卡憑證。如需在 MMC 中檢視憑證存放區的詳細資訊，請參閱 Microsoft 文件中的如何：使用 MMC 嵌入式檢視憑證。
3. 移除智慧卡。
4. 重新插入智慧卡，以便在使用者的憑證存放區中重新填入智慧卡憑證。

> **Warning**
>
> 如果智慧卡沒有將憑證重新複製到使用者存放區，則無法用於 WorkSpaces 智慧卡身分驗證。

AD Connector 的服務帳戶應具有下列項目：

- `my/spn` 已新增至服務原則名稱
- 委派給 LDAP 服務

在智慧卡上重新填入憑證後，應檢查內部部署網域控制器，以確定它們是否被封鎖，而無法映射主體別名的 使用者主體名稱 (UPN)。如需此變更的詳細資訊，請參閱 Microsoft 文件中的如何停用 UPN 映射的主體別名。

使用下列程序來檢查網域控制器的登錄機碼：

- 在登錄編輯器中，導覽至下列 hive 金鑰

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc\UseSubjectAltName

  - 檢查 UseSubjectAltName 的值：

    i. 如果值設為 0，則會停用主體別名映射，而且您必須明確地將指定的憑證映射至僅 1 個使用者。如果憑證映射到多個使用者，且此值為 0，使用該憑證登入將會失敗。

    ii. 如果值未設定或設定為 1，您必須明確地將指定的憑證對應至僅 1 個使用者，或使用主體別名欄位進行登入。

A. 如果憑證上存在主體別名欄位，則會排定優先順序。

B. 如果憑證上不存在主體別名欄位，且憑證明確對應至多個使用者，則使用該憑證登入將會失敗。

> **Note**
>
> 如果在內部部署網域控制站上設定登錄機碼，AD Connector 將無法在 中找到使用者Active Directory，並導致上述錯誤訊息。

Certificate Authority (CA) 憑證應上傳至 AD Connector 智慧卡憑證。憑證應包含 OCSP 資訊。下列列出 CA 的其他需求：

- 憑證應該位於網域控制站的信任根授權機構、憑證授權機構伺服器和 WorkSpaces 中。
- 離線和根 CA 憑證不會包含 OSCP 資訊。這些憑證包含撤銷的相關資訊。
- 如果您使用第三方 CA 憑證進行智慧卡身分驗證，則需要將 CA 和中繼憑證發佈到 Active Directory NTAuth 存放區。它們必須安裝在所有網域控制站、憑證授權機構伺服器和 WorkSpaces 的信任根授權機構中。
  - 您可以使用下列命令，將憑證發佈至 Active Directory NTAuth 存放區：

```
certutil -dspublish -f Third_Party_CA.cer NTAuthCA
```

如需將憑證發佈至 NTAuth 存放區的詳細資訊，請參閱《使用通用存取卡存取 Amazon WorkSpaces 安裝指南》中的將發行 CA 憑證匯入企業 NTAuth 存放區。

您可以依照下列程序檢查 OCSP 是否驗證使用者憑證或 CA 鏈結憑證：

1. 將智慧卡憑證匯出至本機機器上的位置，例如 C： 磁碟機。
2. 開啟命令列提示，並導覽至儲存匯出智慧卡憑證的位置。
3. 輸入以下命令：

```
certutil -URL Certficate_name.cer
```

4. 應該會在 命令之後出現快顯視窗。選取右上角的 OCSP 選項，然後選取擷取。狀態應傳回為已驗證。

如需 certutil 命令的詳細資訊，請參閱 Microsoft 文件中的 certutil

當 AD Connector 所使用的服務帳戶嘗試進行身分驗證時，我收到「憑證無效」錯誤

如果您的網域控制器上的硬碟空間不足，就會發生此問題。請確定您的網域控制器硬碟未滿。

當我嘗試更新 AD Connector 服務帳戶時，收到「發生錯誤」或「未預期的錯誤」

在 Amazon WorkSpaces 主控台啟動精靈等 AWS 企業應用程式中搜尋使用者時，發生下列錯誤或徵狀：

- 發生錯誤。如果您持續遇到問題，請聯絡社群論壇上的 AWS 支援 團隊，並透過 AWS Premium Support 進行聯絡。
- 發生錯誤。您的目錄需要更新登入資料。請更新目錄登入資料。

如果您嘗試更新 AD Connector 中的 AD Connector 服務帳戶登入資料，您可能會收到下列錯誤訊息：

- 未預期的錯誤。發生非預期的錯誤。
- 發生錯誤。服務帳戶/密碼組合發生錯誤。請再試一次。

AD Connector 目錄的服務帳戶位於客戶受管 中Active Directory。帳戶用作身分，以代表 AWS 企業應用程式透過 AD Connector 在客戶受管Active Directory網域上執行查詢和操作。AD Connector 使用 Kerberos 和 LDAP 來執行這些操作。

下列清單說明這些錯誤訊息的意義：

- 時間同步和 Kerberos 可能有問題。AD Connector 會將 Kerberos 身分驗證請求傳送至 Active Directory。這些請求具有時間敏感性，如果請求延遲，則會失敗。確保任何客戶受管網域控制站之間沒有時間同步問題。若要解決此問題，請參閱建議 - 使用授權時間來源設定根 PDC，並避免文件中的廣泛時間偏移。 Microsoft如需時間服務和同步的詳細資訊，請參閱下列內容：
  - Time Windows Service 的運作方式
  - 電腦時鐘同步的最大公差
  - Windows 時間服務工具和設定
- AD Connector 與客戶受管網域控制站之間具有防火牆或 VPN 硬體組態等網路 MTU 限制的中繼網路裝置，可能會因為網路分段而導致此錯誤。

  - 若要驗證 MTU 限制，您可以在客戶受管網域控制器與透過 AD Connector 連線的其中一個目錄子網路中啟動的 Amazon EC2 執行個體之間執行 Ping 測試。影格大小不應大於預設大小的 1500 個位元組
  - ping 測試將協助您了解影格大小是否超過 1500 個位元組（也稱為巨型影格），而且能夠到達 AD Connector VPC 和子網路，而不需要分段。進一步與您的網路團隊驗證，並確保中繼網路裝置上允許巨型訊框。
- 如果已在 AD Connector 上啟用用戶端 LDAPS，且憑證已過期，您可能會遇到此問題。確保伺服器端憑證和 CA 憑證都有效、尚未過期，並符合 LDAPs的要求。
- 如果在客戶受管Active Directory網域中停用虛擬清單檢視支援，則 AWS 應用程式將無法搜尋使用者，因為 AD Connector 在 LDAP 查詢中使用 VLV 搜尋。虛擬清單檢視支援會在 DisableVLVSupport 設定為非零值時停用。確保Active Directory使用下列步驟在 中啟用虛擬清單檢視 (VLV) 支援：

  1. 使用具有結構描述管理員憑證的帳戶，以結構描述主要角色擁有者的身分登入網域控制器。
  2. 選取開始，然後選取執行，然後輸入 **`Adsiedit.msc`**。
  3. 在 ADSI 編輯工具中，連線至組態分割區，然後展開 Configuration【DomainController】 節點。
  4. 展開 CN=Configuration，DC=DomainName 容器。
  5. 展開 CN=Services 物件。
  6. 展開 CN=Windows NT 物件。
  7. 選取 CN=Directory Service 物件。選取屬性。
  8. 在屬性清單中，選取 msds-Other-Settings。選擇 Edit (編輯)。
  9. 在值清單中，選取任何 DisableVLVSupport=x 的執行個體，其中 x 不等於 0，然後選取移除。
  10. 移除後，輸入 **`DisableVLVSupport=0`**。選取新增。
  11. 選取 OK (確定)。您可以關閉 ADSI 編輯工具。下圖顯示 ADSI 編輯視窗中的多值字串編輯器對話方塊：

> **Note**
>
> 在超過 100，000 個使用者的大型Active Directory基礎設施中，您可能只能搜尋特定使用者。不過，如果您嘗試一次列出所有使用者（例如，在 WorkSpaces 啟動精靈中顯示所有使用者)，即使啟用 VLV 支援，也可能導致相同的錯誤。AD Connector 需要使用子樹狀目錄索引來排序屬性 "CN" 的結果。子樹狀目錄索引是索引類型，可讓網域控制站準備執行虛

擬清單檢視 (LDAP) 搜尋操作，以允許 AD Connector 完成排序搜尋。此索引可改善 VLV 搜尋，並防止使用名為 MaxTempTableSize 的暫存資料庫資料表。此資料表的大小可能有所不同，但根據預設，項目數量上限為 10000（預設查詢政策的 MaxTempTableSize 設定）。增加 MaxTempTableSize 比使用子樹狀目錄索引效率低。為了避免在大型 AD 環境中發生這些錯誤，建議使用子樹狀目錄索引。

您可以修改屬性定義上的 searchflags 屬性來啟用子樹狀目錄索引，其結構描述中的值為 65 Active Directory (0x41)，並依照下列步驟使用 ADSEdit：

1. 使用具有結構描述管理員憑證的帳戶，以結構描述主要角色擁有者的身分登入網域控制器。
2. 選取開始和執行，輸入 **`Adsiedit.msc`**。
3. 在 ADSI 編輯工具中，連線至結構描述分割區。
4. 展開 CN=Schema，CN=Configuration，DC=DomainName 容器。
5. 找到「Common-Name」屬性，然後按一下滑鼠右鍵並選取屬性。
6. 找到 searchFlags 屬性，並將其值變更為 **`65 (0x41)`** 以啟用 SubTree 索引與正常索引。

   下圖顯示 ADSI 編輯視窗中的 CN=Common-Name 屬性對話方塊：

7. 選取 OK (確定)。您可以關閉 ADSI 編輯工具。
8. 對於確認，您應該能夠看到事件 ID 1137（來源 ：Active Directory_DomainServices)，這表示 AD 已成功為指定的屬性建立新索引。

如需詳細資訊，請參閱 Microsoft 文件。

使用 AWS 應用程式搜尋使用者或群組時，我收到「無法驗證」錯誤

即使 AD Connector 狀態為作用中，您在搜尋使用者或登入 AWS 應用程式時仍可能會遇到錯誤，例如 WorkSpaces 或 QuickSight。如果 AD Connector 的服務帳戶密碼已變更或已過期，AD Connector 就無法再查詢Active Directory網域。請聯絡您的 AD 管理員並驗證下列項目：

- 檢查 AD Connector 服務帳戶密碼是否尚未過期
- 已檢查 AD Connector 服務帳戶沒有此選項 使用者必須在下次登入時變更密碼。
- 檢查 AD Connector 服務帳戶是否未鎖定。
- 如果您不確定密碼是否已過期或變更，您可以重設服務帳戶密碼，也可以在 AD Connector 中更新相同的密碼。

當我嘗試更新 AD Connector 服務帳戶時，收到有關目錄登入資料的錯誤

嘗試更新 AD Connector 服務帳戶時，您會收到類似下列一或多個項目的錯誤訊息：

訊息：發生錯誤 您的目錄需要更新登入資料。請更新目錄登入資料。發生錯誤 您的目錄需要更新登入資料。更新 AD Connector 服務帳戶登入資料訊息：發生錯誤 您的請求發生問題後，請更新目錄登入資料。請參閱下列詳細資訊。服務帳戶/密碼組合發生錯誤

時間同步和 Kerberos 可能有問題。AD Connector 會將 Kerberos 身分驗證請求傳送至 Active Directory。這些請求具有時間敏感性，如果請求延遲，則會失敗。若要解決此問題，請參閱 建議 - 使用授權時間來源設定根 PDC，並避免文件中的廣泛時間偏移。 Microsoft如需時間服務和同步的詳細資訊，請參閱下列內容：

- Time Windows Service 的運作方式
- 電腦時鐘同步的最大公差
- Windows 時間服務工具和設定

我有一些使用者無法使用我的目錄進行身分驗證

您的使用者帳戶必須啟用 Kerberos 預先驗證。此為新使用者帳戶的預設設定，不應該予以修改。如需此設定的詳細資訊，請前往 Microsoft TechNet 上的預先驗證。

維護問題

以下是 AD Connector 的常見維護問題

- 我的目錄凍結於「已請求」狀態
- Amazon EC2 執行個體的無縫網域聯結已停止運作

我的目錄凍結於「已請求」狀態

如果您的目錄處於「已請求」狀態超過五分鐘，請嘗試刪除目錄後再重新建立。如果問題仍存在，請聯絡 AWS 支援。

Amazon EC2 執行個體的無縫網域聯結已停止運作

如果適用於 EC2 執行個體的無縫域加入原本在運作中，並在 AD Connector 作用中時停止，則 AD Connector 服務帳戶的憑證可能已過期。 過期的登入資料可防止 AD Connector 在 中建立電腦物件 Active Directory。

若要解決這個問題，請依下列順序更新服務帳戶密碼，讓密碼符合以下：

1. 更新 中服務帳戶的密碼Active Directory。
2. 在 中更新 AD Connector 中服務帳戶的密碼 AWS Directory Service。如需詳細資訊，請參閱在 中更新您的 AD Connector 服務帳戶登入資料 AWS Management Console。

> **Important**
>
> 僅更新 中的密碼 AWS Directory Service 不會將密碼變更推送至您現有的內部部署，Active Directory因此請務必依照先前程序中顯示的順序執行。

我無法刪除我的 AD Connector

如果您的 AD Connector 切換到不可操作狀態，您將無法再存取域控制站。當仍有應用程式連結到某個 AD Connector 時，我們會阻止您刪除它，因為可能還有應用程式在使用相應目錄。如需您需要停用的應用程式清單，以便刪除 AD Connector，請參閱 刪除 AD Connector。如果您仍然無法刪除 AD Connector，您可以透過 請求協助AWS 支援。

調查 AD Connector 發行者的一般工具

下列工具可用於疑難排解與建立、身分驗證和連線相關的各種 AD Connector 問題：

DirectoryServicePortTest 工具

DirectoryServicePortTest 測試工具在對 AD Connector 與客戶受管Active Directory或 DNS 伺服器之間的連線問題進行故障診斷時很有幫助。如需如何使用 工具的詳細資訊，請參閱 測試您的 AD Connector。

封包擷取工具

您可以使用內建Windows套件擷取公用程式 (netsh) 來調查和疑難排解潛在的網路或Active Directory通訊 (ldap 和 kerberos) 問題。如需詳細資訊，請參閱 Capture a Network Trace without installing anything 一文。

VPC 流程日誌

若要進一步了解從 AD Connector 接收和傳送哪些請求，您可以設定目錄網路介面的 VPC 流程日誌。您可以透過 AWS Directory Service 描述識別保留給 使用的所有網路介面：`AWS created network interface for directory` *`your-directory-id`*。

簡單的使用案例是在 AD Connector 建立期間，具有大量Active Directory網域控制站的客戶受管網域。您可以使用 VPC 流程日誌並依 Kerberos 連接埠 (88) 進行篩選，以了解Active Directory正在聯絡客戶受管中的哪些網域控制站進行身分驗證。

Simple AD

Simple AD 是由 Samba 4 Active Directory 相容伺服器提供的獨立受管目錄。有兩種大小可用。

- 小型 - 支援最多 500 位使用者 (約 2,000 個物件，包括使用者、群組和電腦)。
- 大型 - 支援最多 5,000 位使用者 (約 20,000 個物件，包括使用者、群組和電腦)。

Simple AD 提供 AWS Managed Microsoft AD 提供的部分功能，包括能夠管理使用者帳戶和群組成員資格、建立和套用群組政策、安全地連線至 Amazon EC2 執行個體，以及提供 Kerberos 型單一登入 (SSO)。不過，請注意 Simple AD 不支援下列功能：多重要素驗證 (MFA)、與其他域的信任關係、Active Directory 管理中心、PowerShell 支援、Active Directory 資源回收筒、群組受管服務帳戶，以及適用於 POSIX 和 Microsoft 應用程式的結構描述延伸。

Simple AD 提供許多優點：

- Simple AD 可讓您更輕鬆地管理執行 Linux 和 Windows 的 amazon EC2 執行個體，並在 AWS 雲端中部署 Windows 應用程式。
- 您現今使用的許多需要 Microsoft Active Directory 支援的應用程式與工具，可搭配簡易 AD 使用。
- Simple AD 中的使用者帳戶允許存取 WorkSpaces、WorkDocs 或 Amazon WorkMail 等 AWS 應用程式。
- 您可以透過 IAM 角色型存取 來管理 AWS 資源 AWS Management Console。
- 每日自動快照允許時間點復原。

Simple AD 不支援下列各項：

- Amazon AppStream 2.0
- Amazon Chime
- Amazon FSx
- Amazon RDS for SQL Server
- Amazon RDS for Oracle
- AWS IAM Identity Center
- 與其他網域的信任關係
- Active Directory 管理中心
- PowerShell

- Active Directory 資源回收桶
- 群組受管服務帳戶
- POSIX 和 Microsoft 應用程式的結構描述延伸

請繼續閱讀本節中的主題，以了解如何建立您自己的 Simple AD。

主題

- Simple AD 入門
- Simple AD 最佳實務
- 維護您的 Simple AD 目錄
- 保護您的 Simple AD 目錄
- 監控您的 Simple AD 目錄
- 從 Simple AD 存取 AWS 應用程式和服務
- 將 Amazon EC2 執行個體加入 Simple AD 的方法
- Simple AD 中的使用者和群組管理
- Simple AD 配額
- Simple AD 疑難排解

Simple AD 入門

Simple AD 在 AWS 雲端中建立全受管的 Samba 型目錄。當您使用 Simple AD 建立目錄時， 會代表您 AWS Directory Service 建立兩個網域控制站和 DNS 伺服器。網域控制站是在 Amazon VPC 中的不同子網路中建立，此備援有助於確保您的目錄即使發生故障，仍能存取。

主題

- Simple AD 先決條件
- 建立您的 Simple AD
- 使用 Simple AD 建立的內容

Simple AD 先決條件

若要建立 Simple AD Active Directory，您需要具有下列項目的 Amazon VPC：

- VPC 必須具有預設硬體租用。
- 兩個不同可用區域中至少有兩個子網路。子網路必須位於相同的無類別網域間路由 (CIDR) 範圍內。如果您想要為您的目錄擴展或調整 VPC 的規模，則務必針對延伸的 VPC CIDR 範圍選取兩個網域控制站子網路。當您建立 Simple AD 時， 會代表您 AWS Directory Service 建立兩個網域控制站和 DNS 伺服器。
  - 如需 CIDR 範圍的詳細資訊，請參閱《Amazon VPCs 使用者指南》中的 VPC 和子網路的 IP 定址。
- 如果您需要 Simple AD 的 LDAPS 支援，我們建議您使用連線至連接埠 389 的 Network Load Balancer 進行設定。此模型可讓您使用強式憑證進行 LDAPS 連線、透過單一 NLB IP 地址簡化 LDAPS 存取，並透過 NLB 自動容錯移轉。Simple AD 不支援在連接埠 636 上使用自簽章憑證。如需如何設定 LDAPS 與簡易 AD 的詳細資訊，請參閱 AWS AWS 安全部落格中的如何設定適用於簡易 AD 的 LDAPS 端點一文。
- 您必須在目錄中啟用下列加密類型：
  - RC4_HMAC_MD5
  - AES128_HMAC_SHA1
  - AES256_HMAC_SHA1
  - 未來加密類型

  > **Note**
  >
  > 停用這些加密類型可能會導致與 RSAT (遠端伺服器管理工具) 的通訊問題，並影響您目錄的可用性。

- 如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的什麼是 Amazon VPC？。

AWS Directory Service 使用兩個 VPC 結構。組成目錄的 EC2 執行個體會在您的 AWS 帳戶之外執行，並由 管理 AWS。其使用兩種網路轉接器，`ETH0` 和 `ETH1`。`ETH0` 是管理轉接器，而且位於您的帳戶外部。`ETH1` 則是建立於您的帳戶內部。

目錄的 `ETH0` 網路的管理 IP 範圍以程式設計方式選擇，以確保它不會與部署目錄的 VPC 發生衝突。此 IP 範圍可以是以下任一對 (因為目錄在兩個子網路中運作)：

- 10.0.1.0/24 & 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 & 192.168.2.0/24

我們透過檢查 ETH1 CIDR 的第一個八位元組來避免衝突。如果以 10 開頭，則我們選擇具有 192.168.1.0/24 和 192.168.2.0/24 子網路並且地址為 192.168.0.0/16 的 VPC。如果第一個八位元位元組不是 10，我們會選擇具有 10.0.1.0/24 和 10.0.2.0/24 子網路並且地址為 10.0.0.0/16 的 VPC。

選取演算法不包含 VPC 上的路由。因此，這種情況可能會導致 IP 路由衝突。

> **Important**
>
> 如果在建立 Simple AD 之後變更任何 Simple AD 先決條件，您的 Simple AD 可能會受損。若要解決 Simple AD 受損狀態，您需要聯絡 AWS 支援。

建立您的 Simple AD

此程序會逐步引導您建立 Simple AD 的所有必要步驟。它旨在讓您快速輕鬆地開始使用 Simple AD，但不適用於大規模生產環境。

步驟

- 先決條件
- 為您的 Simple AD 建立和設定 Amazon VPC
- 建立您的 Simple AD

先決條件

此程序假設下列事項：

- 您有作用中的 AWS 帳戶。
- 您的帳戶尚未達到您想要使用 Simple AD 之區域的 Amazon VPCs 限制。如需 VPC 的詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPC 中的什麼是 Amazon VPC？ 和子網路。
- 您在 區域中沒有 CIDR 為 的現有 VPC`10.0.0.0/16`。
- 您位於可使用 Simple AD 的區域。如需詳細資訊，請參閱的區域可用性 AWS Directory Service。

如需詳細資訊，請參閱Simple AD 先決條件。

為您的 Simple AD 建立和設定 Amazon VPC

首先，您將建立和設定 Amazon VPC 以與 Simple AD 搭配使用。開始此程序之前，請確定您已完成先決條件。

您將建立的 VPC 將有兩個公有子網路。 在您的 VPC 中 AWS Directory Service 需要兩個子網路，且每個子網路必須位於不同的可用區域。

建立 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在 VPC 儀表板中，選擇建立 VPC。
3. 在 VPC 設定下，選擇 VPC 和更多。
4. 如下所示填入欄位：
   - 保持選取名稱標籤自動產生下的自動產生。將專案改為 ADS VPC。
   - IPv4 CIDR 區塊應為 10.0.0.0/16。
   - 保持選取無 IPv6 CIDR 區塊選項。
   - 租用應保留為預設。
   - 針對可用區域數量，選取 2。
   - 針對公有子網路數量，選擇 2。私有子網路數量可以改為 0。
   - 選擇自訂子網路 CIDR 區塊以設定公有子網路 IP 地址範圍。該公有子網路 CIDR 區塊應為 10.0.0.0/20 和 10.0.16.0/20。
5. 選擇建立 VPC。建立 VPC 需要幾分鐘。

建立您的 Simple AD

若要建立新的 Simple AD，請執行下列步驟。開始此程序之前，請確定您已在 先決條件和 中完成下列操作為您的 Simple AD 建立和設定 Amazon VPC。

建立 Simple AD

1. 在 AWS Directory Service 主控台中，選擇目錄，然後選擇設定目錄。
2. 在選取目錄類型頁面上，選擇 Simple AD，然後選擇下一步。
3. 在 Enter directory information (輸入目錄資訊) 頁面上，提供下列資訊：

   Directory size (目錄大小)

   選擇 Small (小型) 或 Large (大型) 尺寸選項。如需尺寸的詳細資訊，請參閱 Simple AD。

組織名稱

將用於登錄用戶端裝置的目錄的唯一組織名稱。

只有當您建立的目錄是啟動 WorkSpaces 的一部分時，此欄位才可用。

目錄 DNS 名稱

目錄的完全合格名稱，例如 `corp.example.com`。

目錄 NetBIOS 名稱

目錄的簡短名稱，例如：`CORP`。

Administrator password (管理員密碼)

目錄管理員的密碼。目錄建立程序會使用使用者名稱`Administrator`和此密碼建立管理員帳戶。

目錄管理者密碼區分大小寫，長度須介於 8 至 64 個字元之間。至少須有一位字元屬於以下四種類型中的三類：

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

Confirm password (確認密碼)

重新輸入管理員密碼。

> **Important**
>
> 請務必儲存此密碼。 AWS Directory Service 不會儲存此密碼，而且無法擷取。不過，您可以從 AWS Directory Service 主控台或使用 ResetUserPassword API 重設密碼。

目錄描述

選擇填寫其他目錄說明。

4. 在 Choose VPC and subnets (選擇 VPC 和子網路) 頁面上，提供下列資訊，然後選擇 Next (下一步)。

VPC

目錄的 VPC。

子網路

選擇網域控制站的子網路。這兩個子網路必須位於不同的可用區域。

5. 在 Review & create (檢閱和建立) 頁面上檢閱目錄資訊，並進行必要的變更。若資訊無誤，請選擇 Create directory (建立目錄)。建立目錄需要幾分鐘的時間。建立後，Status (狀態) 值會變更為 Active (作用中)。

如需使用 Simple AD 建立之項目的詳細資訊，請參閱 使用 Simple AD 建立的內容。

使用 Simple AD 建立的內容

當您Active Directory使用 Simple AD 建立 時， 會代表您 AWS Directory Service 執行下列任務：

- 設定 VPC 內的 Samba 目錄。
- 建立含有使用者名稱 `Administrator` 與指定密碼的目錄管理員帳戶。您可以使用此帳戶來管理目錄。

> **Important**
>
> 請務必儲存此密碼。 AWS Directory Service 不會儲存此密碼，而且無法擷取。不過，您可以從 AWS Directory Service 主控台或使用 ResetUserPassword API 重設密碼。

- 建立目錄控制器的安全群組。
- 建立具備網域管理員權限的帳戶，其名為 `AWSAdminD-`*`xxxxxxxx`*。此帳戶由 用來 AWS Directory Service 執行目錄維護操作的自動化操作，例如擷取目錄快照和 FSMO 角色轉移。此帳戶的登入資料會由 AWS Directory Service安全地存放。
- 自動建立彈性網路介面 (ENI) 並將其與您的每個域控制站建立關聯。這些 ENIs 對 VPC 和 AWS Directory Service 網域控制站之間的連線至關重要，絕不應刪除。您可以透過 AWS Directory Service 描述識別保留給 使用的所有網路介面：「為 directory-idAWS 建立網路介面」。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的彈性網路界面。 AWS Managed Microsoft AD 的預設 DNS 伺服器Active Directory是位於無類別網域間路由 (CIDR)+2 的 VPC DNS 伺服器。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon DNS 伺服器。

> **Note**
>
> 依預設，域控制站會跨區域中的兩個可用區域部署，並連線至您的 Amazon Virtual Private Cloud (VPC)。每天自動進行一次備份，並且對 Amazon Elastic Block Store (EBS) 磁碟區進行加密，以確保靜態資料的安全。一旦域控制站發生故障，將在同一可用區域中使用相同的 IP 地址自動替換，並且可以透過最新的備份執行完整的災難復原。

Simple AD 最佳實務

以下是您應該考慮的一些建議和指導方針，以避免問題並充分利用 Simple AD。

設定：事前準備

建立目錄之前，請考量這些準則。

確認目錄類型是否正確

AWS Directory Service 提供多種方式可Microsoft Active Directory與其他 AWS 服務搭配使用。您可以依所需功能及成本預算，選擇目錄服務：

- AWS Directory Service for Microsoft Active Directory 是一種功能豐富的受Microsoft Active Directory管 AWS 雲端託管。如果您有超過 5，000 名使用者，且需要在託管目錄和內部部署目錄之間 AWS 設定信任關係， AWS 則受管 Microsoft AD 是您的最佳選擇。
- AD Connector 只會將您現有的現場部署連線到 Active Directory AWS。如果您想要將現有的內部部署目錄用於 AWS 服務，AD Connector 會是您的最佳選擇。
- Simple AD 是具有基本Active Directory相容性的低規模、低成本目錄。它支援最多 5,000 名使用者、Samba 4 相容應用程式，以及 LDAP 感知應用程式的 LDAP 相容性。

如需 AWS Directory Service 選項的更詳細比較，請參閱 該選擇哪種。

確認已正確設定您的 VPC 和執行個體

為了連線、管理及使用您的目錄，您必須正確設定與目錄相關聯的 VPC。如需 VPC 安全與聯網需求的資訊，請參閱「建立 AWS Managed Microsoft AD 的先決條件 」、「AD Connector 事前準備 」或「Simple AD 先決條件」。

如果您想要將執行個體新增至網域，請確定您具備連線能力並可遠端存取您的執行個體，如「將 Amazon EC2 執行個體加入 AWS Managed Microsoft AD 的方法」中所述。

留意您的限制

了解特定目錄類型的不同限制。您可以在目錄中儲存的物件數量僅受限於可用儲存空間和物件的彙總大小。有關所選目錄的詳細資訊，請參閱「AWS Managed Microsoft AD 配額」、「AD Connector 配額」或「Simple AD 配額」。

了解目錄 AWS 的安全群組組態和使用

AWS 會建立安全群組，並將其連接到目錄的網域控制器彈性網路介面。 AWS 會設定安全群組，以封鎖到目錄不必要的流量，並允許必要的流量。

修改目錄安全群組

您可以修改目錄的安全群組，但前提是您完全了解安全群組篩選。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的適用於 Linux 執行個體的 Amazon EC2 安全群組一節。不當變更可能會中斷與預期電腦和執行個體的通訊。 AWS 建議不要開啟目錄的其他連接埠，因為這會降低安全性。在進行變更之前，請檢閱AWS 共同責任模型。

> **Warning**
>
> 在技術上，您可以將目錄的安全群組與您建立的其他 EC2 執行個體建立關聯。不過，針對此實務 AWS 建議 。 AWS 可能有理由在不通知的情況下修改安全群組，以解決受管目錄的功能或安全需求。這類變更會影響您要與目錄安全群組建立關聯的任何執行個體，而且可能會干擾具關聯執行個體的操作。此外，將目錄安全群組與您的 EC2 執行個體產生關聯可能會對 EC2 執行個體帶來安全風險。

如果需要信任，請使用 AWS Managed Microsoft AD

Simple AD 不支援信任關係。如果您需要在 AWS Directory Service 目錄和另一個目錄之間建立信任，您應該使用 AWS Directory Service for Microsoft Active Directory。

設定：建立您的目錄

以下是建立目錄時需考慮的一些建議。

記住您的管理員 ID 和密碼

在您設定目錄時，您會提供管理員帳戶的密碼。若是 Simple AD，該帳戶 ID 為 Administrator。請記住您為此帳戶建立的密碼，否則您將無法新增物件至目錄。

了解 AWS 應用程式的使用者名稱限制

AWS Directory Service 支援可用於建構使用者名稱的大多數字元格式。不過，在用於登入 AWS 應用程式的使用者名稱上會強制執行字元限制，例如 WorkSpaces、WorkDocs、Amazon WorkMail 或 QuickSight。這些限制要求不使用下列字元：

- 空格
- 多位元組字元
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> @ 符號只可位於 UPN 尾碼之前。

編寫程式設計自己的應用程式

編寫程式設計自己的應用程式之前，請考慮下列事項：

使用 Windows DC 定位器服務

開發應用程式時，請使用 Windows DC 定位器服務，或使用 AWS Managed Microsoft AD 的動態 DNS (DDNS) 服務來尋找網域控制站 DCs)。請勿使用 DC 地址將應用程式寫死在程式碼中。DC 定位器服務可新增網域控制站到您的部署，協助確保目錄負載分散並讓您充分利用水平擴展。如果您將應用程式繫結到固定的 DC，而該 DC 正在進行修補或復原，則您的應用程式將無法存取該 DC，而不會使用其中一個剩餘的 DC。此外，DC 硬編碼會導致單一 DC 產生熱點。在嚴重的情況下，熱點可能會導致您的 DC 無法回應。這類情況也可能導致 AWS 目錄自動化將目錄標記為受損，並可能觸發取代無回應 DC 的復原程序。

投入生產前先進行負載測試

請務必針對代表您的生產工作負載的物件與請求執行實驗室測試，以確認目錄擴展至您的應用程式負載。如果您需要額外的容量，您應該將 AWS Directory Service 用於 Microsoft Active Directory，這可

讓您新增網域控制站以獲得高效能。如需詳細資訊，請參閱部署 AWS Managed Microsoft AD 的其他網域控制站。

使用高效 LDAP 查詢

從上千個物件針對網域控制站執行廣泛 LDAP 查詢，會佔用單一 DC 的大量 CPU 周期，進而產生熱點現象。這可能會導致查詢期間使用相同 DC 的應用程式受到影響。

維護您的 Simple AD 目錄

您可以使用 AWS Management Console 來維護 Simple AD day-to-day管理任務。您可以維護 Simple AD 的方式包括：

- 檢視 Simple AD 的詳細資訊，例如 DNS 名稱、目錄 ID 和目錄狀態。
- 更新 Simple AD 的 DNS 地址。
- 使用快照還原您的 Simple AD。您也可以建立快照和刪除快照。
- 不再需要 Simple AD 時將其刪除。

檢視 Simple AD 目錄資訊

檢視詳細目錄資訊

1. 在AWS Directory Service 主控台導覽窗格中的 下Active Directory，選取目錄。
2. 選擇您目錄的目錄 ID 連結。目錄的相關資訊會顯示在目錄詳細資訊頁面。

如需 Status (狀態) 欄位的詳細資訊，請參閱「了解您的 Simple AD 目錄狀態」。

設定適用於 Simple AD 的 DNS 伺服器

Simple AD 會將 DNS 請求轉送到 Amazon 為您 VPC 提供的 DNS 伺服器 IP 地址。這些 DNS 伺服器會解析您在 Amazon Route 53 私有託管區域中設定的名稱。只要將您的內部部署電腦指向您的 Simple AD，您就可以解析私有託管區域的 DNS 請求。如需 Route 53 的詳細資訊，請參閱什麼是 Route 53。

請注意，若要讓您的 Simple AD 回應外部 DNS 查詢，包含您 Simple AD 之 VPC 網路存取控制清單 (ACL) 必須設定成允許 VPC 以外的流量。

- 如果您使用的不是 Route 53 私有託管區域，您的 DNS 請求會轉送到公有 DNS 伺服器。

- 如果您使用的是 VPC 外的自訂 DNS 伺服器，而且想要使用私有 DNS，則必須重新設定以使用 VPC 中 EC2 執行個體上的自訂 DNS 伺服器。如需詳細資訊，請參閱使用私有託管區域。
- 如果您希望您的 Simple AD 同時使用您 VPC 內的 DNS 伺服器以及您 VPC 外的私有 DNS 伺服器來解析名稱，您可以使用 DHCP 選項集執行此操作。如需詳細範例，請參閱這篇文章。
- 將 Directory Service'的 DNS 解析與 整合 Amazon Route 53 Resolver。

> **Note**
>
> Simple AD 域不支援 DNS 動態更新。您可以改使用已加入您網域之執行個體上的 DNS 管理員來連線到您的目錄，直接進行變更。

使用快照還原您的 Simple AD

AWS Directory Service 可讓您為 Simple AD 目錄手動擷取資料快照。您可以使用這些快照來執行目錄的時間點還原。您無法擷取 AD Connector 目錄的快照。

主題

- 建立目錄的快照
- 從快照還原您的目錄
- 刪除快照

建立目錄的快照

您可以使用快照，將目錄還原到擷取快照的時間點。若要建立您目錄的手動快照，請執行下列步驟。

> **Note**
>
> 每個目錄只能建立 5 個手動快照。如果您已達到此上限，則必須刪除其中一個現有的手動快照，才能建立其他手動快照。

建立手動快照

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。

3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Maintenance (維護) 索引標籤。
4. 在快照區段中，選擇動作，然後選取建立快照。
5. 在 建立目錄快照對話方塊中，提供快照的名稱 (如果需要)。準備就緒時，選擇建立。

根據您的目錄大小，建立快照可能需要幾分鐘。快照準備就緒時，Status (狀態) 值會變更為 `Completed` (已完成)。

從快照還原您的目錄

從快照還原目錄等同於回到過去的目錄。目錄快照對於它們的建立來源目錄而言是唯一的。一個快照只能還原到建立它的來源目錄。此外，手動快照的支援保留期限上限為 180 天。如需詳細資訊，請參閱 Microsoft 網站上的 Useful shelf life of a system-state backup of Active Directory。

> **Warning**
>
> 我們建議您在進行任何快照還原之前聯絡 AWS 支援 中心；我們也許能夠協助您避免執行快照還原。系統會從時間點進行還原，因此快照還原可能導致資料遺失。請務必了解在完成還原操作之前，所有與目錄相關聯的 DC 和 DNS 伺服器都會處於離線狀態。

若要從快照還原您的目錄，請執行下列步驟。

從快照還原目錄

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Maintenance (維護) 索引標籤。
4. 在快照區段中，選取清單中的快照，選擇動作，然後選取還原快照。
5. 檢閱還原目錄快照對話方塊中的資訊，然後選擇還原。

若是 Simple AD 目錄，還原目錄可能需要幾分鐘。成功還原之後，目錄的狀態值會變更為 `Active`。快照日期之後所進行的任何目錄變更都會遭到覆寫。

刪除快照

刪除快照

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。

2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 Directory details (目錄詳細資訊) 頁面上，選擇 Maintenance (維護) 索引標籤。
4. 在快照區段中，選擇動作，然後選取刪除快照。
5. 確認您要刪除快照，然後選擇刪除。

刪除您的 Simple AD

刪除 Simple AD 時，會刪除所有目錄資料和快照，而且無法復原。刪除目錄之後，所有加入目錄的執行個體會保持不變。不過，您無法使用目錄憑證來登入這些執行個體。您需要使用執行個體的本機使用者帳戶來登入這些執行個體。

刪除 AWS Managed Microsoft AD、Simple AD 或混合目錄時，會刪除所有目錄資料和快照，且無法復原。刪除目錄之後，所有加入目錄的執行個體會保持不變。不過，您無法使用目錄憑證來登入這些執行個體。您需要使用執行個體的本機使用者帳戶來登入這些執行個體。

刪除 AD Connector 時，您的內部部署目錄會保持不變。所有加入目錄的執行個體也會保持不變，並保持在已加入您內部部署目錄的狀態。您仍然可以使用目錄登入資料來登入這些執行個體。

刪除目錄

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。確保您位於部署 Active Directory AWS 區域 的 中。如需詳細資訊，請參閱選擇區域。
2. 確定您要刪除的目錄未啟用 AWS 任何應用程式。啟用 AWS 的應用程式會阻止您刪除 AWS Managed Microsoft AD 或 Simple AD。

   a. 在 Directories (目錄) 頁面中，選擇目錄 ID。

   b. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。在AWS 應用程式和服務區段中，您會看到您的目錄已啟用哪些 AWS 應用程式。

      - 停用 AWS Management Console 存取。如需詳細資訊，請參閱停用 AWS Management Console 存取。
      - 若要停用 Amazon WorkSpaces，您必須從 WorkSpaces 主控台的目錄中取消登錄該服務。如需詳細資訊，請參閱《Amazon WorkSpaces 管理指南》中的刪除目錄。
      - 若要停用 WorkDocs，您必須在 WorkDocs 主控台中刪除 WorkDocs 網站。如需詳細資訊，請參閱《Amazon WorkDocs 管理指南》中的刪除網站一節。

- 若要停用 Amazon WorkMail，您必須在 Amazon WorkMail 主控台中移除 Amazon WorkMail 組織。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的移除組織一節。
- 若要停用 Amazon FSx for Windows File Server，您必須從域中移除 Amazon FSx 檔案系統。如需詳細資訊，請參閱《Amazon FSx for Windows File Server 使用者指南》中的Active Directory在 FSx for Windows File Server 中使用 。 FSx
- 若要停用 Amazon Relational Database Service，您必須從域中移除 Amazon RDS 執行個體。如需詳細資訊，請參閱《Amazon RDS 使用者指南》中的管理域中的資料庫執行個體一節。
- 若要停用 AWS Client VPN 服務，您必須從 Client VPN 端點移除目錄服務。如需詳細資訊，請參閱《 AWS Client VPN 管理員指南》中的使用 Client VPN。
- 若要停用 Amazon Connect，您必須刪除 Amazon Connect 執行個體。如需詳細資訊，請參閱《Amazon Connect 管理指南》中的刪除 Amazon Connect 執行個體。 Amazon Connect
- 若要停用 Amazon QuickSight，您必須取消訂閱 Amazon QuickSight。如需詳細資訊，請參閱《Amazon QuickSight 使用者指南》中的關閉 Amazon QuickSight 您的帳戶。

> **Note**
>
> 如果您正在使用 ， AWS IAM Identity Center 且先前已將其連線至您計劃刪除的 AWS Managed Microsoft AD 目錄，您必須先變更身分來源，才能將其刪除。如需詳細資訊，請參閱《IAM Identity Center 使用者指南》中的變更身分來源一節。

3. 在導覽窗格中，選擇目錄。
4. 只選取要刪除的目錄，然後按一下刪除。刪除目錄需要幾分鐘的時間。刪除目錄之後，該目錄會從您的目錄清單中移除。

保護您的 Simple AD 目錄

本節說明保護 Simple AD 環境的考量事項。

主題

- 如何重設 Simple AD krbtgt 帳戶密碼

如何重設 Simple AD krbtgt 帳戶密碼

krbtgt 帳戶在 Kerberos 票證交換中扮演重要角色。krbtgt 帳戶是用於 Kerberos 票證授予票證 (TGT) 加密的特殊帳戶，在 Kerberos 身分驗證通訊協定的安全性中扮演關鍵角色。在 Samba AD 中，krbtgt 以（已停用）使用者帳戶表示。此帳戶的密碼會在佈建網域時隨機產生。存取此秘密可能會導致無法偵測的網域總數遭到入侵，因為新的 Kerberos 票證可以在不進行稽核的情況下列印。如需詳細資訊，請參閱 Samba 文件。

建議每 90 天定期變更此密碼。您可以從加入 Simple AD 的 Amazon EC2 Windows執行個體重設 krbtgt 帳戶密碼。

> **Note**
>
> AWS Simple AD 採用 Samba-AD 技術。Samba-AD 不會儲存 krbtgt 帳戶的 N-1 雜湊。因此，當 krbtgt 帳戶密碼重設時，Kerberos 用戶端將需要在下次服務票證 (ST) 請求期間交涉新的票證授予票證 (TGT)。為了將潛在的服務中斷降至最低，您應該在上班時間之外排定 krbtgt 帳戶密碼重設。此方法可減輕對持續操作的影響，並確保順暢的身分驗證持續性。

下列程序說明如何從 Amazon EC2 Windows執行個體重設 krbtgt 帳戶密碼。

先決條件

- 在開始此程序之前，請先完成下列步驟：
  - 您已將 EC2 執行個體加入 Simple AD 目錄的網域。
    - 如需如何將 EC2 Windows執行個體加入 Simple AD 的詳細資訊，請參閱 the section called “加入 Windows 執行個體”。
  - 您有 Simple AD 目錄管理員登入資料。您將以此程序的 Simple AD 目錄管理員身分登入。

> **Note**
>
> 有些 Amazon WorkDocs 和 Amazon WorkSpaces AWS 服務 等 會代表您建立 Simple AD。

重設 Simple AD krbtgt 帳戶密碼

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在 Amazon EC2 主控台中，選擇執行個體，然後選取Windows伺服器執行個體。然後選擇 連線。

3. 在連線至執行個體頁面中，選擇 RDP 用戶端。
4. 在 Windows 安全對話方塊中，複製您的本機管理員登入資料，供Windows伺服器電腦登入。使用者名稱可以是下列格式： `NetBIOS-Name\administrator`或 `DNS-Name\administrator`。例如，如果您遵循 中的程序， `corp\administrator` 會是使用者名稱the section called “建立您的 Simple AD”。
5. 登入Windows伺服器電腦後，從開始功能表選擇Windows管理工具資料夾來開啟Windows管理工具。
6. 在Windows管理工具儀表板中，選擇Active Directory使用者和電腦來開啟Active Directory使用者和電腦。
7. 在Active Directory使用者和電腦視窗中，選取檢視，然後選擇啟用進階功能。
8. 在Active Directory使用者和電腦視窗中，從左側面板選取使用者。
9. 尋找名為 krbtgt 的使用者，在使用者上按一下滑鼠右鍵，然後選取重設密碼。
10. 在新視窗中，輸入新密碼，再次輸入，然後選擇確定以重設 krbtgt 帳戶密碼。
11. 在Windows管理工具儀表板中，選擇Active Directory網站和服務。
12. 在Active Directory站台和服務視窗中，展開站台、Default-First-Site-Name和伺服器。
13. 在 NTDS 設定視窗中，在伺服器上按一下滑鼠右鍵，然後選取立即複寫。
14. 針對其他伺服器重複步驟 13 - 14。

監控您的 Simple AD 目錄

您可以進一步了解不同的 Simple AD 狀態及其對 Simple AD 的意義，以充分利用 Simple AD。您也可以使用 Amazon Simple Notification Service 之類的 AWS 服務來監控 Simple AD。Amazon Simple Notification Service 可以傳送 Simple AD 目錄狀態的通知給您。

監控 Simple AD 的任務

- 了解您的 Simple AD 目錄狀態
- 使用 Amazon Simple Notification Service 啟用 Simple AD 目錄狀態通知

了解您的 Simple AD 目錄狀態

下列是各種目錄狀態。

Active (作用中)

此目錄運作正常。 AWS Directory Service 未在目錄中偵測到任何問題。

正在建立

目前正在建立目錄。建立目錄通常需要 20 到 45 分鐘，但所需時間可能因系統負載而不同。

Deleted (已刪除)

目錄已刪除。目錄的所有資源皆已釋出。一旦目錄進入此狀態，便無法復原。

正在刪除

目前正在刪除目錄。目錄會保持這個狀態，直到完全刪除為止。一旦目錄進入此狀態，將無法取消刪除操作，且目錄無法復原。

失敗

無法建立目錄。請刪除此目錄。如果此問題仍存在，請聯絡 AWS 支援 中心 。

Impaired (受損)

目錄正在降級狀態下執行。已偵測到一個或多個問題，且並非所有目錄操作都能以完整的操作容量運作；目前處於狀態有許多可能的原因。其中包括正常的運作維護活動 (例如修補或 EC2 執行個體輪換)、應用程式在您的其中一個網域控制站上的暫時作用區，或您對不慎中斷目錄通訊的網路所做的變更。如果您變更 中概述的設定，目錄的狀態可能會受損Simple AD 先決條件。如需詳細資訊，請參閱 Managed AWS Microsoft AD 故障診斷、AD Connector 疑難排解、Simple AD 疑難排解。對於正常維護相關問題， 會在 40 分鐘內 AWS 解決這些問題。在檢閱疑難排解主題之後，如果您的目錄處於「受損」 狀態超過 40 分鐘，建議您聯絡 AWS 支援 中心。

> **Important**
>
> 目錄處於 Impaired (受損) 狀態時，請勿還原快照。還原快照很難解決受損問題。如需詳細資訊，請參閱使用快照還原 AWS Managed Microsoft AD。

Inoperable (無法操作)

目錄無法運作。所有目錄端點均已回報問題。

Requested (已請求)

目錄的建立請求目前待定中。

RestoreFailed (還原失敗)

從快照中還原目錄失敗，請重試還原操作。如果此情況持續發生，請嘗試其他快照，或聯絡 AWS 支援 中心。

Restoring (正在還原)

目前正從自動或手動快照中還原目錄。從快照中還原目錄通常需要幾分鐘的時間，取決於快照中目錄資料的大小。

如需詳細資訊，請參閱故障診斷 Simple AD 目錄狀態訊息。

使用 Amazon Simple Notification Service 啟用 Simple AD 目錄狀態通知

使用 Amazon Simple Notification Service (Amazon SNS)，當目錄狀態有所變更時，您便可以收到電子郵件或文字 (SMS) 簡訊。如果您的目錄從 Active (作用中) 狀態變成「受損」或「無法操作」狀態，您便會收到通知。當目錄恢復到 Active (作用中) 狀態時，您也會收到通知。

運作方式

Amazon SNS 使用「主題」收集和分發訊息。每個主題都有一或多個訂閱者，接收發佈到該主題的訊息。您可以使用下列步驟，將 AWS Directory Service 做為發佈者新增至 Amazon SNS 主題。當 AWS Directory Service 偵測到目錄狀態變更時，它會發佈訊息至該主題，然後傳送給主題的訂閱者。

您可以將多個目錄當成發布者，建立它們與單一主題的關聯性。您也可以於您之前在 Amazon SNS 中建立的主題中新增目錄狀態訊息。您對可以發佈和訂閱主題的人有精細的控制權。如需 Amazon SNS 的完整資訊，請參閱「什麼是 Amazon SNS？」。

為您的目錄啟用 SNS 簡訊

1. 登入 AWS Management Console 並開啟 AWS Directory Service 主控台。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 選取維護索引標籤。

4. 在目錄監控區段中，選擇動作，然後選取建立通知。
5. 在建立通知頁面上，選取選擇通知類型，然後選擇建立新通知。或者，如果您已有現有的 SNS 主題，您可以選擇與現有的 SNS 主題建立關聯性從這個目錄傳送狀態訊息到該主題。

> **Note**
>
> 如果您選擇建立新的通知，但接著卻為已存在的 SNS 主題使用了相同的主題名稱，則 Amazon SNS 不會建立新的主題，只會在現有的主題中新增新的訂閱資訊。
> 如果您選擇與現有的 SNS 主題建立關聯性，您只能選擇和目錄同一個區域的 SNS 主題。

6. 選擇收件人類型，然後輸入收件人聯絡資訊。如果您輸入適用於 SMS 的電話號碼，請只使用數字。不要包含破折號、空格或括號。
7. (選用) 提供主題的名稱和 SNS 顯示名稱。顯示名稱為不超過 10 個字元的簡稱，包含在這個主題的所有 SMS 訊息中。當您使用 SMS 選項時，需要有顯示名稱。

> **Note**
>
> 如果您登入時使用的是只有 DirectoryServiceFullAccess 受管政策的 IAM 使用者或角色，則您的主題名稱必須以 “DirectoryMonitoring” 開頭。如果您想進一步自訂您的主題名稱，您會需要額外的 SNS 權限。

8. 選擇 Create (建立)。

如果您想要指定其他 SNS 訂閱者，例如額外的電子郵件地址、Amazon SQS 佇列或 AWS Lambda，您可以從 Amazon SNS 主控台執行此操作。

從主題中移除目錄狀態訊息

1. 登入 AWS Management Console 並開啟 AWS Directory Service 主控台。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 選取維護索引標籤。
4. 在目錄監控區段中，選取清單中的相應 SNS 主題名稱，選擇動作，然後選取移除。
5. 選擇移除。

這會移除您在選取的 SNS 主題中做為發布者的目錄。如果您想要刪除整個主題，您可以從 Amazon SNS 主控台執行此操作。

> **Note**
>
> 使用 SNS 主控台刪除 Amazon SNS 主題之前，您應該確保目錄不會向該主題傳送狀態訊息。如果您使用 SNS 主控台刪除 Amazon SNS 主題，此變更不會立即反映在 Directory Services 主控台中。您只會在下次目錄發佈通知到已刪除的主題時收到通知；在這種情況下，您會在目錄的 Monitoring (監控) 標籤中看到指出找不到主題的更新狀態。
> 因此，為了避免遺失重要的目錄狀態訊息，在刪除接收訊息的任何主題之前 AWS Directory Service，請將您的目錄與不同的 Amazon SNS 主題建立關聯。

從 Simple AD 存取 AWS 應用程式和服務

您可以授予 Simple AD 使用者的存取權，以存取 AWS 應用程式和服務。其中一些 AWS 應用程式和服務包括：

- Amazon WorkDocs
- AWS Management Console
- Amazon WorkSpaces

您也可以搭配 Simple AD 使用存取 URLs 和單一登入。

主題

- Simple AD 應用程式相容性政策
- 為您的 Simple AD 啟用存取 AWS 應用程式和服務
- AWS Management Console 使用 Simple AD 登入資料啟用對 的存取
- 建立 Simple AD 的存取 URL
- 啟用單一登入

Simple AD 應用程式相容性政策

Simple AD 是 Samba 的實作，提供許多 Active Directory 的基本功能。由於使用 Active Directory 的自訂和商業off-the-shelf應用程式數量很大， AWS 不會也無法執行正式或廣泛的第三方應用程式與 Simple AD 的相容性驗證。雖然 會與客戶 AWS 合作，嘗試克服他們可能遇到的任何潛在應用程式安裝挑戰，但我們無法保證任何應用程式目前或未來都與 Simple AD 相容。

以下第三方應用程式與 Simple AD 相容：

- 下列平台上的 Microsoft Internet Information Services (IIS)：
  - Windows Server 2003 R2
  - Windows Server 2008 R1
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
- Microsoft SQL Server：
  - SQL Server 2005 R2 (Express、Web 和 Standard 版本)
  - SQL Server 2008 R2 (Express、Web 和 Standard 版本)
  - SQL Server 2012 (Express、Web 和 Standard 版本)
  - SQL Server 2014 (Express、Web 和 Standard 版本)
- Microsoft SharePoint：
  - SharePoint 2010 Foundation
  - SharePoint 2010 Enterprise
  - SharePoint 2013 Enterprise

客戶可以選擇使用 AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD)，根據實際的 Active Directory 提高相容性。

為您的 Simple AD 啟用存取 AWS 應用程式和服務

使用者可以授權 Simple AD 提供 AWS 應用程式和服務，例如 Amazon WorkSpaces 存取您的 Active Directory。您可以啟用或停用下列 AWS 應用程式和服務，以使用 Simple AD。

AWS 應用程式/服務	詳細資訊...
Amazon WorkDocs	如需詳細資訊，請參閱《Amazon WorkDocs 管理指南》
Amazon WorkMail	如需詳細資訊，請參閱《Amazon WorkMail 管理指南》。
Amazon WorkSpaces	您可以直接從 WorkSpaces 建立 Simple AD、AWS Managed Microsoft AD 或 AD Connector

AWS 應用程式/服務	詳細資訊...
	。只要在建立工作空間時啟動 Advanced Setup (進階設定) 即可。 如需詳細資訊，請參閱《Amazon WorkSpaces 管理指南》。
AWS Management Console	如需詳細資訊，請參閱使用 AWS Managed Microsoft AD 登入資料啟用 AWS Management Console 存取。

一旦啟用，您就可以在要授權存取目錄之應用程式或服務的主控台中，管理您目錄的存取。若要在 AWS Directory Service 主控台中尋找 AWS 上述應用程式和服務連結，請執行下列步驟。

顯示目錄的應用程式與服務

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。
4. 檢視 AWS 應用程式和服務區段下的清單。

如需如何使用 授權或取消授權 AWS 應用程式和服務的詳細資訊 AWS Directory Service，請參閱使用 AWS 的應用程式和服務授權 AWS Directory Service。

AWS Management Console 使用 Simple AD 登入資料啟用對 的存取

AWS Directory Service 可讓您授予目錄成員對 的存取權 AWS Management Console。根據預設，您的目錄成員無法存取任何 AWS 資源。您可以將 IAM 角色指派給目錄成員，讓他們能夠存取各種 AWS 服務和資源。IAM 角色定義您的目錄成員可以存取的服務、資源和層級。

您的目錄必須具有存取 URL，才能授予主控台存取權給目錄成員。如需如何檢視目錄詳細資訊及取得您存取 URL 的詳細資訊，請參閱「檢視 AWS Managed Microsoft AD 目錄資訊」。如需如何建立存取 URL 的詳細資訊，請參閱「建立 AWS Managed Microsoft AD 的存取 URL」。

如需如何建立 IAM 角色並將之指派給您目錄成員的詳細資訊，請參閱「授予 AWS Managed Microsoft AD 使用者和群組存取 AWS 具有 IAM 角色的資源」。

主題

- 啟用 AWS Management Console 存取
- 停用 AWS Management Console 存取
- 設定登入工作階段長度

相關 AWS 安全部落格文章

- 如何使用 AWS Management ConsoleAWS Managed Microsoft AD 和您的現場部署登入資料來存取

相關 AWS re:Post 文章

- 如何授予 AWS Management Console 現場部署Active Directory使用者的 存取權？

啟用 AWS Management Console 存取

預設不會啟用任何目錄的主控台存取。若要啟用您目錄使用者和群組的主控台存取，請執行下列步驟：

啟用主控台存取

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。
4. 在 AWS Management Console 區段下，選擇啟用。現在已啟用目錄的主控台存取。

> **Important**
>
> 您必須先將使用者新增至 IAM 角色，使用者才能使用您的存取 URL 登入主控台。如需將使用者指派給 IAM 角色的一般資訊，請參閱「將使用者或群組指派給現有的 IAM 角色」。指派 IAM 角色之後，使用者即可使用您的存取 URL 存取主控台。例如，如果您目錄的存取 URL 是 example-corp.awsapps.com，存取主控台的 URL 會是 https://example-corp.awsapps.com/console/。

停用 AWS Management Console 存取

若要停用您目錄使用者和群組的主控台存取，請執行下列步驟：

停用主控台存取

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。
4. 在 AWS Management Console 區段下，選擇停用。現在已停用目錄的主控台存取。
5. 如果已將任何 IAM 角色指派給目錄中的使用者或群組，則停用按鈕可能無法使用。在此情況下，您必須移除目錄的所有 IAM 角色指派，再繼續進行，包括您目錄中已刪除的使用者或群組指派，這些指派會顯示為已刪除的使用者或已刪除的群組。

   移除所有 IAM 角色指派之後，請重複上述步驟。

設定登入工作階段長度

根據預設，使用者在成功登入主控台到被登出之間，有一小時的時間可以使用其工作階段。在此之後，使用者必須重新登入，才能開始下一小時的工作階段，直到再次被登出。您可以使用下列程序，將每個工作階段的時間長度變更至最多 12 小時。

設定登入工作階段長度

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。
4. 在 AWS 應用程式與服務區段下，選擇 AWS 管理主控台。
5. 在管理資源存取權 AWS 對話方塊中，選擇繼續。
6. 在 Assign users and groups to IAM roles (將使用者和群組指派給 IAM 角色) 頁面中，編輯 Set login session length (設定登入工作階段長度) 下的數值，然後選擇 Save (儲存)。

建立 Simple AD 的存取 URL

存取 URL 會與 AWS 應用程式和服務搭配使用，例如 Amazon WorkDocs，以連線到與您的目錄相關聯的登入頁面。此 URL 必須是全域唯一的。您可以透過執行下列步驟，來建立目錄的存取 URL。

> **Warning**
>
> 為此目錄建立應用程式存取 URL 後即無法變更。建立存取 URL 之後，其他人便無法使用之。如果您刪除目錄，此存取 URL 也會被刪除，在此之後便可供其他帳戶使用。

建立存取 URL

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。
4. 在存取 URL 區段中，如果尚未將存取 URL 指派給目錄，則會顯示建立存取 URL 按鈕。輸入目錄別名，然後選擇建立存取 URL。如果傳回 實體已經存在錯誤，代表指定的目錄別名已經配置。請選擇其他別名並重複此程序。

   存取 URL 以 *<alias>*.awsapps.com 格式顯示。

啟用單一登入

AWS Directory Service 可讓您的使用者從加入目錄的電腦存取 WorkDocs，而不必另外輸入登入資料。

啟用單一登入之前，您需要採取額外的步驟，讓您使用者的 Web 瀏覽器支援單一登入。使用者可能需要修改其 Web 瀏覽器設定，才能啟用單一登入。

> **Note**
>
> 單一登入僅適用於加入 AWS Directory Service 目錄的電腦。它無法用於未加入目錄的電腦。

如果您的目錄是 AD Connector 目錄，且 AD Connector 服務帳戶沒有新增或移除其服務主要名稱屬性的權限，則對於以下的步驟 5 和 6，您有兩個選項：

1. 您可以繼續進行，且系統會提示您輸入具有此權限之目錄使用者的使用者名稱和密碼，以便在 AD Connector 服務帳戶上新增或移除服務主要名稱屬性。這些憑證只會用來啟用單一登入，服務不會存放此資料。 AD Connector 服務帳戶權限不會變更。

2. 您可以委派權限，以允許 AD Connector 服務帳戶新增或移除本身的服務主要名稱屬性，您可以從加入網域的電腦使用具有修改 AD Connector 服務帳戶權限的帳戶，以執行下列 PowerShell 命令。下列命令會讓 AD Connector 服務帳戶只能為本身新增和移除服務主要名稱屬性。

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

使用 WorkDocs 啟用或停用單一登入

1. 在 AWS Directory Service 主控台導覽窗格中，選取目錄。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 Directory details (目錄詳細資訊) 頁面上，選取 Application management (應用程式管理) 索引標籤。
4. 在應用程式存取 URL 區段中，選擇啟用以啟用 WorkDocs 的單一登入。

   如果您看不到啟用按鈕，您可能需要先建立存取 URL，此選項才會顯示。如需如何建立存取 URL 的詳細資訊，請參閱「建立 AWS Managed Microsoft AD 的存取 URL」。
5. 在啟用此目錄的單一登入對話方塊中，選擇啟用。這會啟用目錄的單一登入。

6. 如果您稍後想要使用 WorkDocs 停用單一登入，請選擇停用，然後在停用此目錄的單一登入對話方塊中，再次選擇停用。

主題

- IE 和 Chrome 的單一登入
- Firefox 的單一登入

IE 和 Chrome 的單一登入

若要讓 Microsoft Internet Explorer (IE) 和 Google Chrome 瀏覽器支援單一登入，您必須在用戶端電腦上執行下列任務：

- 將您的存取 URL (例如 https://<##>.awsapps.com) 新增至允許單一登入的網站清單。
- 啟用動態指令碼處理 (JavaScript)。
- 允許自動登入。
- 啟用整合式身分驗證。

您或您的使用者可以手動執行這些任務，或者您可以使用群組原則設定來變更這些設定。

主題

- 手動更新 Windows 上的單一登入
- 手動更新 OS X 的單一登入
- 單一登入的群組政策設定

手動更新 Windows 上的單一登入

若要在 Windows 電腦上手動啟用單一登入，請在用戶端電腦上執行下列步驟。其中一些設定可能已正確設定。

在 Windows 上手動啟用 Internet Explorer 和 Chrome 的單一登入

1. 若要開啟網際網路內容對話方塊，請選擇開始選單，在搜尋方塊中輸入 `Internet Options`，然後選擇網際網路選項。
2. 執行下列步驟，將您的存取 URL 新增至允許單一登入的網站清單：

   a. 在網際網路內容對話方塊中，選取安全性標籤。

b. 選取近端內部網路，然後選擇網站。

c. 在近端內部網路對話方塊中，選擇進階。

d. 將您的存取 URL 新增至網站清單，然後選擇關閉。

e. 在近端內部網路對話方塊中，選擇確定。

3. 若要啟用動態指令碼處理，請執行下列步驟：

a. 在網際網路內容對話方塊的安全性標籤中，選擇自訂等級。

b. 在安全性設定 - 近端內部網路區域對話方塊中，向下捲動到指令碼處理，然後在 Active scripting 下選取啟用。

c. 在安全性設定 - 近端內部網路區域對話方塊中，選擇確定。

4. 若要啟用自動登入，請執行下列步驟：

a. 在網際網路內容對話方塊的安全性標籤中，選擇自訂等級。

b. 在安全性設定 - 近端內部網路區域對話方塊中，向下捲動到使用者驗證，然後在登入下選取只在近端內部網路區域自動登入。

c. 在安全性設定 - 近端內部網路區域對話方塊中，選擇確定。

d. 在安全性設定 - 近端內部網路區域對話方塊中，選擇確定。

5. 若要啟用整合式身分驗證，請執行下列步驟：

a. 在網際網路內容對話方塊中，選取進階標籤。

b. 向下捲動到安全性，然後選取啟用整合式 Windows 驗證。

c. 在網際網路內容對話方塊中，選擇確定。

6. 關閉並重新開啟您的瀏覽器，讓這些變更生效。

手動更新 OS X 的單一登入

若要在 OS X 上手動啟用 Chrome 的單一登入，請在用戶端電腦上執行下列步驟。您需要電腦的管理員權限，才能完成下列步驟。

在 OS X 上手動啟用 Chrome 的單一登入

1. 執行下列命令，將您的存取 URL 新增至 AuthServerAllowlist 政策：

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. 開啟 System Preferences，前往 Profiles 面板，然後刪除 `Chrome Kerberos Configuration` 描述檔。
3. 重新啟動 Chrome，然後在 Chrome 中開啟 chrome://policy 以確認具有此新的設定。

單一登入的群組政策設定

網域管理員可以實作群組原則設定，在加入網域的用戶端電腦上進行單一登入變更。

> **Note**
>
> 如果您使用 Chrome 政策在域中的電腦上管理 Chrome Web 瀏覽器，您必須將存取 URL 新增至 AuthServerAllowlist 政策。如需設定 Chrome 政策的詳細資訊，請前往 Policy Settings in Chrome。

使用群組原則設定啟用 Internet Explorer 和 Chrome 的單一登入

1. 執行下列步驟，建立新的群組原則物件：
   a. 開啟群組原則管理工具，導覽至您的網域，然後選取 Group Policy Objects (群組原則物件)。
   b. 從主選單選擇動作，然後選取新增。
   c. 在新增 GPO 對話方塊中，輸入群組政策物件的描述性名稱 (例如 `IAM Identity Center Policy`)，並將來源入門 GPO 保留設定為 (無)。按一下 OK (確定)。
2. 執行下列步驟，將存取 URL 新增至允許單一登入的網站清單：
   a. 在群組政策管理工具中，導覽至您的域並選取群組政策物件，開啟您 IAM Identity Center 政策的內容 (右鍵) 選單，然後選擇編輯。
   b. 在原則樹狀目錄中，導覽至使用者設定 > 喜好設定 > Windows 設定。
   c. 在 Windows 設定清單中，開啟登錄的內容 (右鍵) 選單，然後選擇新增登錄項目。
   d. 在新登錄內容對話方塊中，輸入下列設定並選擇確定：

      Action

      `Update`

      Hive

      `HKEY_CURRENT_USER`

路徑

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com\<alias>
```

<##> 的值是衍生自您的存取 URL。如果您的存取 URL 是 `https://examplecorp.awsapps.com`，則別名是 `examplecorp` 且登錄機碼會是 `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`。

值名稱

```
https
```

值類型

```
REG_DWORD
```

值資料

```
1
```

3. 若要啟用動態指令碼處理，請執行下列步驟：

   a. 在群組政策管理工具中，導覽至您的域並選取群組政策物件，開啟您 IAM Identity Center 政策的內容 (右鍵) 選單，然後選擇編輯。

   b. 在原則樹狀目錄中，導覽至電腦設定 > 原則 > 系統管理範本 > Windows 元件 > Internet Explorer > 網際網路控制台 > 安全性畫面 > 內部網路區域。

   c. 在內部網路區域清單中，開啟允許動態指令碼處理的內容 (右鍵) 選單，然後選擇編輯。

   d. 在允許動態指令碼處理對話方塊中，輸入下列設定並選擇確定：

      - 選取已啟用選項按鈕。
      - 在選項下，將允許動態指令碼處理設定為啟用。

4. 若要啟用自動登入，請執行下列步驟：

   a. 在群組原則管理工具中，導覽至您的網域並選取群組原則物件，開啟您 SSO 原則的內容 (右鍵) 選單，然後選擇編輯。

   b. 在原則樹狀目錄中，導覽至電腦設定 > 原則 > 系統管理範本 > Windows 元件 > Internet Explorer > 網際網路控制台 > 安全性畫面 > 內部網路區域。

   c. 在內部網路區域清單中，開啟登入選項的內容 (右鍵) 選單，然後選擇編輯。

d. 在登入選項對話方塊中，輸入下列設定並選擇確定：

- 選取已啟用選項按鈕。
- 在選項下，將登入選項設定為只在近端內部網路區域自動登入。

5. 若要啟用整合式身分驗證，請執行下列步驟：

a. 在群組政策管理工具中，導覽至您的域並選取群組政策物件，開啟您 IAM Identity Center 政策的內容 (右鍵) 選單，然後選擇編輯。

b. 在原則樹狀目錄中，導覽至使用者設定 > 喜好設定 > Windows 設定。

c. 在 Windows 設定清單中，開啟登錄的內容 (右鍵) 選單，然後選擇新增登錄項目。

d. 在新登錄內容對話方塊中，輸入下列設定並選擇確定：

Action

```
Update
```

Hive

```
HKEY_CURRENT_USER
```

路徑

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

值名稱

```
EnableNegotiate
```

值類型

```
REG_DWORD
```

值資料

```
1
```

6. 關閉仍然保持開啟狀態的群組原則管理編輯器視窗。

7. 執行下列步驟，將新的原則指派給您的網域：

a. 在群組原則管理樹狀目錄中，開啟網域的內容 (右鍵) 選單，然後選擇連結到現有的 GPO。

b. 在群組政策物件清單中，選取您的 IAM Identity Center 政策，然後選擇確定。

這些變更會在用戶端上的群組原則下次更新，或在使用者下次登入之後生效。

Firefox 的單一登入

若要讓 Mozilla 的 Firefox 瀏覽器支援單一登入，請將您的存取 URL (例如 https://<##>.awsapps.com) 新增至允許單一登入的網站清單。這可手動或透過指令碼自動完成。

主題

- 手動更新單一登入
- 自動更新單一登入

手動更新單一登入

若要在 Firefox 中將您的存取 URL 手動新增至允許的網站清單，請在用戶端電腦上執行下列步驟。

在 Firefox 中將您的存取 URL 手動新增至允許的網站清單

1. 開啟 Firefox，然後開啟 `about:config` 頁面。
2. 開啟 `network.negotiate-auth.trusted-uris` 偏好設定，然後將您的存取 URL 新增至網站清單。請使用逗號 (,) 來分隔多個項目。

自動更新單一登入

身為域管理員，您可以使用指令碼，將存取 URL 新增至網路上所有電腦的 Firefox `network.negotiate-auth.trusted-uris` 使用者偏好設定。如需詳細資訊，請前往 https://support.mozilla.org/zh-TW/questions/939037。

將 Amazon EC2 執行個體加入 Simple AD 的方法

您可以在執行個體啟動時，將 Amazon EC2 執行個體無縫加入您的Active Directory網域。如需詳細資訊，請參閱將 Amazon EC2 Windows 執行個體加入您的 AWS Managed Microsoft AD Active Directory。您也可以啟動 EC2 執行個體，並透過AWS Systems Manager 自動化直接從 AWS Directory Service 主控台加入 Active Directory網域。

如果您需要手動將 EC2 執行個體加入Active Directory網域，您必須在適當的區域和安全群組或子網路中啟動執行個體，然後將執行個體加入網域。

若要從遠端連線到這些執行個體，您必須具備從來源網路連線到執行個體的 IP 連線能力。在大多數情況下，這需要將網際網路閘道連接到您的 VPC，而且執行個體必須具備公有 IP 地址。

主題

- 將 Amazon EC2 Windows 執行個體加入您的 Simple AD Active Directory
- 將 Amazon EC2 Linux 執行個體加入您的 Simple AD Active Directory
- 委派 Simple AD 的目錄聯結權限
- 為 Simple AD 建立 DHCP 選項集

將 Amazon EC2 Windows 執行個體加入您的 Simple AD Active Directory

您可以啟動 Amazon EC2 Windows執行個體並將其加入 Simple AD。或者，您可以手動將現有的 EC2 Windows執行個體加入 Simple AD

Seamlessly join an EC2 Windows

若要無縫加入 EC2 執行個體的網域，您需要完成下列操作：

先決條件

- 擁有 Simple AD 若要進一步了解，請參閱 建立您的 Simple AD。
- 您需要下列 IAM 許可才能無縫加入 EC2 Windows執行個體：
  - 具有下列 IAM 許可的 IAM 執行個體設定檔：
    - `AmazonSSMManagedInstanceCore`
    - `AmazonSSMDirectoryServiceAccess`
  - 將 EC2 加入 Simple AD 的使用者無縫網域需要下列 IAM 許可：
    - AWS Directory Service 許可：
      - `"ds:DescribeDirectories"`
      - `"ds:CreateComputer"`
    - Amazon VPC 許可：
      - `"ec2:DescribeVpcs"`
      - `"ec2:DescribeSubnets"`
      - `"ec2:DescribeNetworkInterfaces"`
      - `"ec2:CreateNetworkInterface"`
      - `"ec2:AttachNetworkInterface"`
    - EC2 許可：
      - `"ec2:DescribeInstances"`
      - `"ec2:DescribeImages"`

    - "ec2:DescribeInstanceTypes"
    - "ec2:RunInstances"
    - "ec2:CreateTags"
  - AWS Systems Manager 許可：
    - "ssm:DescribeInstanceInformation"
    - "ssm:SendCommand"
    - "ssm:GetCommandInvocation"
    - "ssm:CreateBatchAssociation"

建立 Simple AD 時，會使用傳入和傳出規則建立安全群組。若要進一步了解這些規則和連接埠，請參閱 使用 Simple AD 建立的內容。若要無縫加入 EC2 Windows執行個體的網域，您要啟動執行個體的 VPC 應允許 Simple AD 安全群組傳入和傳出規則中允許的相同連接埠。

- 根據您的網路安全和防火牆設定，您可能需要允許額外的傳出流量。此流量適用於 HTTPS （連接埠 443) 到下列端點：

端點	角色
ec2messages. *region*.amazonaws.com	使用 Session Manager 服務建立和刪除工作階段通道。如需詳細資訊，請參閱 AWS Systems Manager 端點和配額。
ssm.*region*.amazonaws.com	的端點 AWS Systems Manager Session Manager。如需詳細資訊，請參閱 AWS Systems Manager 端點和配額。
ssmmessages. *region*.amazonaws.com	使用 Session Manager 服務建立和刪除工作階段通道。如需詳細資訊，請參閱 AWS Systems Manager 端點和配額。
ds.*region*.amazonaws.com	的端點 AWS Directory Service。如需詳細資訊，請參閱的區域可用性 AWS Directory Service。

- 我們建議您使用 DNS 伺服器來解析 Simple AD 網域名稱。若要這樣做，您可以建立 DHCP 選項集。如需詳細資訊，請參閱為 Simple AD 建立 DHCP 選項集。

- 如果您選擇不建立 DHCP 選項集，則 DNS 伺服器將是靜態的，並由 Simple AD 設定為 。

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/ec2/：// 開啟 Amazon EC2 主控台。
2. 在導覽列中，選擇 AWS 區域 與現有目錄相同的 。
3. 在 EC2 儀表板的啟動執行個體區段中，選擇啟動執行個體。
4. 在啟動執行個體頁面上的名稱和標籤區段下，輸入您想要用於 Windows EC2 執行個體的名稱。
5. (選用) 針對新增標籤，新增一個或多個標籤鍵值對來組織、追蹤或控制對此 EC2 執行個體的存取。
6. 在應用程式和作業系統映像 (Amazon Machine Image) 區段中，選擇快速啟動窗格中的 Windows。您可以從 Amazon Machine Image (AMI)下拉式清單中變更 Windows Amazon Machine Image (AMI)。
7. 在執行個體類型區段中，從執行個體類型下拉式清單中選擇您要使用的執行個體類型。
8. 在金鑰對 (登入) 區段中，您可以選擇建立新金鑰對或從現有金鑰對中進行選擇。

   a. 若要建立新的金鑰對，請選擇建立新金鑰對。

   b. 輸入金鑰對的名稱，然後選取金鑰對類型和私有金鑰檔案格式的選項。

   c. 若要將私有金鑰儲存為可與 OpenSSH 搭配使用的格式，請選擇 .pem。若要將私有金鑰儲存為可與 PuTTY 搭配使用的格式，請選擇 .ppk。

   d. 選擇建立金鑰對。

   e. 您的瀏覽器會自動下載私有金鑰檔案。將私有金鑰檔案存放在安全的地方。

   > **Important**
   >
   > 這是您儲存私有金鑰檔案的唯一機會。

9. 在啟動執行個體頁面上的網路設定區段下，選擇編輯。從 VPC – required 下拉式清單中選擇在其中建立目錄的 VPC。
10. 從子網路下拉式清單中選擇 VPC 中的公有子網路之一。您所選取的子網路必須將所有外部流量路由到網際網路閘道。如果沒有，則將無法從遠端連線到執行個體。

    如需有關連線至網際網路閘道的詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用網際網路閘道連線至網際網路一節。

11. 在自動指派公有 IP 下，選擇啟用。

    如需公有和私有 IP 定址的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 執行個體 IP 定址。 Amazon EC2

12. 對於防火牆 (安全群組)設定，您可以使用預設設定或根據需要進行變更。
13. 對於設定儲存設定，您可以使用預設設定或根據需要進行變更。
14. 選取進階詳細資訊區段，從域加入目錄下拉式清單中選取域。

    > **Note**
    >
    > 選擇網域加入目錄後，您可能會看到：
    >
    > 如果 EC2 啟動精靈識別具有非預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
    >
    > - 如果您先前已編輯 SSM 文件，且預期屬性，請選擇關閉並繼續啟動 EC2 執行個體，而不進行任何變更。
    > - 選取此處的刪除現有 SSM 文件連結，以刪除 SSM 文件。這將允許建立具有正確屬性的 SSM 文件。當您啟動 EC2 執行個體時，系統會自動建立 SSM 文件。

15. 對於 IAM 執行個體設定檔，您可以選取現有的 IAM 執行個體設定檔或建立新的設定檔。從 IAM 執行個體設定檔下拉式清單中選取具有 AWS AmazonSSMManagedInstanceCore 和 AmazonSSMDirectoryServiceAccess 受管政策的 IAM 執行個體設定檔。若要建立新的 IAM 設定檔，請選擇建立新的 IAM 設定檔連結，然後執行下列動作：

    1. 選擇建立角色。
    2. 在選取信任的實體下，選取 AWS 服務。
    3. 在 Use case (使用案例) 下，選擇 EC2。
    4. 在新增許可下的政策清單中，選取 AmazonSSMManagedInstanceCore 和 AmazonSSMDirectoryServiceAccess 政策。在搜尋方塊中，輸入 **SSM** 以篩選政策。選擇下一步。

    > **Note**
    >
    > AmazonSSMDirectoryServiceAccess 提供將執行個體加入 Active Directory受管的許可 AWS Directory Service。AmazonSSMManagedInstanceCore 提供使用 AWS Systems Manager 服務所需的最低許可。有關建立具有這些許可的角色的更

多資訊，以及有關可以指派給 IAM 角色的其他許可和政策的資訊，請參閱《AWS Systems Manager 使用者指南》中的為 Systems Manager 建立 IAM 執行個體設定檔一節。

5. 在命名、檢閱和建立頁面上，針對角色名稱輸入角色名稱。您將需要此角色名稱來連接到 EC2 執行個體。
6. (選用) 您可以在描述欄位中提供 IAM 執行個體設定檔的描述。
7. 選擇建立角色。
8. 返回啟動執行個體頁面，然後選擇 IAM 執行個體設定檔旁的重新整理圖示。剛剛建立的 IAM 執行個體設定檔應顯示在 IAM 執行個體設定檔下拉式清單中。選擇這個新的設定檔並將其餘設定保留為預設值。

16. 選擇啟動執行個體。

Manually join an EC2 Windows

若要手動將現有的 Amazon EC2 Windows 執行個體加入 Simple AD Active Directory，必須使用 中指定的參數啟動執行個體將 Amazon EC2 Windows 執行個體加入您的 Simple AD Active Directory。

您需要 Simple AD DNS 伺服器的 IP 地址。此資訊可在目錄服務 > 目錄 > 目錄的目錄 ID 連結 > 目錄詳細資料和網路與安全部分下找到。

將 Windows 執行個體加入 Simple AD Active Directory

1. 使用任何遠端桌面協定用戶端連線到執行個體。
2. 在執行個體上開啟 TCP/IPv4 屬性內容對話方塊。

   a. 開啟 Network Connections (網路連線)。

> **Tip**
>
> 您可以在執行個體上，透過從命令提示執行下列命令，來直接開啟 Network Connections (網路連線)。
>
> ```
> %SystemRoot%\system32\control.exe ncpa.cpl
> ```

b. 開啟任何已啟用網路連線的內容 (右鍵) 選單，然後選擇 Properties (內容)。

c. 在連線內容對話方塊中，開啟 (按兩下) Internet Protocol Version 4 (網際網路協定第 4 版)。

3. 選取使用下列 DNS 伺服器地址，將偏好的 DNS 伺服器和備用 DNS 伺服器地址變更為 Simple AD 提供的 DNS 伺服器的 IP 地址，然後選擇確定。

4. 開啟執行個體的 System Properties (系統內容) 對話方塊，選取 Computer Name (電腦名稱) 標籤，然後選擇 Change (變更)。

> **Tip**
>
> 您可以在執行個體上，透過從命令提示執行下列命令，來直接開啟 System Properties (系統內容對話方塊)。
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. 在成員欄位中，選取網域，輸入 Simple AD Active Directory 的完整名稱，然後選擇確定。

6. 當系統提示您輸入網域管理員的名稱和密碼時，請輸入具有網域加入權限的帳戶使用者名稱和密碼。如需委派這些權限的詳細資訊，請參閱「委派 Simple AD 的目錄聯結權限」。

> **Note**
>
> 您可以輸入網域的完整名稱或 NetBIOS 名稱，後面接著反斜線 (\)，然後輸入使用者名稱。使用者名稱為管理員。例如 **corp.example.com\administrator** 或 **corp\administrator**。

7. 收到歡迎您加入網域的訊息之後，請重新啟動執行個體，讓變更生效。

現在您的執行個體已加入 Simple AD Active Directory 網域，您可以遠端登入該執行個體，並安裝公用程式來管理目錄，例如新增使用者和群組。Active Directory 管理工具可用來建立使用者和群組。如需詳細資訊，請參閱安裝 Simple AD 的 Active Directory 管理工具。

將 Amazon EC2 Linux 執行個體加入您的 Simple AD Active Directory

您可以在 中啟動 Amazon EC2 Linux 執行個體並將其加入您的 Simple AD AWS Management Console。您也可以手動將 EC2 Linux 執行個體加入您的 Simple AD。

系統支援下列 Linux 執行個體分佈和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 位元 x86)
- Red Hat Enterprise Linux 8 (HVM) (64 位元 x86)
- Ubuntu Server 18.04 LTS 及 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Ubuntu 14 和 Red Hat Enterprise Linux 7 和 8 之前的分佈不支援無縫網域聯結功能。

加入 EC2 Linux 執行個體的網域方式：

- 將 Amazon EC2 Linux 執行個體無縫加入您的 Simple AD Active Directory
- 手動將 Amazon EC2 Linux 執行個體加入您的 Simple AD Active Directory

將 Amazon EC2 Linux 執行個體無縫加入您的 Simple AD Active Directory

此程序會將 Amazon EC2 Linux 執行個體無縫加入您的 Simple AD Active Directory。

系統支援下列 Linux 執行個體分佈和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 位元 x86)
- Red Hat Enterprise Linux 8 (HVM) (64 位元 x86)
- Ubuntu Server 18.04 LTS 及 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Ubuntu 14 和 Red Hat Enterprise Linux 7 和 8 之前的分佈不支援無縫網域聯結功能。

先決條件

您必須先完成本節中的程序，才能設定無縫網域加入 Linux 執行個體。

選取無縫域加入服務帳戶

您可以將 Linux 電腦無縫加入 Simple AD 域。為此，您必須建立一個具有建立電腦帳戶許可的使用者帳戶，才能將電腦加入域。儘管 Domain Admins 或其他群組的成員可能有足夠的權限將電腦加入域，但我們不建議這樣做。我們建議您使用具有將電腦加入域所需的最低權限的服務帳戶，這才是最佳做法。

如需如何處理並向服務帳戶委派許可以建立電腦帳戶的資訊，請參閱 委派權限給您的服務帳戶。

建立儲存域服務帳戶的機密

您可以使用 AWS Secrets Manager 來存放網域服務帳戶。如需詳細資訊，請參閱建立 AWS Secrets Manager 秘密。

> **Note**
>
> Secrets Manager 需支付相關費用。如需詳細資訊，請參閱AWS Secrets Manager 《 使用者指南》中的 定價。

建立機密並儲存域服務帳戶資訊

1. 登入 AWS Management Console 並在 https：//https://console.aws.amazon.com/secretsmanager/ 開啟 AWS Secrets Manager 主控台。
2. 選擇 Store a new secret (存放新機密)。
3. 在 Store a new secret (儲存新機密) 頁面中，執行下列動作：
   a. 在秘密類型下，選擇其他類型的秘密。
   b. 在鍵/值對下，執行下列動作：
      i. 在第一個方塊中，輸入 **awsSeamlessDomainUsername**。在相同資料列的下一個方塊中，輸入服務帳戶的使用者名稱。例如，如果您之前使用的是 PowerShell 命令，則服務帳戶名稱將為 **awsSeamlessDomain**。

> **Note**
>
> 您必須輸入完全正確的 **awsSeamlessDomainUsername**。確認頭尾沒有任何空格。否則域加入將會失敗。

ii. 選擇新增列。

iii. 在新的一列的第一個方塊中，輸入 **awsSeamlessDomainPassword**。在同一列的下一個方塊中，輸入服務帳戶的密碼。

> **Note**
>
> 您必須輸入完全正確的 **awsSeamlessDomainPassword**。確認頭尾沒有任何空格。否則域加入將會失敗。

iv. 在加密金鑰下，保留預設值 `aws/secretsmanager`。 選擇此選項時， AWS Secrets Manager 一律會加密秘密。您也可以選擇您建立的金鑰。

v. 選擇下一步。

4. 在秘密名稱下，使用下列格式輸入包含目錄 ID 的秘密名稱，將 *d-xxxxxxxxx* 取代為您的目錄 ID：

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

這在應用程式中將用於擷取機密。

> **Note**
>
> 您必須輸入完全正確的 **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join**，但需要將 *d-xxxxxxxxxx* 替換為目錄 ID。確認頭尾沒有任何空格。否則域加入將會失敗。

5. 將其他所有設定保留為預設值，然後選擇下一步。

6. 針對設定自動輪換，選擇停用自動輪換，然後選擇下一步。

   您可以在儲存後開啟此秘密的輪換。

7. 檢查設定，然後選擇儲存以儲存變更。Secrets Manager 主控台會傳回帳戶中的秘密清單，清單中包含現在的新秘密。

8. 從清單中選擇您新建立的機密名稱，並記下 Secret ARN 值。您會在下一節中用到它。

開啟網域服務帳戶秘密的輪換

我們建議您定期輪換秘密，以改善您的安全狀態。

開啟網域服務帳戶秘密的輪換

- 遵循AWS Secrets Manager 《 使用者指南》中設定 AWS Secrets Manager 秘密的自動輪換中的指示。

  對於步驟 5，請使用AWS Secrets Manager 《 使用者指南》中的輪換範本 Microsoft Active Directory 登入資料。

  如需協助，請參閱AWS Secrets Manager 《 使用者指南》中的疑難排解 AWS Secrets Manager 輪換。

建立必要的 IAM 政策和角色

透過下列步驟建立自訂政策，以允許對 Secrets Manager 無縫域加入機密 (您先前建立的) 進行唯讀存取，以及建立新的 LinuxEC2DomainJoin IAM 角色。

建立 Secrets Manager IAM 讀取政策

您需要使用 IAM 主控台建立一個政策，授予對 Secrets Manager 機密的唯讀存取權。

建立 Secrets Manager IAM 讀取政策

1. 以具有建立 IAM 政策許可的使用者 AWS Management Console 身分登入 。前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。

2. 在導覽窗格中，存取管理，選擇政策。

3. 選擇建立政策。

4. 選擇 JSON 標籤並從下列 JSON 政策文件複製文字。然後將其貼到 JSON 文字方塊中。

> **Note**
>
> 請務必將區域和資源 ARN 取代為您先前建立之秘密的實際區域和 ARN。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. 完成時，選擇 Next (下一步)。政策驗證程式會回報任何語法錯誤。如需詳細資訊，請參閱驗證 IAM 政策。
6. 在檢閱政策頁面上，輸入政策的名稱，例如 **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**。檢閱摘要區段來查看您的政策所授予的許可。然後選擇建立政策來儲存變更。新的政策會出現在受管政策清單中，並且已準備好連接至身分。

> **Note**
>
> 我們建議您為每個機密建立一個政策。這樣做可以確保執行個體只能存取適當的機密，並在執行個體受到入侵時將影響降至最低。

建立 LinuxEC2DomainJoin 角色

您可以使用 IAM 主控台建立將用於域加入 Linux EC2 執行個體的角色。

建立 LinuxEC2DomainJoin 角色

1. 以具有建立 IAM 政策許可的使用者 AWS Management Console 身分登入 。前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格的存取管理下，選擇角色。
3. 在內容窗格中，選擇建立角色。
4. 在 Select type of trusted entity (選擇可信任執行個體類型) 下，選擇 AWS service (服務)。
5. 在使用案例中，選擇 EC2，然後選擇下一步。
6. 對於篩選政策，請執行下列操作：
   a. 輸入 **AmazonSSMManagedInstanceCore**。然後選取清單中相應項目的核取方塊。
   b. 輸入 **AmazonSSMDirectoryServiceAccess**。然後選取清單中相應項目的核取方塊。
   c. 輸入 **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read** 或您在上一個程序中建立的 IAM 政策名稱。然後選取清單中相應項目的核取方塊。
   d. 新增上述三個政策後，選取建立角色。

   > **Note**
   >
   > AmazonSSMDirectoryServiceAccess 提供將執行個體加入 Active Directory受管 的許可 AWS Directory Service。AmazonSSMManagedInstanceCore 提供使用 AWS Systems Manager 服務所需的最低許可。有關建立具有這些許可的角色的更多資訊，以及有關可以指派給 IAM 角色的其他許可和政策的資訊，請參閱《AWS Systems Manager 使用者指南》中的為 Systems Manager 建立 IAM 執行個體設定檔一節。

7. 在角色名稱欄位中輸入新角色的名稱，例如 **LinuxEC2DomainJoin**或您偏好的另一個名稱。
8. (選用) 針對 Role description (角色描述)，輸入描述。
9. （選用）選擇步驟 3：新增標籤以新增標籤下的新增標籤。標籤鍵值對用於組織、追蹤或控制此角色的存取。
10. 選擇建立角色。

將 Linux 執行個體無縫加入您的 Simple AD Active Directory

無縫加入您的 Linux 執行個體

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/ec2/ ：// 開啟 Amazon EC2 主控台。
2. 從導覽列的區域選擇器中，選擇 AWS 區域 與現有目錄相同的 。
3. 在 EC2 儀表板的啟動執行個體區段中，選擇啟動執行個體。
4. 在啟動執行個體頁面的名稱和標籤區段下，輸入您要用於 Linux EC2 執行個體的名稱。
5. （選用）選擇新增其他標籤以新增一或多個標籤鍵值對，以組織、追蹤或控制此 EC2 執行個體的存取。
6. 在應用程式和作業系統映像 (Amazon Machine Image) 區段中，選擇您要啟動的 Linux AMI。

> **Note**
>
> 使用的 AMI 必須具有 AWS Systems Manager (SSM Agent) 2.3.1644.0 版或更新版本。若要透過從 AMI 啟動執行個體來檢查 AMI 中已安裝的 SSM 代理程式版本，請參閱取得目前安裝的 SSM 代理程式版本。如需升級 SSM 代理程式，請參閱在適用於 Linux 的 EC2 執行個體上安裝和設定 SSM 代理程式。
> SSM 在將 Linux 執行個體加入Active Directory網域時使用 `aws:domainJoin` 外掛程式。外掛程式會將 Linux 執行個體的主機名稱變更為 EC2AMAZ-*XXXXXXX* 格式。如需 的詳細資訊`aws:domainJoin`，請參閱AWS Systems Manager 《 使用者指南》中的AWS Systems Manager 命令文件外掛程式參考。

7. 在執行個體類型區段中，從執行個體類型下拉式清單中選擇您要使用的執行個體類型。
8. 在金鑰對 (登入) 區段中，您可以選擇建立新金鑰對或從現有金鑰對中進行選擇。若要建立新的金鑰對，請選擇建立新金鑰對。輸入金鑰對的名稱，然後選取金鑰對類型和私有金鑰檔案格式的選項。若要將私有金鑰儲存為可與 OpenSSH 搭配使用的格式，請選擇 .pem。若要將私有金鑰儲存為可與 PuTTY 搭配使用的格式，請選擇 .ppk。選擇建立金鑰對。您的瀏覽器會自動下載私有金鑰檔案。將私有金鑰檔案存放在安全的地方。

> **Important**
>
> 這是您儲存私有金鑰檔案的唯一機會。

9. 在啟動執行個體頁面上的網路設定區段下，選擇編輯。從 VPC – required 下拉式清單中選擇在其中建立目錄的 VPC。

10. 從子網路下拉式清單中選擇 VPC 中的公有子網路之一。您所選取的子網路必須將所有外部流量路由到網際網路閘道。如果沒有，則將無法從遠端連線到執行個體。

    如需有關連線至網際網路閘道的詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用網際網路閘道連線至網際網路一節。

11. 在自動指派公有 IP 下，選擇啟用。

    如需公有和私有 IP 定址的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 執行個體 IP 定址。 Amazon EC2

12. 對於防火牆 (安全群組)設定，您可以使用預設設定或根據需要進行變更。
13. 對於設定儲存設定，您可以使用預設設定或根據需要進行變更。
14. 選取進階詳細資訊區段，從域加入目錄下拉式清單中選取域。

    > **Note**
    >
    > 選擇網域加入目錄後，您可能會看到：
    >
    > 如果 EC2 啟動精靈識別具有非預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
    >
    > - 如果您先前已編輯 SSM 文件，且預期屬性，請選擇關閉並繼續啟動 EC2 執行個體，而不進行任何變更。
    > - 選取此處的刪除現有 SSM 文件連結，以刪除 SSM 文件。這將允許建立具有正確屬性的 SSM 文件。當您啟動 EC2 執行個體時，系統會自動建立 SSM 文件。

15. 針對 IAM 執行個體描述檔，選擇您先前在先決條件區段 步驟 2：建立 LinuxEC2DomainJoin 角色中建立的 IAM 角色。
16. 選擇啟動執行個體。

> **Note**
>
> 如果您使用 SUSE Linux 執行無縫域加入，則需要重新啟動才能進行身分驗證。若要從 Linux 終端重新啟動 SUSE，請鍵入 sudo reboot。

手動將 Amazon EC2 Linux 執行個體加入您的 Simple AD Active Directory

除了 Amazon EC2 Windows 執行個體之外，您也可以將特定 Amazon EC2 Linux 執行個體加入 Simple AD Active Directory。系統支援下列 Linux 執行個體分佈和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 位元 x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64 位元 x86)
- Ubuntu Server 18.04 LTS 及 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> 其他 Linux 分佈和版本也許能正常運作，但尚未經過測試。

先決條件

在將 Amazon Linux、CentOS、Red Hat 或 Ubuntu 執行個體加入目錄之前，必須先依照 將 Amazon EC2 Linux 執行個體無縫加入您的 Simple AD Active Directory 中的指定啟動執行個體。

> **Important**
>
> 以下某些程序若未正確執行，可能會導致您的執行個體無法連線或無法使用。因此，我們強烈建議您在執行這些程序之前，對您的執行個體進行備份或擷取快照。

將 Linux 執行個體加入您的目錄

使用以下其中一個標籤，依照您的特定 Linux 執行個體的步驟：

Amazon Linux

1. 使用任何 SSH 用戶端連線到執行個體。

2. 設定 Linux 執行個體以使用 AWS Directory Service所提供 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動進行設定，請參閱 AWS 知識中心的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，了解為特定 Linux 分佈和版本設定持久性 DNS 伺服器的方式。
3. 請確定您的 Amazon Linux - 64 位元執行個體處於最新狀態。

```
sudo yum -y update
```

4. 在您的 Linux 執行個體上安裝所需的 Amazon Linux 套件。

> **Note**
>
> 系統可能已安裝其中一些套裝服務。
> 在安裝套件時，可能會出現好幾個跳出式設定畫面。您通常可以將這些畫面中的欄位留白。

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> 如需協助確定您所使用的 Amazon Linux 版本，請參閱 《Amazon EC2 Linux 執行個體使用者指南》中的識別 Amazon Linux 映像。

5. 使用下列命令將執行個體加入目錄。

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

example.com 域中具備域加入權限的帳戶。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
...
 * Successfully enrolled machine in realm
```

6. 設定 SSH 服務以允許密碼身分驗證。

   a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. 將 PasswordAuthentication 設定設為 yes。

   ```
   PasswordAuthentication yes
   ```

   c. 重新啟動 SSH 服務。

   ```
   sudo systemctl restart sshd.service
   ```

   或使用：

   ```
   sudo service sshd restart
   ```

7. 重新啟動執行個體之後，請執行下列步驟，以使用任何 SSH 用戶端連線到該執行個體，並將 Domain Admins 群組新增至 sudoers 清單：

   a. 使用下列命令開啟 sudoers 檔案：

   ```
   sudo visudo
   ```

   b. 在 sudoers 檔案的底部加入下列程式碼，然後儲存檔案。

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (上述範例使用 "\<space>" 來建立 Linux 空白字元。)

CentOS

1. 使用任何 SSH 用戶端連線到執行個體。

2. 設定 Linux 執行個體以使用 AWS Directory Service所提供 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動進行設定，請參閱 AWS 知識中心的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，了解為特定 Linux 分佈和版本設定持久性 DNS 伺服器的方式。
3. 請確定您的 CentOS 7 執行個體處於最新狀態。

```
sudo yum -y update
```

4. 在您的 CentOS 7 執行個體上安裝必要的套裝服務。

> **Note**
>
> 系統可能已安裝其中一些套裝服務。
> 在安裝套件時，可能會出現好幾個跳出式設定畫面。您通常可以將這些畫面中的欄位留白。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 使用下列命令將執行個體加入目錄。

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

example.com 域中具備域加入權限的帳戶。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
...
 * Successfully enrolled machine in realm
```

6. 設定 SSH 服務以允許密碼身分驗證。
   a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

```
sudo vi /etc/ssh/sshd_config
```

b. 將 PasswordAuthentication 設定設為 yes。

```
PasswordAuthentication yes
```

c. 重新啟動 SSH 服務。

```
sudo systemctl restart sshd.service
```

或使用：

```
sudo service sshd restart
```

7. 重新啟動執行個體之後，請執行下列步驟，以使用任何 SSH 用戶端連線到該執行個體，並將 Domain Admins 群組新增至 sudoers 清單：

a. 使用下列命令開啟 sudoers 檔案：

```
sudo visudo
```

b. 在 sudoers 檔案的底部加入下列程式碼，然後儲存檔案。

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(上述範例使用 "\<space>" 來建立 Linux 空白字元。)

Red hat

1. 使用任何 SSH 用戶端連線到執行個體。
2. 設定 Linux 執行個體以使用 AWS Directory Service所提供 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動進行設定，請參閱 AWS 知識中心的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，了解為特定 Linux 分佈和版本設定持久性 DNS 伺服器的方式。
3. 確定 Red Hat 64 位元執行個體是最新版本。

```
sudo yum -y update
```

4. 在您的 Linux 執行個體上，安裝必要的 Red Hat 套件。

> **Note**
>
> 系統可能已安裝其中一些套裝服務。
> 在安裝套件時，可能會出現好幾個跳出式設定畫面。您通常可以將這些畫面中的欄位留白。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 使用下列命令將執行個體加入目錄。

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

在 *example.com* 域中帳戶的 sAMAccountName 具備域加入權限。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
...
 * Successfully enrolled machine in realm
```

6. 設定 SSH 服務以允許密碼身分驗證。
   a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

```
sudo vi /etc/ssh/sshd_config
```

   b. 將 PasswordAuthentication 設定設為 yes。

```
PasswordAuthentication yes
```

   c. 重新啟動 SSH 服務。

```
sudo systemctl restart sshd.service
```

或使用：

```
sudo service sshd restart
```

7. 重新啟動執行個體之後，請執行下列步驟，以使用任何 SSH 用戶端連線到該執行個體，並將 Domain Admins 群組新增至 sudoers 清單：

   a. 使用下列命令開啟 sudoers 檔案：

   ```
   sudo visudo
   ```

   b. 在 sudoers 檔案的底部加入下列程式碼，然後儲存檔案。

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (上述範例使用 "\<space>" 來建立 Linux 空白字元。)

Ubuntu

1. 使用任何 SSH 用戶端連線到執行個體。
2. 設定 Linux 執行個體以使用 AWS Directory Service所提供 DNS 伺服器的 DNS 伺服器 IP 地址。欲執行此作業，您可以在連接到 VPC 的 DHCP 選項集中進行設定，或在執行個體上手動設定。如果您想要手動進行設定，請參閱 AWS 知識中心的如何將靜態 DNS 伺服器指派給私有 Amazon EC2 執行個體，了解為特定 Linux 分佈和版本設定持久性 DNS 伺服器的方式。
3. 確定 Ubuntu 64 位元執行個體是最新版本。

   ```
   sudo apt-get update
   sudo apt-get -y upgrade
   ```

4. 在您的 Linux 執行個體上，安裝必要的 Ubuntu 套件。

   > **Note**
   >
   > 系統可能已安裝其中一些套裝服務。

在安裝套件時，可能會出現好幾個跳出式設定畫面。您通常可以將這些畫面中的欄位留白。

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. 停用反向 DNS 解析，並將預設領域設定為網域的 FQDN。Ubuntu 執行個體在 DNS 中必須能夠反向解析，領域才能使用。否則，您必須依照下列步驟，停用在 /etc/krb5.conf 中的反向 DNS：

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. 使用下列命令將執行個體加入目錄。

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

在 *example.com* 域中帳戶的 sAMAccountName 具備域加入權限。請在系統提示時，輸入該帳戶的密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS Managed Microsoft AD 的目錄聯結權限」。

example.com

目錄的完整 DNS 名稱。

```
...
 * Successfully enrolled machine in realm
```

7. 設定 SSH 服務以允許密碼身分驗證。

a. 在文字編輯器中開啟 /etc/ssh/sshd_config 檔案。

```
sudo vi /etc/ssh/sshd_config
```

b. 將 PasswordAuthentication 設定設為 yes。

```
PasswordAuthentication yes
```

c. 重新啟動 SSH 服務。

```
sudo systemctl restart sshd.service
```

或使用：

```
sudo service sshd restart
```

8. 重新啟動執行個體之後，請執行下列步驟，以使用任何 SSH 用戶端連線到該執行個體，並將 Domain Admins 群組新增至 sudoers 清單：

a. 使用下列命令開啟 `sudoers` 檔案：

```
sudo visudo
```

b. 在 `sudoers` 檔案的底部加入下列程式碼，然後儲存檔案。

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(上述範例使用 "\<space>" 來建立 Linux 空白字元。)

> **Note**
>
> 使用 Simple AD 時，若您在 Linux 執行個體上，以「強制使用者在第一次登入時變更密碼」選項建立使用者帳戶，則該使用者最初便無法使用 kpasswd 變更其密碼。為了能夠在第一次登入時變更密碼，網域管理員必須使用 Active Directory 管理工具更新使用者密碼。

從 Linux 執行個體管理帳戶

若要從 Linux 執行個體在 Simple AD 中管理帳戶，您必須更新 Linux 執行個體上的特定組態檔案，如下所示：

1. 在 /etc/sssd/sssd.conf 檔案中將 krb5_use_kdcinfo 設為 False。例如：

```
[domain/example.com]
    krb5_use_kdcinfo = False
```

2. 您需要重新啟動 sssd 服務，才能使設定生效：

```
$ sudo systemctl restart sssd.service
```

或者，您可以使用：

```
$ sudo service sssd start
```

3. 如果您將從 CentOS Linux 執行個體管理使用者，您還必須編輯 /etc/smb.conf 檔案以包含：

```
[global]
  workgroup = EXAMPLE.COM
  realm = EXAMPLE.COM
  netbios name = EXAMPLE
  security = ads
```

限制帳戶登入存取

由於在 Active Directory 中定義了所有帳戶，因此目錄中的所有使用者預設可登入該執行個體。您可以在 sssd.conf 中使用 ad_access_filter 只允許特定使用者登入執行個體。例如：

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

表示唯有使用者是特定群組的成員時，才可以存取執行個體。

cn

應該具備存取權的群組通用名稱。在此範例中，群組名稱為 *admins*。

ou

這代表上述群組所在的組織單位。在此範例中，OU 為 *Testou*。

dc

這代表網域的網域元件。在此範例中為 *example*。

dc

這代表額外的網域元件。在此範例中為 *com*。

您必須將 ad_access_filter 手動新增至 /etc/sssd/sssd.conf。

在文字編輯器中開啟 /etc/sssd/sssd.conf 檔案。

```
sudo vi /etc/sssd/sssd.conf
```

執行此動作後，您的 sssd.conf 可能如下所示：

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

您需要重新啟動 sssd 服務，才能使設定生效：

```
sudo systemctl restart sssd.service
```

或者，您可以使用：

```
sudo service sssd restart
```

ID 映射

ID 映射可以透過兩種方法執行，以維護 UNIX/Linux 使用者識別符 (UID) 和群組識別符 (GID) 以及 Windows 和Active Directory安全識別符 (SID) 身分之間的統一體驗。這些方法是：

1. 集中
2. 分散式

> **Note**
>
> 中的集中式使用者身分映射Active Directory需要可攜式作業系統界面或 POSIX。

集中式使用者身分映射

Active Directory 或其他輕量型目錄存取通訊協定 (LDAP) 服務為 Linux 使用者提供 UID 和 GID。在 中 Active Directory，如果已設定 POSIX 延伸，這些識別符會存放在使用者的屬性中：

- UID - Linux 使用者名稱（字串）
- UID 號碼 - Linux 使用者 ID 號碼（整數）
- GID 號碼 - Linux 群組 ID 號碼（整數）

若要將 Linux 執行個體設定為使用來自 的 UID 和 GIDActive Directory，`ldap_id_mapping = False`請在 sssd.conf 檔案中設定 。在設定此值之前，請確認您已將 UID、UID 號碼和 GID 號碼新增至 中的使用者和群組Active Directory。

分散式使用者身分映射

如果 Active Directory沒有 POSIX 擴充功能，或者如果您選擇不集中管理身分映射，Linux 可以計算 UID 和 GID 值。Linux 使用使用者的唯一安全識別符 (SID) 來維持一致性。

若要設定分散式使用者 ID 映射，`ldap_id_mapping = True`請在 sssd.conf 檔案中設定 。

常見問題

如果您設定 `ldap_id_mapping = False`，有時啟動 SSSD 服務將會失敗。此失敗的原因是因為不支援變更 UIDs。當您從 ID 映射變更為 POSIX 屬性，或從 POSIX 屬性變更為 ID 映射時，我們建議您刪除 SSSD 快取。如需 ID 映射和 ldap_id_mapping 參數的進一步詳細資訊，請參閱 Linux 命令列中的 sssd-ldap(8) man 頁面。

連線至 Linux 執行個體

當使用者使用 SSH 用戶端連線到執行個體時，系統會提示其輸入使用者名稱。如果使用者想輸入使用者名稱，可以善用 username@example.com 或 EXAMPLE\username 格式。視您使用的 Linux 發行版本而定，回應將如下所示：

Amazon Linux、Red Hat Enterprise Linux 及 CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
```

```
  Swap usage:   0%
```

委派 Simple AD 的目錄聯結權限

若要將電腦加入到您的目錄，您需要有將電腦加入目錄權限的帳戶。

使用 Simple AD，Domain Admins 群組的成員就有足夠的權限，可將電腦加入目錄。

不過，最佳實務是您應該使用只有所需最低權限的帳戶。下列程序示範如何建立稱為 `Joiners` 的新群組，並將權限委派給需要將電腦加入目錄的這個群組。

您必須在已加入您的目錄，並已安裝 Active Directory User and Computers (Active Directory 使用者和電腦) MMC 嵌入的電腦上執行此程序。您也必須以網域管理員的身分登入。

委派 Simple AD 目錄加入權限

1. 開啟 Active Directory User and Computers (Active Directory 使用者和電腦)，並在導覽樹狀目錄中選取您的根網域。
2. 在左側的導覽樹狀目錄中，開啟 Users (使用者) 內容選單 (按一下滑鼠右鍵)，然後選擇 New (新增)，然後選擇 Group (群組)。
3. 在 New Object - Group (新增物件 - 群組) 對話方塊中輸入如下內容，並選擇 OK (確定)。
   - 在 Group Name (群組名稱) 中，輸入 **`Joiners`**。
   - 針對 Group scope (群組範圍) 選擇 Global (全域)。
   - 針對 Group type (群組類型)，選擇 Security (安全性)。
4. 在導覽樹狀目錄中，選取您的根網域。從 Action (動作) 選單，選擇 Delegate Control (委派控制)。
5. 在 Delegation of Control Wizard (委派控制精靈) 頁面，選擇 Next (下一步)，然後選擇 Add (新增)。
6. 在 Select Users, Computers, or Groups (選取使用者、電腦或群組) 對話方塊中輸入 `Joiners`，並選擇 OK (確定)。如果找到多個物件，請選取在上述步驟中建立的 `Joiners` 群組。選擇下一步。
7. 在 Tasks to Delegate (要委派的任務) 頁面上，選取 Create a custom task to delegate (建立要委派的自訂任務)，然後選擇 Next (下一步)。
8. 選取 Only the following objects in the folder (僅限資料夾中的下列物件)，然後選取 Computer objects (電腦物件)。
9. 選取 Create selected objects in this folder (在此資料夾中建立選取的物件) 和 Delete selected objects in this folder (在此資料夾中刪除選取的物件)。然後選擇下一步。

10. 選取 Read (讀取) 和 Write (寫入)，然後選擇 Next (下一步)。

11. 驗證 Completing the Delegation of Control Wizard (完成委派控制精靈) 頁面中的資訊，然後選擇 Finish (完成)。
12. 建立使用高強度密碼的使用者，並將此使用者新增至 `Joiners` 群組。然後，使用者將有足夠的權限 AWS Directory Service 連接到 目錄。

為 Simple AD 建立 DHCP 選項集

AWS 建議您為 AWS Directory Service 目錄建立 DHCP 選項集，並將 DHCP 選項集指派給目錄所在的 VPC。這可讓該 VPC 中的任何執行個體指向指定的網域和 DNS 伺服器，以解析其網域名稱。

如需 DHCP 選項集的詳細資訊，請參閱《Amazon VPC 使用者指南》https://docs.aws.amazon.com/vpc/latest/userguide/VPC_DHCP_Options.html中的 DHCP 選項集。

為目錄建立 DHCP 選項集

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 DHCP Options Sets (DHCP 選項集)，然後選擇 Create DHCP options set (建立 DHCP 選項集)。
3. 在 Create DHCP options set (建立 DHCP 選項集) 頁面上，輸入您目錄的下列值：

   名稱

   選項集的選用標籤。

   網域名稱

   您目錄的完整名稱，例如 `corp.example.com`。

   Domain name servers (網域名稱伺服器)

   您 AWS提供的目錄 DNS 伺服器的 IP 地址。

   > **Note**
   >
   > 您可以前往 AWS Directory Service 主控台導覽窗格，選取目錄，然後選擇正確的目錄 ID，來找到這些地址。

NTP servers (NTP 伺服器)

將此欄位留白。

NetBIOS name servers (NetBIOS 名稱伺服器)

將此欄位留白。

NetBIOS node type (NetBIOS 節點類型)

將此欄位留白。

4. 選擇 Create DHCP options set (建立 DHCP 選項集)。DHCP 選項清單會隨即顯示新的 DHCP 選項集。
5. 記下新 DHCP 選項集的 ID (dopt-*xxxxxxxx*)。您可以使用它建立新選項集與 VPC 的關聯。

變更與 VPC 相關的 DHCP 選項集

建立 DHCP 選項集之後，便無法再進行修改。如果您希望 VPC 使用不同的 DHCP 選項集，則必須建立新選項集，並與 VPC 建立關聯。您也可以將 VPC 設定為完全不使用 DHCP 選項。

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 選取 VPC，然後選擇動作、編輯 VPC 設定。
4. 對於 DHCP 選項集，選取選項集或選取無 DHCP 選項集，然後選取儲存。

若要使用命令列變更與 VPC 相關聯的 DHCP 選項集，請參閱以下內容：

- AWS CLI：associate-dhcp-options
- AWS Tools for Windows PowerShell：Register-EC2DhcpOption

Simple AD 中的使用者和群組管理

使用者代表具有目錄存取權的個人或實體。群組非常適合對使用者群組授予或拒絕權限，而無需將這些權限逐一套用到各個使用者。如果使用者移到不同的組織，只要將該使用者移到不同的群組，他們就會自動接收新組織所需的權限。

若要在 AWS Directory Service 目錄中建立使用者和群組，您必須使用任何已加入 AWS Directory Service 目錄的執行個體 （從內部部署或 EC2)，並以具有建立使用者和群組權限的使用者身分登入。您也需要在 EC2 執行個體上安裝Active Directory工具，以便使用使用者和電腦嵌入來新增Active Directory使用者和群組。如需有關如何設定 EC2 執行個體及安裝必要工具的詳細資訊，請參閱「將 Amazon EC2 執行個體加入 Simple AD 的方法」。

> **Note**
>
> 您的使用者帳戶必須啟用 Kerberos 預先驗證。此為新使用者帳戶的預設設定，不應該予以修改。如需此設定的詳細資訊，請前往 Microsoft TechNet 上的 Preauthentication (預先驗證)。

下列主題說明如何建立和管理使用者和群組。

主題

- 安裝 Simple AD 的 Active Directory 管理工具
- 建立 Simple AD 使用者
- 刪除 Simple AD 使用者
- 重設 Simple AD 使用者密碼
- 建立 Simple AD 群組
- 將 Simple AD 使用者新增至群組

安裝 Simple AD 的 Active Directory 管理工具

若要Active Directory從 Amazon EC2 Windows Server 執行個體管理 ，您需要在執行個體上安裝 Active Directory Domain Services 和Active Directory輕量型目錄服務工具。使用下列程序在 EC2 Windows Server 執行個體上安裝這些工具。

先決條件

在開始此程序之前，請先完成下列操作：

1. 建立 Simple ADActive Directory。如需詳細資訊，請參閱建立您的 Simple AD。
2. 啟動 EC2 Windows Server 執行個體並將其加入您的 Simple ADActive Directory。EC2 執行個體需要下列政策才能建立使用者和群組： **`AmazonSSMManagedInstanceCore`**和 **`AmazonSSMDirectoryServiceAccess`**。如需詳細資訊，請參閱將 Amazon EC2 Windows 執行個體加入您的 Simple AD Active Directory。

3. 您需要 Active Directory 網域管理員的登入資料。這些登入資料是在建立 Simple AD 時建立的。如果您遵循 中的程序建立您的 Simple AD，您的管理員使用者名稱會包含您的 NetBIOS 名稱 **corp\administrator**。

在 EC2 Windows Server 執行個體上安裝 Active Directory 管理工具

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在 Amazon EC2 主控台中，選擇 執行個體並選取您剛建立的執行個體，然後選擇連線。
3. 在連線至執行個體頁面中，選擇 RDP 用戶端。
4. 在 RDP 用戶端索引標籤中，選擇下載遠端桌面檔案，然後選擇取得密碼以擷取密碼。
5. 在取得 Windows 密碼中，選擇上傳私有金鑰檔案。選擇與 Windows Server 執行個體關聯的 .pem 私有金鑰檔案。上傳私有金鑰檔案後，選取解密密碼。
6. 在 Windows 安全對話方塊中，複製 Windows Server 電腦的本機管理員登入資料以登入。使用者名稱可以是下列格式：*NetBIOS-Name*\administrator或 *DNS-Name*\administrator。例如，如果您遵循 中的程序， **corp\administrator** 會是使用者名稱建立您的 Simple AD。
7. 登入 Windows Server 執行個體後，請選擇 Server Manager，從開始功能表開啟 Server Manager。
8. 在伺服器管理員儀表板中，選擇新增角色和功能。
9. 在 Add Roles and Features Wizard (新增角色和功能精靈) 中選擇 Installation Type (安裝類型)，並選取 Role-based or feature-based installation (角色型或功能型安裝)，接著選擇 Next (下一步)。
10. 在 Server Selection (伺服器選項) 下，請確認本機伺服器已選取，然後在左側導覽窗格中選擇 Features (功能)。
11. 在功能樹狀目錄中，開啟遠端伺服器管理工具和角色管理工具，接著選取 AD DS 和 AD LDS 工具。選取 AD DS 和 AD LDS 工具後，會選取 、AD DS 工具和 AD LDS Snap-in 和 Command-Line Tools Active Directory的模組PowerShell。向下捲動並選取 DNS 伺服器工具，然後選擇下一步。
12. 請檢閱資訊，然後選擇 Install (安裝)。功能安裝完成後，即可在「開始」功能表的系統管理工具資料夾中，使用 Active Directory 域服務和 Active Directory 輕量型目錄服務工具。

建立 Simple AD 使用者

使用下列程序建立已加入 Simple AD 目錄的 Amazon EC2 執行個體的使用者。在建立使用者之前，您需要完成安裝 Active Directory 管理工具中所述的程序。

> **Note**
>
> 使用 Simple AD 時，若您在 Linux 執行個體上，以「強制使用者在第一次登入時變更密碼」選項建立使用者帳戶，則該使用者最初便無法使用 kpasswd 變更其密碼。為了能夠在第一次登入時變更密碼，網域管理員必須使用 Active Directory 管理工具更新使用者密碼。

建立使用者

1. 連線至安裝了 Active Directory 管理工具的執行個體。
2. 從 Windows 開始功能表開啟 Active Directory 使用者和電腦工具。您可以在 Windows 管理工具資料夾中找到此工具的捷徑。

   > **Tip**
   >
   > 您可以在執行個體上透過命令提示執行下列命令，以直接開啟 Active Directory 使用者和電腦工具箱。
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. 在目錄樹狀目錄中，選取您要存放使用者的目錄 NetBIOS 名稱 OU 下的 OU（例如 **corp\Users**）。如需 中目錄使用的 OU 結構的詳細資訊 AWS，請參閱 使用 AWS Managed Microsoft AD 建立的內容。
4. 在動作選單上，選擇新增，再選擇使用者開啟新增使用者精靈。
5. 在精靈的第一頁上，輸入下列欄位的值，然後選擇下一步。
   - 名字
   - 姓氏
   - User logon name (使用者登入名稱)
6. 在精靈的第二頁上，針對密碼和確認密碼輸入臨時密碼。確定使用者必須在下次登入時變更密碼選項已選取。其他選項則不需選取。選擇下一步。

7. 在精靈的第三頁上，確認新使用者的資訊正確，然後選擇完成。新使用者就會顯示在 Users (使用者) 資料夾中。

刪除 Simple AD 使用者

使用下列程序刪除已加入 Simple AD 目錄的 Amazon EC2 Windows 執行個體的使用者。

刪除使用者

1. 連線至安裝了 Active Directory 管理工具的執行個體。
2. 從 Windows 開始功能表開啟 Active Directory 使用者和電腦工具。此工具的捷徑位於 Windows 管理工具資料夾中。

   > **Tip**
   >
   > 您可以在執行個體上透過命令提示執行下列命令，以直接開啟 Active Directory 使用者和電腦工具箱。
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. 在目錄樹狀目錄中，選取包含您要刪除之使用者的 OU （例如，**corp\Users**)。
4. 選取要刪除的使用者。在動作功能表上，選擇刪除。
5. 將出現一個對話方塊，提示您確認要刪除該使用者。選擇是以刪除使用者。這將永久刪除所選使用者。

重設 Simple AD 使用者密碼

使用者必須遵守 中定義的密碼政策Active Directory。有時這可以充分利用使用者，包括Active Directory管理員，他們忘記密碼。發生這種情況時， AWS Directory Service 如果使用者位於 Simple AD 中，您可以使用 快速重設使用者的密碼。

您必須以具有重設密碼所需許可的使用者身分登入。如需許可的詳細資訊，請參閱「管理 AWS Directory Service 資源存取許可的概觀」。

您可以為 中的任何使用者重設密碼，Active Directory但有下列例外：

- 您可以根據建立 時使用的 NetBIOS 名稱，重設組織單位 (OU) 內任何使用者的密碼Active Directory。例如，如果您遵循 中的程序建立您的 Simple AD，您的 NetBIOS 名稱會是 CORP，而您可以重設的使用者密碼會是 Corp/Users OU 的成員。
- 您無法根據建立 時所使用的 NetBIOS 名稱，重設 OU 外任何使用者的密碼Active Directory。如需 Simple AD OU 結構的詳細資訊，請參閱 使用 Simple AD 建立的內容。
- 您無法為屬於兩個網域的任何使用者重設密碼。除了管理員使用者之外，您也無法重設網域管理員或企業管理員群組成員的任何使用者的密碼。
- 您無法為網域管理員或企業管理員群組成員的任何使用者重設密碼，但管理員使用者除外。

您可以使用下列任一方法來重設使用者密碼：

- AWS Management Console
- AWS CLI

AWS Management Console

1. 在AWS Directory Service 主控台導覽窗格的 下Active Directory，選擇目錄，然後在清單中選取Active Directory您要重設使用者密碼的 。
2. 在目錄詳細資訊頁面上，選擇動作，然後選擇重設密碼。
3. 在重設使用者密碼對話方塊中，在使用者名稱中輸入密碼需要變更的使用者名稱。
4. 在新密碼和確認密碼中輸入密碼，然後選擇重設密碼。

AWS CLI

1. 若要安裝 AWS CLI，請參閱安裝或更新最新版本的 AWS CLI。
2. 開啟 AWS CLI。
3. 輸入下列命令，並將目錄 ID、使用者名稱和密碼取代**`jane.doeP@ssw0rd`**為您的Active Directory目錄 ID 和所需登入資料。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 reset-user-password 一節。

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "P@ssw0rd"
```

建立 Simple AD 群組

使用下列程序，以加入 Simple AD 目錄的 Amazon EC2 執行個體建立安全群組。在建立安全群組之前，您需要完成安裝 Active Directory 管理工具中所述的程序。

建立群組

1. 連線至安裝了 Active Directory 管理工具的執行個體。
2. 開啟 Active Directory 使用者和電腦工具。系統管理工具資料夾具有此工具的捷徑。

> **Tip**
>
> 您可以在執行個體上透過命令提示執行下列命令，以直接開啟 Active Directory 使用者和電腦工具箱。
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. 在樹狀目錄中，在目錄的 NetBIOS 名稱 OU 下選取要在其中儲存群組的 OU (例如，"Corp \Users")。如需 中目錄使用的 OU 結構的詳細資訊 AWS，請參閱 使用 AWS Managed Microsoft AD 建立的內容。
4. 在 Action (動作) 選單上，按一下 New (新增)，再按一下 Group (群組) 開啟新增群組精靈。
5. 在群組名稱中輸入群組名稱，選取滿足您需求的群組範圍，然後為群組類型選取安全性。如需 Active Directory 群組範圍和安全群組的詳細資訊，請參閱 Microsoft Windows Server 文件中的 Active Directory 安全群組一節。
6. 按一下 OK (確定)。新安全群組就會顯示在使用者資料夾中。

將 Simple AD 使用者新增至群組

請使用下列步驟以在加入您 Simple AD 目錄的 EC2 執行個體上將使用者新增至安全群組。

將使用者新增至群組

1. 連線至安裝了 Active Directory 管理工具的執行個體。
2. 開啟 Active Directory 使用者和電腦工具。系統管理工具資料夾具有此工具的捷徑。

> **Tip**
>
> 您可以在執行個體上透過命令提示執行下列命令，以直接開啟 Active Directory 使用者和電腦工具箱。
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. 在樹狀目錄中，選取目錄的 NetBIOS 名稱 OU 下儲存群組的 OU，然後選取要向其新增使用者為成員的群組。

4. 在動作選單上，按一下屬性開啟群組的屬性對話方塊。
5. 選取成員索引標籤，然後按一下新增...。
6. 對於輸入要選取的物件名稱，輸入您要新增的使用者名稱，然後按一下確定。相應名稱將顯示在成員清單中。再按一次 OK (確定) 以更新群組成員資格。
7. 透過在使用者資料夾中選取使用者並點選動作選單中的屬性開啟屬性對話方塊，確認使用者現在是否是該群組的成員。選取成員群組索引標籤。您應該可以在群組清單中看到使用者所屬的群組的名稱。

Simple AD 配額

一般而言，您不應新增超過 500 名使用者至小型 Simple AD 目錄，且不應新增超過 5,000 個使用者至大型 Simple AD 目錄。如需更靈活的擴展選項和其他 Active Directory 功能，請考慮改用 AWS Directory Service for Microsoft Active Directory (Standard Edition 或 Enterprise Edition)。

以下是 Simple AD 的預設配額。除非另有說明，否則每項配額都是依區域規定。

Simple AD 配額

資源	預設配額
Simple AD 目錄	10
手動快照 *	每個 Simple AD 5 個

* 手動快照配額無法變更。

> **Note**
>
> 您無法將公有 IP 地址連接至 AWS 彈性網路介面 (ENI)。

Simple AD 疑難排解

以下可協助您疑難排解在建立或使用 Simple AD 時可能遇到的一些常見問題Active Directory。

主題

- 密碼復原
- 將使用者新增至 Simple AD 時，我收到「KDC 無法滿足請求的選項」錯誤
- 我無法更新已加入我的網域之執行個體的 DNS 名稱或 IP 地址 (DNS 動態更新)
- 我無法使用 SQL Server 帳戶登入 SQL Server
- 我的 Simple AD 卡在「請求」狀態
- 我在建立 Simple AD 時收到「可用區域限制」錯誤
- 我的一些使用者無法使用我的 Simple AD 進行身分驗證
- 其他資源
- 故障診斷 Simple AD 目錄狀態訊息

密碼復原

如果使用者忘記密碼或無法登入您的 Simple AD 目錄，您可以使用 AWS Management ConsolePowerShell或 重設密碼 AWS CLI。

如需詳細資訊，請參閱重設 Simple AD 使用者密碼。

將使用者新增至 Simple AD 時，我收到「KDC 無法滿足請求的選項」錯誤

當 Samba CLI 用戶端未正確將`net`命令傳送至所有網域控制站時，就會發生這種情況。如果您在使用`net ads`命令將使用者新增至 Simple AD 目錄時看到此錯誤訊息，請使用 `-S`引數並指定其中一個網域控制站的 IP 地址。如果仍然發生錯誤，請嘗試其他網域控制器。您也可以使用 Active Directory 管理工具，以將使用者新增到目錄。如需詳細資訊，請參閱安裝 Simple AD 的 Active Directory 管理工具。

我無法更新已加入我的網域之執行個體的 DNS 名稱或 IP 地址 (DNS 動態更新)

Simple AD 域不支援 DNS 動態更新。您可以改使用已加入您網域之執行個體上的 DNS 管理員來連線到您的目錄，直接進行變更。

我無法使用 SQL Server 帳戶登入 SQL Server

如果您嘗試搭配 SQL Server 帳戶使用 SQL Server Management Studio (SSMS) 來登入在 2012 R2 Amazon EC2 Windows 執行個體上執行的 SQL Server，您可能會收到錯誤。當 SSMS 以網域使用者身分執行並可能導致錯誤 時，即使提供有效的登入資料`Login failed for user`，也會發生此問題。這是一個已知問題，並且 AWS 正在積極努力解決它。

若要解決此問題，您可以使用身分Windows驗證而非 SQL 身分驗證登入 SQL Server。或是以本機使用者身分啟動 SSMS，而不是簡易 AD 網域使用者。

我的 Simple AD 卡在「請求」狀態

如果您的 Simple AD 已處於 `Requested` 狀態超過五分鐘，請嘗試刪除目錄並重新建立。如果問題仍存在，請聯絡 AWS 支援 中心 。

我在建立 Simple AD 時收到「可用區域限制」錯誤

在 2012 年之前建立的某些 AWS 帳戶可能可以存取美國東部（維吉尼亞北部）、美國西部（加利佛尼亞北部）或亞太區域（東京）區域中不支援 AWS Directory Service 目錄的可用區域。如果您在建立目錄時收到類似錯誤，請選擇不同可用區域中的子網路，然後重試建立目錄。

我的一些使用者無法使用我的 Simple AD 進行身分驗證

您的使用者帳戶必須啟用 Kerberos 預先驗證。這是新使用者帳戶的預設設定，不應該予以修改。如需此設定的詳細資訊，請前往 Simple AD TechNet 上的預先驗證。

其他資源

下列資源可協助您在使用 時進行故障診斷 AWS。

- AWS 知識中心 – 尋找FAQs和其他資源的連結，以協助您疑難排解問題。
- AWS 支援中心 - 取得技術支援。

- AWS 進階支援中心 - 取得進階技術支援。

主題

- 故障診斷 Simple AD 目錄狀態訊息

故障診斷 Simple AD 目錄狀態訊息

當 Simple AD 受損或無法操作時，目錄狀態訊息會包含其他資訊。狀態訊息會顯示在 AWS Directory Service 主控台中，或由 `DescribeDirectories` API 在`DirectoryDescription.StageReason`成員中傳回。如需目錄狀態的詳細資訊，請參閱「了解 AWS Managed Microsoft AD 目錄狀態」。

以下是 Simple AD 目錄的狀態訊息：

主題

- 目錄服務的彈性網路介面未連接
- 執行個體偵測到的問題
- 目錄中缺少重要的 AWS Directory Service 預留使用者
- 關鍵 AWS Directory Service 預留使用者需要屬於網域管理員群組
- 關鍵 AWS Directory Service 預留使用者已停用
- 主要網域控制器沒有所有 FSMO 角色
- 網域控制器複寫失敗

目錄服務的彈性網路介面未連接

描述

在目錄建立期間代表您建立以建立與 VPC 網路連線的關鍵彈性網路界面 (ENI) 不會連接到目錄執行個體。此目錄支援 AWS 的應用程式將無法運作。您的目錄無法連線至內部部署網路。

故障診斷

如果 ENI 已分離但仍然存在，請聯絡 支援。如果 ENI 被刪除，則無法解決問題，且目錄將永久無法使用。您必須刪除目錄並建立新的目錄。

執行個體偵測到的問題

描述

執行個體偵測到內部錯誤。這通常表示監控服務正在積極嘗試復原受損的執行個體。

故障診斷

在大多數情況下，這是一個暫時性問題，目錄最終會回到「作用中」狀態。如果問題仍然存在，請聯絡 支援 以取得更多協助。

目錄中缺少重要的 AWS Directory Service 預留使用者

描述

建立 Simple AD 時， 會在目錄中 AWS Directory Service 建立名為 的服務帳戶`AWSAdmin`*`D-xxxxxxxxx`*。當找不到此服務帳戶時，就會收到此錯誤。若沒有此帳戶， AWS Directory Service 就無法對目錄執行管理功能，而導致目錄無法使用。

故障診斷

若要修正此問題，請將目錄還原到刪除服務帳戶之前所建立的舊版快照。系統會自動一天擷取 Simple AD 目錄快照一次。如果刪除此帳戶之後已超過五天，您可能無法將目錄還原到此帳戶存在時的狀態。如果您無法從此帳戶存在的快照還原目錄，您的目錄可能會變成永久無法使用。若是這種情況，您必須刪除目錄並建立新的目錄。

關鍵 AWS Directory Service 預留使用者需要屬於網域管理員群組

描述

建立 Simple AD 時， 會在目錄中 AWS Directory Service 建立名為 的服務帳戶`AWSAdmin`*`D-xxxxxxxxx`*。當此服務帳戶不是 `Domain Admins` 群組的成員時，就會收到此錯誤。需要此群組的成員資格，才能授予執行維護和復原操作所需的 AWS Directory Service 權限，例如轉移 FSMO 角色、加入新目錄控制器的網域，以及從快照還原。

故障診斷

使用 Active Directory 使用者和電腦工具將服務帳戶重新加入 `Domain Admins` 群組。

關鍵 AWS Directory Service 預留使用者已停用

描述

建立 Simple AD 時，會在目錄中 AWS Directory Service 建立名為 的服務帳戶`AWSAdmin`*`D-xxxxxxxxx`*。當停用此服務帳戶時，就會收到此錯誤。必須啟用此帳戶，AWS Directory Service 才能對目錄執行維護和復原操作。

故障診斷

使用 Active Directory 使用者和電腦工具來重新啟用服務帳戶。

主要網域控制器沒有所有 FSMO 角色

描述

Simple AD 目錄控制器不會擁有所有 FSMO 角色。如果 FSMO 角色所屬的 Simple AD 目錄控制器不正確，AWS Directory Service 就無法保證特定行為和功能。

故障診斷

使用 Active Directory 工具將 FSMO 角色移回原始工作目錄控制器。如需有關移動 FSMO 角色的詳細資訊，請參閱 https://docs.microsoft.com/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles-in-ad-ds。如果這無法修正問題，請聯絡 支援 以取得更多協助。

網域控制器複寫失敗

描述

Simple AD 目錄控制器無法彼此複寫。這可能是由於下列一或多個問題所致：

- 目錄控制器的安全群組未開啟正確的連接埠。
- 網路 ACL 的限制太高。
- VPC 路由表未正確地在目錄控制器之間路由網路流量。
- 另一個執行個體已升階為目錄中的網域控制器。

故障診斷

如需 VPC 網路需求的詳細資訊，請參閱 AWS Managed Microsoft AD 的 建立 AWS Managed Microsoft AD 的先決條件、AD Connector 的 AD Connector 事前準備 或 Simple AD 的 Simple AD 先決條件。如果您的目錄中有不明的網域控制器，您必須將它降階。如果您的 VPC 網路設定正確，但仍然繼續出現錯誤，請聯絡 支援 以取得更多協助。

中的安全性 AWS Directory Service

的雲端安全性 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，這些架構專為符合最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。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 Directory Service，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 時套用共同責任模型 AWS Directory Service。下列主題說明如何設定 AWS Directory Service 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 AWS Directory Service 資源。

安全性主題

您可以在本節中找到下列安全性主題：

- 的身分和存取管理 AWS Directory Service
- 在 中記錄和監控 AWS Directory Service
- 的合規驗證 AWS Directory Service
- 中的彈性 AWS Directory Service
- 中的基礎設施安全性 AWS Directory Service

其他安全性主題

您可以在本指南中找到更多的安全性主題：

帳戶、信任 AWS 和資源存取

- AWS Managed Microsoft AD Administrator 帳戶和群組許可
- 群組受管服務帳戶
- 在 AWS Managed Microsoft AD 和自我管理 AD 之間建立信任關係
- Kerberos 限制委派

- 授予 AWS Managed Microsoft AD 使用者和群組存取 AWS 具有 IAM 角色的資源
- 使用 AWS 的應用程式和服務授權 AWS Directory Service

保護您的目錄

- 保護您的 AWS Managed Microsoft AD
- 保護您的 AD Connector 目錄

記錄和監控

- 監控您的 AWS Managed Microsoft AD
- 監控您的 AD Connector 目錄

彈性

- AWS Managed Microsoft AD 修補和維護

的身分和存取管理 AWS Directory Service

存取 AWS Directory Service 需要 AWS 登入資料，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 Directory Service 目錄。下列各節提供如何使用 AWS Identity and Access Management (IAM) 的詳細資訊 AWS Directory Service ，並透過控制可存取的人員來協助保護您的資源：

- 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 AWS Directory Service 資源。例如，您必須擁有建立 AWS Directory Service 目錄或建立目錄快照的許可。

下列各節說明如何管理 的許可 AWS Directory Service。我們建議您先閱讀概觀。

- 管理 AWS Directory Service 資源存取許可的概觀
- 針對 使用身分型政策 (IAM 政策） AWS Directory Service
- AWS Directory Service API 許可：動作、資源和條件參考

管理 AWS Directory Service 資源存取許可的概觀

每個 AWS 資源都由 AWS 帳戶擁有。因此，建立或存取資源的許可受許可政策的約束。不過，帳戶管理員是具有管理員許可的使用者，可以將許可連接到資源。也能夠將許可政策連接至 IAM 身分，例如使用者、群組和角色，以及一些服務，例如 AWS Lambda 也支援將許可政策連接至 資源。

> **Note**
>
> 如需帳戶管理員角色的相關資訊，請參閱《IAM 使用者指南》中的 IAM 最佳實務。

主題

- AWS Directory Service 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、資源和主體
- 在政策中指定條件

AWS Directory Service 資源和操作

在 中 AWS Directory Service，主要資源是目錄。由於 AWS Directory Service 支援目錄快照資源，因此您只能在現有目錄的內容中建立快照。此快照稱為子資源。

這些資源各與唯一的 Amazon Resource Name (ARN) 相關聯，如下表所示。

資源類型	ARN 格式
目錄	`arn:aws:ds: region:account-id :directory/ external-directory-id`

資源類型	ARN 格式
快照	`arn:aws:ds:` *`region`*`:`*`account-id`* `:snapshot/` *`external-snapshot-id`*

AWS Directory Service 包含兩個服務命名空間，根據您執行的操作類型而定。

- `ds` 服務命名空間提供一組操作，以使用適當的資源。如需可用操作的清單，請參閱 Directory Service 動作。
- `ds-data` 服務命名空間為 Active Directory 物件提供一組操作。如需可用操作的清單，請參閱目錄服務資料 API 參考。

了解資源所有權

資源擁有者是建立資源 AWS 的帳戶。也就是說，資源擁有者是驗證建立資源之請求的委託人實體（根帳戶、IAM 使用者或 IAM 角色）AWS 的帳戶。下列範例說明其如何運作：

- 如果您使用 AWS 帳戶的根帳戶登入資料來建立 AWS Directory Service 資源，例如 目錄， AWS 您的帳戶就是該資源的擁有者。
- 如果您在 AWS 帳戶中建立 IAM 使用者，並將建立 AWS Directory Service 資源的許可授予該使用者，該使用者也可以建立 AWS Directory Service 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 AWS Directory Service 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 AWS Directory Service 資源。該角色所屬 AWS 的帳戶擁有資源 AWS Directory Service 。

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 內容中使用 IAM AWS Directory Service。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 IAM 政策語法和說明的詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策參考。

連接至 IAM 身分的政策稱為以身分為基礎的政策 (IAM 政策），而連接至資源的政策稱為以資源為基礎的政策。 僅 AWS Directory Service 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)

您可以將政策連接到 IAM 身分。例如，您可以執行下列動作：

- 將許可政策連接至您帳戶中的使用者或群組 – 帳戶管理員可以使用與特定使用者相關聯的許可政策，授予該使用者建立 AWS Directory Service 資源的許可，例如新目錄。
- 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 `Describe` 之所有動作的許可。這些動作會顯示 AWS Directory Service 資源的相關資訊，例如目錄或快照。請注意， `Resource`元素中的萬用字元 (*) 表示允許對帳戶擁有的所有 AWS Directory Service 資源執行動作。

JSON

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

如需搭配 使用身分型政策的詳細資訊 AWS Directory Service，請參閱 針對 使用身分型政策 (IAM 政策） AWS Directory Service。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。 AWS Directory Service 不支援以資源為基礎的政策。

指定政策元素：動作、效果、資源和主體

對於每個 AWS Directory Service 資源，服務會定義一組 API 操作。如需詳細資訊，請參閱AWS Directory Service 資源和操作。如需可用的 API 操作清單，請參閱 Directory Service 動作。

若要授予這些 API 操作的許可， AWS Directory Service 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。對於 AWS Directory Service 資源，一律在 IAM 政策中使用萬用字元 (*)。如需詳細資訊，請參閱AWS Directory Service 資源和操作。
- 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，`ds:DescribeDirectories` 許可允許使用者執行 AWS Directory Service `DescribeDirectories` 操作。
- 效果 - 您可以指定使用者請求特定動作的效果。可以為允許或拒絕。如果您未明確授予存取 (允許) 資源，則隱含地拒絕存取。您也可以明確拒絕資源存取，這樣做可確保使用者無法存取資源，即使不同政策授予存取也是一樣。
- 委託人：在身分識別型政策 (IAM 政策) 中，政策所連接的使用者就是隱含委託人。對於以資源為基礎的政策，您可以指定要接收許可的使用者、帳戶、服務或其他實體 （僅適用於以資源為基礎的政策）。 AWS Directory Service 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 IAM JSON 政策參考。

如需顯示所有 AWS Directory Service API 動作及其適用的資源的資料表，請參閱 AWS Directory Service API 許可：動作、資源和條件參考。

在政策中指定條件

當您授予許可時，可以使用存取政策語言來指定政策應該何時生效的條件。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。沒有 AWS Directory Service特定的條件金鑰。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。

AWS 的 受管政策 AWS Directory Service

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。 AWS 服務 當新的 啟動或新的 API 操作可供現有服務使用時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

下列各節說明特定的 AWS 受管政策 AWS Directory Service。您可以將這些政策連接到您帳戶中的使用者。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管政策： AWSDirectoryServiceFullAccess

您可將 `AWSDirectoryServiceFullAccess` 政策連接到 IAM 身分。若要檢視此政策的完整許可，請參閱《 AWS 受管政策參考》中的 AWSDirectoryServiceFullAccess。

此政策會授予管理許可，允許委託人完整存取所有 AWS Directory Service 動作。具有這些許可的主體可以建立、設定和管理目錄，包括 Simple AD、AD Connector 和 Managed Microsoft AD。他們也可以管理目錄共用、信任關係和監控組態。此政策包含管理目錄服務所需基礎網路基礎設施的許可。

許可詳細資訊

此政策包含以下許可：

- `ds` – 允許主體完整存取所有 AWS Directory Service 動作。

- ec2 – 允許主體管理網路介面、安全群組，並描述目錄操作所需的 VPC 資源。
- sns – 允許主體建立和管理 SNS 主題以進行目錄監控，特別是名稱開頭為「DirectoryMonitoring」的主題。
- iam – 允許主體列出目錄服務操作的 IAM 角色。
- organizations – 允許主體管理 AWS Organizations 整合，並啟用/停用目錄服務的服務存取。

AWS 受管政策： AWSDirectoryServiceReadOnlyAccess

您可將 AWSDirectoryServiceReadOnlyAccess 政策連接到 IAM 身分。若要檢視此政策的完整許可，請參閱《 AWS 受管政策參考》中的 AWSDirectoryServiceReadOnlyAccess。

此政策授予唯讀許可，允許使用者檢視 中的資訊 AWS Directory Service。已連接此政策的主體無法對目錄或其組態進行任何更新。例如，具有這些許可的主體可以檢視目錄詳細資訊、信任關係和監控組態，但無法建立新的目錄或修改現有的目錄。他們也可以檢視與目錄相關聯的相關 EC2 網路資源和 SNS 主題。

許可詳細資訊

此政策包含以下許可：

- ds – 允許使用者執行唯讀動作，以傳回目錄資訊。這包括以 Check、Describe、List、 Get或開頭的 API 操作Verify。
- ec2 – 允許使用者描述與目錄服務相關聯的網路介面、子網路和 VPCs。
- sns – 允許使用者列出並取得用於目錄監控的 SNS 主題和訂閱的相關資訊。
- organizations – 允許使用者描述 AWS Organizations 與目錄服務相關的帳戶和服務存取組態。

AWS 受管政策： AWSDirectoryServiceDataFullAccess

您可將 AWSDirectoryServiceDataFullAccess 政策連接到 IAM 身分。若要檢視此政策的完整許可，請參閱《 AWS 受管政策參考》中的 AWSDirectoryServiceDataFullAccess。

此政策會授予管理許可，允許委託人完整存取 Directory Service Data 操作。具有這些許可的主體可以在受管目錄中建立、更新和刪除 Active Directory 使用者和群組。他們可以管理群組成員資格、啟用或停用使用者，以及執行全面的使用者和群組管理操作。此政策專為需要以程式設計方式管理 Active Directory 物件的管理員而設計。

許可詳細資訊

此政策包含以下許可：

- ds – 允許主體透過 Directory Service Data API 存取目錄資料。
- ds-data – 允許主體完整存取所有 Directory Service Data 操作，包括建立、更新和刪除使用者和群組、管理群組成員資格，以及搜尋目錄物件。

AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess

您可將 AWSDirectoryServiceDataReadOnlyAccess 政策連接到 IAM 身分。若要檢視此政策的完整許可，請參閱《 AWS 受管政策參考》中的 AWSDirectoryServiceDataReadOnlyAccess。

此政策授予唯讀許可，允許使用者檢視和搜尋受管目錄中的 Active Directory 物件。附加此政策的主體無法對使用者、群組或群組成員資格進行任何更新。例如，具有這些許可的主體可以搜尋使用者和群組、檢視使用者和群組詳細資訊，以及列出群組成員資格，但無法建立、修改或刪除任何目錄物件。

許可詳細資訊

此政策包含以下許可：

- ds – 允許主體透過 Directory Service Data API 存取目錄資料。
- ds-data – 允許使用者執行唯讀動作，以傳回目錄物件資訊。這包括以 Describe、 List或 開頭的 API 操作Search。

AWSDirectoryServiceServiceRolePolicy

您無法將AWSDirectoryServiceServiceRolePolicy政策連接至 IAM 身分。此政策會連接到服務連結角色，允許 AWS Directory Service 代表您執行動作。若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 AWSDirectoryServiceServiceRolePolicy。

此政策授予許可，允許 AWS Directory Service 在混合式 Active Directory 環境中監控和評估自我管理的網域控制站。此服務使用這些許可來執行自動化運作狀態評估、執行 PowerShell 指令碼進行相容性測試，以及收集網路組態資訊，以確保適當的混合連線能力和自動化復原功能。

許可詳細資訊

此政策包含以下許可：

- ssm – 允許服務將 PowerShell 命令傳送至內部部署網域控制站，並擷取命令執行結果以進行監控和評估。
- ec2 – 允許服務描述網路資源，例如 VPCs、子網路、安全群組和網路介面，以驗證混合連線組態。

受管政策的 AWS IAM 和 AWS Directory Service 更新

檢視自服務開始追蹤這些變更以來，IAM 和 AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 IAM 和 AWS Directory Service 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AWSDirectoryServiceServiceRolePolicy – 新政策	AWS Directory Service 新增了新的政策， AWS 以允許 監控客戶的自我管理網域控制站。	2025 年 7 月 30 日
AWS 受管政策：AWSDirectoryServiceDataReadOnlyAccess – 新政策	AWS Directory Service 新增了新的政策，以允許使用者或群組存取檢視和搜尋 AD 使用者、成員和群組。	2024 年 9 月 17 日
AWS 受管政策： AWSDirectoryServiceDataFullAccess – 新政策	AWS Directory Service 新增了新的政策，以允許使用者或群組使用 Directory Service Data 存取內建物件管理，以建立、管理和檢視 AD 使用者、成員和群組。	2024 年 9 月 17 日
AWS Directory Service 開始追蹤變更	AWS Directory Service 已開始追蹤其 AWS 受管政策的變更。	2024 年 9 月 17 日

針對 使用身分型政策 (IAM 政策） AWS Directory Service

這個主題提供身分型政策範例，在該政策中帳戶管理員可以將許可政策連接至 IAM 身分 (使用者、群組和角色)。這些範例示範 中的 IAM 政策 AWS Directory Service。您應該修改和建立自己的政策，以符合您的需求和環境。

> **Important**
>
> 建議您先檢閱簡介主題，說明可用於管理 AWS Directory Service 資源存取的基本概念和選項。如需詳細資訊，請參閱管理 AWS Directory Service 資源存取許可的概觀。

本主題中的各節涵蓋下列內容：

- 使用 AWS Directory Service 主控台所需的許可
- AWS 的 受管 （預先定義） 政策 AWS Directory Service
- 客戶受管政策範例
- 搭配 IAM 政策使用標籤

以下顯示許可政策範例。

JSON

```
{
   "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDsEc2IamGetRole",
            "Effect": "Allow",
            "Action": [
                "ds:CreateDirectory",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcs",
                "ec2:CreateSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSubnets",
                "iam:GetRole"
            ],
            "Resource": "*"
        },
        {
            "Sid": "WarningAllowsCreatingRolesWithDirSvcPrefix",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:PutRolePolicy"
            ],
```

```
            "Resource": "arn:aws:iam::111122223333:role/DirSvc*"
        },
        {
            "Sid": "AllowPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/Your-Role-Name",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudwatch.amazonaws.com"
                }
            }
        }
    ]
}
```

政策中的三個陳述式授予許可，如下所示：

- 第一個陳述式會授予建立 AWS Directory Service 目錄的許可。由於 AWS Directory Service 不支援資源層級的許可，因此政策會指定萬用字元 (*) 做為`Resource`值。
- 第二個陳述式會授予存取 IAM 動作的許可，讓 AWS Directory Service 可以代表您讀取和建立 IAM 角色。`Resource` 值結尾的萬用字元 (*) 表示該陳述式允許對任何 IAM 角色執行動作的許可。若要限制此許可只提供給特定角色，請將資源 ARN 中的萬用字元 (*) 更換為特定角色的名稱。如需詳細資訊，請參閱 IAM 動作。
- 第三個陳述式會將許可授予 Amazon EC2 中允許 AWS Directory Service 建立、設定和銷毀其目錄所需的特定資源集。將角色 ARN 取代為您的角色。如需詳細資訊，請參閱 Amazon EC2 動作。

您不會在政策中看到`Principal`元素，因為在身分型政策中，您不會指定取得許可的委託人。當您將該政策連接至使用者時，這名使用者是隱含委託人。當您將許可政策連接至 IAM 角色，該角色的信任政策中所識別的主體即取得許可。

如需顯示所有 AWS Directory Service API 動作及其適用的資源的表格，請參閱 AWS Directory Service API 許可：動作、資源和條件參考。

使用 AWS Directory Service 主控台所需的許可

若要讓使用者使用 AWS Directory Service 主控台，該使用者必須擁有上述政策中列出的許可，或 Directory Service 完整存取角色或 Directory Service 唯讀角色授予的許可，如中所述AWS 的 受管（預先定義）政策 AWS Directory Service。

如果您建立比最基本必要許可更嚴格的 IAM 政策，則對於採取該 IAM 政策的使用者而言， 主控台就無法如預期運作。

AWS 的 受管 （預先定義） 政策 AWS Directory Service

AWS 提供由 建立和管理的預先定義或受管 IAM 政策，以解決許多常見的使用案例 AWS。受管政策會授予常見使用案例的必要許可，這可協助您決定所需的許可。如需詳細資訊，請參閱AWS 的 受管政策 AWS Directory Service。

客戶受管政策範例

在本節中，您可以找到授予各種 AWS Directory Service 動作許可的使用者政策範例。

> **Note**
>
> 所有範例皆使用美國西部 (奧勒岡) 區域 (us-west-2) 及虛構帳戶 ID。

範例

- 範例 1：允許使用者對任何 AWS Directory Service 資源執行任何描述動作
- 範例 2：允許使用者建立目錄

範例 1：允許使用者對任何 AWS Directory Service 資源執行任何描述動作

下列許可政策會將許可授予使用者，以執行 AWS Managed Microsoft AD Describe中開頭為 且目錄 ID 位於 d-1234567890中的所有 AWS 帳戶 動作111122223333。這些動作會顯示 AWS Directory Service 資源 (如目錄或快照) 的相關資訊。請務必將 AWS 區域 和 帳號變更為您要使用的區域和您的帳號。

JSON

```
{
"Version":"2012-10-17",
   "Statement":[
      {
"Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource": "arn:aws:ds:us-west-2:111122223333:directory/d-1234567890"
```

```
      }
   ]
}
```

範例 2：允許使用者建立目錄

下列許可政策會授予允許使用者建立目錄和所有其他相關資源 (如快照和信任) 的許可。若要授予該許可，還需要特定 Amazon EC2 服務的許可。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ds:CreateDirectory",
                "ds:DescribeDirectories"
            ],
            "Resource": "arn:aws:ds:*:111122223333:*"
        }
    ]
}
```

搭配 IAM 政策使用標籤

您可以在用於大多數 AWS Directory Service API 動作的 IAM 政策中套用標籤型資源層級許可。這可讓您更有效地控制使用者可以建立、修改或使用哪些資源。您可以使用 `Condition` 元素 (也稱為 `Condition` 區塊)，以及 IAM 政策中的以下條件內容金鑰和值，來根據資源標籤控制使用者存取 (許可)：

- 使用 `aws:ResourceTag/`**`tag-key`**`: `**`tag-value`** 以允許或拒絕資源上具有特定標籤的使用者動作。
- 使用 `aws:ResourceTag/`**`tag-key`**`: `**`tag-value`** 以在提出 API 請求時，要求使用 (或不使用) 特定標籤，以建立或修改允許標籤的資源。
- 使用 `aws:TagKeys: [`**`tag-key`**`, ...]` 以在提出 API 請求時，要求使用 (或不使用) 特定標籤金鑰集，以建立或修改允許標籤的資源。

> **Note**
>
> IAM 政策中的條件內容金鑰和值，只會套用到資源識別符可標記為必要參數的那些 AWS Directory Service 動作。

《IAM 使用者指南》中的使用標籤控制存取有如何使用標籤的其他資訊。該指南的 IAM JSON 政策參考章節有詳細的語法、說明，還有元素、變數範例，以及在 IAM 中的 JSON 政策評估邏輯。

下列標籤政策允許建立 AWS Directory Service 目錄，只要使用下列標籤：

- 環境：生產
- 擁有者：基礎設施團隊
- 成本中心：1234

JSON

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

```
            "Effect": "Allow",
            "Action": [
                "ds:CreateDirectory"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Environment": "Production",
                    "aws:RequestTag/Owner": "Infrastructure-Team",
                    "aws:RequestTag/CostCenter": "12345"
                }
            }
        }
    ]
}
```

下列標籤政策允許更新和刪除 AWS Directory Service 目錄，只要使用下列標籤：

- 專案：Atlas
- 部門：工程
- 環境：預備

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:DeleteDirectory",
                "ds:UpdateDirectory"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Project": "Atlas",
                    "aws:ResourceTag/Department": "Engineering",
                    "aws:ResourceTag/Environment": "Staging"
                }
```

```
            }
        }
    ]
}
```

下列標籤政策拒絕資源具有下列其中一個標籤 AWS Directory Service 的資源標記：

- 生產
- 安全
- 機密

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ds:AddTagsToResource"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": ["Production", "Security", "Confidential"]
                }
            }
        }
    ]
}
```

如需 ARNs 的詳細資訊，請參閱 Amazon Resource Name (ARNs) AWS 和服務命名空間。

下列 AWS Directory Service API 操作清單支援標籤型資源層級許可：

- AcceptSharedDirectory
- AddIpRoutes
- AddTagsToResource

- CancelSchemaExtension
- CreateAlias
- CreateComputer
- CreateConditionalForwarder
- CreateSnapshot
- CreateLogSubscription
- CreateTrust
- DeleteConditionalForwarder
- DeleteDirectory
- DeleteLogSubscription
- DeleteSnapshot
- DeleteTrust
- DeregisterEventTopic
- DescribeConditionalForwarders
- DescribeDomainControllers
- DescribeEventTopics
- DescribeSharedDirectories
- DescribeSnapshots
- DescribeTrusts
- DisableRadius
- DisableSso
- EnableRadius
- EnableSso
- GetSnapshotLimits
- ListIpRoutes
- ListSchemaExtensions
- ListTagsForResource
- RegisterEventTopic
- RejectSharedDirectory
- RemoveIpRoutes

- RemoveTagsFromResource
- ResetUserPassword
- RestoreFromSnapshot
- ShareDirectory
- StartSchemaExtension
- UnshareDirectory
- UpdateConditionalForwarder
- UpdateNumberOfDomainControllers
- UpdateRadius
- UpdateTrust
- VerifyTrust

AWS Directory Service API 許可：動作、資源和條件參考

當您在設定 存取控制 並撰寫可連接到 IAM 身分 (以身分為基礎的政策) 的許可政策時，可以使用 AWS Directory Service API 許可：動作、資源和條件參考 資料表作為參考。中的每個 API 項目包含以下內容：

- 每個 API 操作的名稱
- 每個 API 操作的對應動作或動作，您可以在其中授予執行動作的許可
- 您可以在其中授予許可 AWS 的資源

您要在政策的 `Action` 欄位中指定動作，並在政策的 `Resource` 欄位中指定資源值。若要指定動作，請使用後接 API 操作名稱的 `ds:` 字首 (例如，`ds:CreateDirectory`)。有些 AWS 應用程式可能需要在其政策`ds:UnauthorizeApplication`中使用非公有 AWS Directory Service API 操作，例如 `ds:AuthorizeApplication`、`ds:CheckAlias`、`ds:UpdateAuthorizedApplication`、、`ds:CreateIdentityPoolDirectory` `ds:GetAuthorizedApplicationDetails`和 。

有些 AWS Directory Service APIs只能透過 呼叫 AWS Management Console。它們不是公有 APIs，因此無法以程式設計方式呼叫，而且不是由任何 SDK 提供。他們接受使用者登入資料。這些 API 操作包括 `ds:DisableRoleAccess`、 `ds:EnableRoleAccess`和 `ds:UpdateDirectory`。

您可以在 AWS Directory Service 和 Directory Service Data 政策中使用 AWS 全域條件金鑰來表達條件。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。

AWS Directory Service 動作的 API 和必要許可

AWS Directory Service Data API 和動作的必要許可

> **Note**
>
> 若要指定動作，請使用 `ds-data:` 字首，後面接著 API 操作的名稱（例如，`ds-data:AddGroupMember`）。

Directory Service Data API 操作	所需許可 (API 動作)	資源
AddGroupMember	`ds-data:AddGroupMember`	*
CreateGroup	`ds-data:CreateGroup`	*
CreateUser	`ds-data:CreateUser`	*
DeleteGroup	`ds-data:DeleteGroup`	*
DeleteUser	`ds-data:DeleteUser`	*
DescribeGroup	`ds-data:DescribeGroup`	*
DescribeUser	`ds-data:DescribeUser`	*
DisableUser	`ds-data:DisableUser`	*
ListGroups	`ds-data:ListGroups`	*
ListGroupMembers	`ds-data:ListGroupMembers`	*
ListGroupsForMember	`ds-data:ListGroups ForMember`	*
ListUsers	`ds-data:ListUsers`	*
RemoveGroupMember	`ds-data:RemoveGroupMember`	*
SearchGroups	`ds-data:DescribeGroup`	*

Directory Service Data API 操作	所需許可 (API 動作)	資源
	ds-data:SearchGroups	
SearchUsers	ds-data:DescribeUser ds-data:SearchUsers	*
UpdateGroup	ds-data:UpdateGroup	*
UpdateUser	ds-data:UpdateUser	*

相關主題

- 存取控制

Directory Service Data 條件索引鍵

使用 Directory Service Data 條件索引鍵，將特定陳述式新增至使用者和群組層級存取。這可讓使用者決定哪些委託人可以對哪些資源以及在哪些條件下執行動作。

Condition 元素或 Condition 區塊可讓您指定陳述式生效的條件。Condition 元素是可選用的。您可以建立使用條件運算子的條件式表達式，例如等於 (=) 或小於 (<)，以比對政策中的條件與請求中的值。

如果您在陳述式中指定多個條件元素，或在單一條件元素中指定多個索引鍵， 會使用邏輯 AND 操作 AWS 來評估它們。如果您為單一條件索引鍵指定多個值， 會使用邏輯 OR 操作 AWS 來評估條件。必須符合所有條件，才會授與陳述式的許可。您也可以在指定條件時使用預留位置變數。例如，您可以授予 IAM 使用者存取資源的許可，前提是該資源已加上使用者名稱的標籤。如需詳細資訊，請參閱《IAM 使用者指南》中的具有多個索引鍵或值的條件。

如需支援這些條件金鑰的動作清單，請參閱《服務授權參考》中的 AWS Directory Service Data 定義的動作。

> **Note**
>
> 如需標籤型資源層級許可的詳細資訊，請參閱 搭配 IAM 政策使用標籤。

ds-data：SAMAccountName

適用於字串運算子。

檢查具有指定 的政策SAMAccountName是否符合請求中使用的輸入。每個請求只能提供單一 SAM 帳戶名稱。

> **Note**
>
> 此條件索引鍵不區分大小寫。無論字母大小寫為何，您都必須使用 StringEqualsIgnoreCase或 StringNotEqualsIgnoreCase條件運算子來比較字串值。

允許使用者或群組搜尋 AD 物件

下列政策允許使用者jstiles或任何 成員test-group搜尋 AWS Managed Microsoft AD 網域中的使用者、成員和群組。

> **Important**
>
> 使用 SAMAccountName或 時MemberName，建議您指定 ds-data:Identifier為 SAMAccountName。這可防止 AWS Directory Service Data 支援的未來識別符，例如 SID中斷現有的許可。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SearchOnTrustedDomain",
      "Effect": "Allow",
      "Action": "ds-data:Search*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:SAMAccountName": [
            "jstiles",
```

```
            "test-group"
          ],
        "StringEqualsIgnoreCase": {
            "ds-data:identifier": [
              "SAMAccountName"
            ]
          }
        }
      }
    }
  ]
}
```

ds-data：Identifier

適用於字串運算子。

指定請求中使用的識別符類型。我們建議一律在識別符條件索引鍵SAMAccountName中指定 ，因此 Directory Service Data 中支援的任何未來識別符都不會破壞現有的許可。

> **Note**
>
> 目前， SAMAccountName是唯一允許的值。不過，未來可能會允許更多值。

允許使用者或群組依領域更新使用者

下列政策允許使用者jstiles或任何 成員test-group更新example-domain.com領域中的使用者資訊。識別符金鑰可確保 SAMAccountName是在請求內容中傳遞的 ID 類型。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateUsersonDomain",
      "Effect": "Allow",
      "Action": "ds-data:UpdateUser",
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "ds-data:SAMAccountName": [
            "jstiles",
            "test-group"
          ],
        "StringEquals": {
            "ds-data:Identifier": [
              "SAMAccountName"
            ],
        "StringEquals": {
              "ds-data:Realm": [
                "example-domain.com"
              ]
            }
          }
        }
      }
    ]
}
```

ds-data：MemberName

適用於字串運算子。

檢查具有指定 的政策MemberName是否符合請求中使用的成員名稱。

> **Note**
>
> 此條件索引鍵不區分大小寫。無論字母大小寫為何，您都必須使用 StringEqualsIgnoreCase或 StringNotEqualsIgnoreCase條件運算子來比較字串值。

允許成員新增至群組

如果新增至群組的 以 開頭，則下列政策允許使用者或角色將成員MemberName新增至指定目錄中的群組region-1。

> **Important**
>
> 使用 MemberName或 時SAMAccountName，建議您指定 ds-data:Identifier為 SAMAccountName。這可防止 Directory Service Data 支援的未來識別符，例如 SID中斷現有的許可。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateGroupsWithRegionalMembers",
      "Effect": "Allow",
      "Action": "ds-data:UpdateGroup",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:MemberName": [
            "region-1-*"
          ]
        }
      }
    }
  ]
}
```

ds-data：MemberRealm

適用於字串運算子。

檢查政策MemberRealm中的 是否符合請求中使用的成員領域。

> **Note**
>
> 此條件索引鍵不區分大小寫。無論字母大小寫為何，您都必須使用 StringEqualsIgnoreCase或 StringNotEqualsIgnoreCase條件運算子來比較字串值。

允許成員新增至領域中的群組

下列政策允許使用者或角色將成員新增至跨網域信任領域中的群組。

> **Note**
>
> 下列範例僅使用 ds-data:MemberName 內容金鑰。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateMembersInRealm",
      "Effect": "Allow",
      "Action": "ds-data:UpdateGroup",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:MemberRealm": [
            "region-1-*"
          ]
        }
      }
    }
  ]
}
```

ds-data：Realm

適用於字串運算子。

檢查政策Realm中的 是否符合請求中使用的領域。

> **Note**
>
> 此條件索引鍵不區分大小寫。無論字母大小寫為何，您都必須使用 StringEqualsIgnoreCase或 StringNotEqualsIgnoreCase條件運算子來比較字串值。

允許將群組新增至領域

下列政策允許使用者或角色在指定的領域中建立群組。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateGroupsInRealm",
      "Effect": "Allow",
      "Action": "ds-data:CreateGroup",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:Realm": [
            "example-domain.com"
          ]
        }
      }
    }
  ]
}
```

使用 AWS 的應用程式和服務授權 AWS Directory Service

本主題說明使用 和 AWS Directory Service AWS Directory Service Data AWS 的應用程式和服務授權

在 Active Directory 上授權 AWS 應用程式

AWS Directory Service 當您授權應用程式時， 會授予所選 AWS 應用程式的特定許可，以與您的 Active Directory 無縫整合。 AWS 應用程式只會獲得其特定使用案例所需的存取權。以下是授權後授予應用程式和應用程式管理員的一組內部許可：

> **Note**
>
> 需要 `ds:AuthorizationApplication`許可才能授權 Active Directory 的新 AWS 應用程式。僅應向設定目錄服務整合的管理員提供此動作的許可。

- 在 AWS Managed Microsoft AD、Simple AD、AD Connector 目錄的所有組織單位 (OU)，以及 AWS Managed Microsoft AD 的受信任網域中，對 Active Directory 使用者、群組、組織單位、電腦或認證授權單位資料的讀取存取權。
- 對 AWS Managed Microsoft AD 組織單位中使用者、群組、群組成員資格、電腦或憑證授權單位資料的寫入存取權。對 Simple AD 的所有 OU 具有的寫入權限。
- 所有目錄類型 Active Directory 使用者的驗證和工作階段管理。

Amazon RDS 和 Amazon FSx 等特定 AWS Managed Microsoft AD 應用程式透過直接網路連線與您的 Active Directory 整合。在這種情況下，目錄互動使用本機 Active Directory 協定，例如 LDAP 和 Kerberos。這些 AWS 應用程式的許可由應用程式授權期間在 AWS 預留組織單位 (OU) 中建立的目錄使用者帳戶控制，其中包括 DNS 管理和為應用程式建立的自訂 OU 的完整存取權。為了使用此帳戶，應用程式需要透過呼叫者憑證或 IAM 角色來取得 `ds:GetAuthorizedApplicationDetails` 動作的許可。

如需 AWS Directory Service API 許可的詳細資訊，請參閱 AWS Directory Service API 許可：動作、資源和條件參考。

如需為 AWS Managed Microsoft AD 啟用 AWS 應用程式和服務的詳細資訊，請參閱 從 AWS Managed Microsoft AD 存取 AWS 應用程式和服務。如需為 Simple AD 啟用 AWS 應用程式和服務的詳細資訊，請參閱 從 Simple AD 存取 AWS 應用程式和服務。如需啟用 AD Connector AWS 應用程式和服務的詳細資訊，請參閱 從 AD Connector 存取 AWS 應用程式和服務。

在 Active Directory 上取消授權 AWS 應用程式

需要 `ds:UnauthorizedApplication`許可才能移除 AWS 應用程式存取 Active Directory 的許可。遵循應用程式提供的程序來停用它。

AWS 具有 Directory Service Data 的應用程式授權

對於 AWS Managed Microsoft AD 目錄， Directory Service Data (ds-data) API 提供使用者和群組管理任務的程式設計存取權。 AWS 應用程式的授權模式與 Directory Service Data 的存取控制不同，這表示 Directory Service Data 動作的存取政策不會影響 AWS 應用程式的授權。拒絕存取 ds-data 中的目錄不會中斷 AWS 應用程式整合或 AWS 應用程式的使用案例。

為授權 AWS 應用程式的 AWS Managed Microsoft AD 目錄撰寫存取政策時，請注意使用者和群組功能可能可透過呼叫授權 AWS 的應用程式或目錄服務資料 API 來使用。Amazon WorkDocs、Amazon WorkMail、Amazon WorkSpaces、Amazon QuickSight 和 Amazon Chime 在其 APIs 中提供使用者和群組管理動作。使用 IAM 政策控制對 AWS 此應用程式功能的存取。

範例

下列程式碼片段顯示當 WorkDocs 和 Amazon WorkMail 等 AWS 應用程式在 目錄中獲得授權時，拒絕`DeleteUser`功能的錯誤正確方法。

不正確

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "ds-data:DeleteUser"
            ],
            "Resource": "*"
        }
    ]
}
```

正確

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "ds-data:DeleteUser",
                "workmail:DeleteUser",
                "workdocs:DeleteUser"
            ],
            "Resource": "*"
        }
    ]
}
```

使用 AWS Directory Service的服務連結角色

AWS Directory Service use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 的唯一 IAM 角色類型 AWS Directory Service。服務連結角色由 預先定義， AWS Directory Service 並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更 AWS Directory Service 輕鬆地設定，因為您不必手動新增必要的許可。 AWS Directory Service 會定義其服務連結角色的許可，除非另有定義，否則只能 AWS Directory Service 擔任其角色。定義的許可包含信任政策和許可政策，這些政策不能附接至任何其他 IAM 實體。

您必須先刪除角色的相關資源，才能刪除服務連結角色。這可防止您失去對 AWS Directory Service 資源的存取權，因為您不會不小心移除存取資源的許可。

關於支援服務連結角色的其他服務，如需相關資訊，請參閱搭配 IAM 使用的AWS 服務。

主題

- 的服務連結角色許可 AWS Directory Service
- 為 建立服務連結角色 AWS Directory Service
- 編輯 的服務連結角色 AWS Directory Service
- 刪除 的服務連結角色 AWS Directory Service
- AWS Directory Service 服務連結角色支援的區域

的服務連結角色許可 AWS Directory Service

AWS Directory Service 使用名為 AWSServiceRoleForDirectoryService 的服務連結角色 – 允許 AWS 監控客戶的自我管理網域控制站。

AWSServiceRoleForDirectoryService 服務連結角色信任下列服務擔任該角色：

- `ds.amazonaws.com`

名為 AWSDirectoryServiceServiceRolePolicy 的角色許可政策允許 對指定的資源 AWS Directory Service 完成下列動作。如需完整的政策許可，請參閱《 AWS 受管政策參考》中的 AWSDirectoryServiceServiceRolePolicy。

- ec2 – 允許 服務描述網路資源，例如 VPCs、子網路、安全群組和網路介面，以驗證混合連線組態：
  - `ec2:DescribeAvailabilityZones`

  - ec2:DescribeDhcpOptions
  - ec2:DescribeNetworkInterfaces
  - ec2:DescribeRouteTables
  - ec2:DescribeSecurityGroups
  - ec2:DescribeSubnets
  - ec2:DescribeVpcs
- ssm – 允許服務傳送和監控 PowerShell guilabel 至內部部署網域控制站，以用於監控和評估目的：
  - ssm:Sendguilabel
  - ssm:Listguilabels
  - ssm:GetguilabelInvocation
  - ssm:DescribeInstanceInformation
  - ssm:GetConnectionStatus

您必須設定許可，以允許您的使用者、群組或角色建立、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 建立服務連結角色 AWS Directory Service

您不需要手動建立一個服務連結角色。當您允許 在 AWS Management Console、 AWS CLI或 AWS API 中 AWS 監控客戶的自我管理網域控制站時， 會為您 AWS Directory Service 建立服務連結角色。如需此變更的詳細資訊，請參閱政策更新。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。此外，如果您在 2017 年 1 月 1 日之前使用 AWS Directory Service 服務，當服務連結角色開始支援時， 會在您的帳戶中 AWS Directory Service 建立 AWSServiceRoleForDirectoryService 角色。若要進一步了解，請參閱我的 中出現的新角色 AWS 帳戶。

編輯 的服務連結角色 AWS Directory Service

AWS Directory Service 不允許您編輯 AWSServiceRoleForDirectoryService 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」的編輯服務連結角色。

刪除 的服務連結角色 AWS Directory Service

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 如果 AWS Directory Service 服務在您嘗試刪除資源時正在使用角色，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 AWSServiceRoleForDirectoryService 使用 AWS Directory Service 的資源

- 若要刪除您的目錄，請參閱 刪除您的 AWS Managed Microsoft AD。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除 AWSServiceRoleForDirectoryService 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。

AWS Directory Service 服務連結角色支援的區域

AWS Directory Service 不支援在提供服務的每個區域中使用服務連結角色。不過， 只會 AWS Directory Service 在您可以選擇加入混合目錄 AWS 區域 的 中使用 AWSServiceRoleForDirectoryService 角色。

混合目錄選擇加入區域支援

區域名稱	區域身分	選擇加入支援
美國東部 (維吉尼亞北部)	us-east-1	是
美國東部 (俄亥俄)	us-east-2	是

區域名稱	區域身分	選擇加入支援
美國西部 (加利佛尼亞北部)	us-west-1	是
美國西部 (奧勒岡)	us-west-2	是
Europe (Stockholm)	eu-north-1	是
Middle East (Bahrain)	me-south-1	是
亞太區域 (孟買)	ap-south-1	是
歐洲 (巴黎)	eu-west-3	是
亞太區域 (雅加達)	ap-southeast-3	是
Africa (Cape Town)	af-south-1	是
歐洲 (愛爾蘭)	eu-west-1	是
中東 (阿拉伯聯合大公國)	me-central-1	是
歐洲 (法蘭克福)	eu-central-1	是
南美洲 (聖保羅)	sa-east-1	是
亞太區域 (香港)	ap-east-1	是
亞太區域 (海德拉巴)	ap-south-2	是
亞太區域 (首爾)	ap-northeast-2	是
亞太區域 (大阪)	ap-northeast-3	是
歐洲 (倫敦)	eu-west-2	是
亞太區域 (墨爾本)	ap-southeast-4	是
歐洲 (米蘭)	eu-south-1	是
亞太區域 (東京)	ap-northeast-1	是

區域名稱	區域身分	選擇加入支援
亞太區域 (新加坡)	ap-southeast-1	是
亞太區域 (雪梨)	ap-southeast-2	是
加拿大 (中部)	ca-central-1	是
歐洲 (西班牙)	eu-south-2	是
歐洲 (蘇黎世)	eu-central-2	是

在 中記錄和監控 AWS Directory Service

最佳實務是監控您的組織，以確保所做的變更都會記錄。這可協助您確保可以調查任何非預期的變更，也可以復原不需要的變更。 AWS Directory Service 目前支援下列兩項 AWS 服務，因此您可以監控組織及其內發生的活動。

- Amazon CloudWatch - 您可以使用 CloudWatch Events 搭配 AWS Managed Microsoft AD 目錄類型。如需詳細資訊，請參閱啟用 AWS Managed Microsoft AD 的 Amazon CloudWatch Logs 日誌轉送。此外，您可以使用 CloudWatch Metrics 來監控域控制站效能。如需詳細資訊，請參閱決定何時使用 CloudWatch 指標新增網域控制站。
- AWS CloudTrail
  - 您可以搭配所有 AWS Directory Service 目錄類型使用 CloudTrail。如需詳細資訊，請參閱使用 記錄 AWS Directory Service API 呼叫 AWS CloudTrail。
  - 您可以在 Directory Service Data API 中使用 CloudTrail 搭配 AWS Managed Microsoft AD。如需詳細資訊，請參閱使用 記錄 AWS 目錄服務資料 API 呼叫 AWS CloudTrail。

使用 記錄 AWS Directory Service API 呼叫 AWS CloudTrail

AWS Managed Microsoft AD API 已與 整合 AWS CloudTrail，此服務會擷取您 中由 AWS Managed Microsoft AD 發出或代表其發出的 API 呼叫， AWS 帳戶 並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。CloudTrail 會從 AWS Managed Microsoft AD 主控台以及對 AWS Managed Microsoft AD API 的程式碼呼叫擷取 APIs 呼叫。使用 CloudTrail 收集的資訊，您可以判斷向 AWS Managed Microsoft AD 提出的請求、提出請求的來源 IP 地址、提出請求的人員、提出請求的時間等。若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

AWS CloudTrail 中的受管 Microsoft AD 資訊

當您建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在 AWS Managed Microsoft AD 中發生時，該活動會與事件歷史記錄中的其他服務 AWS 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》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html。

若要持續記錄 中的事件 AWS 帳戶，包括 AWS Managed Microsoft AD 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，當您在主控台中建立線索時，線索會套用至所有 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 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，請參閱下列內容：

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

在您的 中啟用 CloudTrail 記錄時 AWS 帳戶，對 AWS Managed Microsoft AD 動作進行的所有 API 呼叫都會在日誌檔案中追蹤。 AWS 受管 Microsoft AD 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。CloudTrail 會記錄對 AWS Directory Service API 或 CLI 呼叫的所有呼叫。

每個日誌項目都會包含產生要求之人員的資訊。日誌中的使用者身分資訊可協助您判斷請求是使用根或 IAM 使用者登入資料、角色或聯合身分使用者的臨時安全登入 AWS 資料，還是由其他服務提出。如需詳細資訊，請參閱 CloudTrail 事件參考中的 userIdentity 欄位。

日誌檔案可存放於儲存貯體任意長時間，但您也可以定義 Amazon S3 生命週期規則，自動封存或刪除日誌檔案。預設情況下，將使用 Amazon S3 伺服器端加密 (SSE) 對日誌檔案進行加密。

若您想在日誌檔案一送達就快速採取動作，您可選擇在傳送新的日誌檔案時，讓 CloudTrail 發佈 Amazon SNS 通知。如需詳細資訊，請參閱「設定 Amazon SNS 通知」。

您也可以將來自多個 AWS 區域和 AWS 帳戶 的 AWS Managed Microsoft AD 日誌檔案彙總到單一 Amazon S3 儲存貯體。如需詳細資訊，請參閱「將 CloudTrail 日誌檔案彙整至單一 Amazon S3 儲存貯體」。

了解 AWS Managed Microsoft AD 日誌檔案項目

CloudTrail 日誌檔案可以包含一或多個日誌項目，其中每個項目是由多個 JSON 格式的事件組成。日誌項目代表任何來源提出的單一要求，並且包含所要求動作、任何參數、動作日期和時間等等的資訊。日誌項目不保證為任何特定順序；也就是說，它們不是公有 API 呼叫的排序堆疊追蹤。

像密碼、身分驗證字符、檔案評論及檔案內容這類敏感資訊是在日誌項目中修訂。

下列範例顯示 AWS Managed Microsoft AD 的 CloudTrail 日誌項目範例：

```
{
  "Records" : [
    {
      "eventVersion" : "1.02",
      "userIdentity" :
      {
        "type" : "IAMUser",
        "principalId" : "<user_id>",
        "arn" : "<user_arn>",
        "accountId" : "<account_id>",
        "accessKeyId" : "<access_key_id>",
        "userName" : "<username>"
      },
      "eventTime" : "<event_time>",
      "eventSource" : "ds.amazonaws.com",
      "eventName" : "CreateDirectory",
      "awsRegion" : "<region>",
      "sourceIPAddress" : "<IP_address>",
      "userAgent" : "<user_agent>",
      "requestParameters" :
      {
        "name" : "<name>",
        "shortName" : "<short_name>",
        "vpcSettings" :
        {
          "vpcId" : "<vpc_id>",
          "subnetIds" : [
            "<subnet_id_1>",
            "<subnet_id_2>"
          ]
        },
        "type" : "<size>",
        "setAsDefault" : <option>,
```

```
        "password" : "***OMITTED***"
      },
      "responseElements" :
      {
        "requestId" : "<request_id>",
        "directoryId" : "<directory_id>"
      },
      "requestID" : "<request_id>",
      "eventID" : "<event_id>",
      "eventType" : "AwsApiCall",
      "recipientAccountId" : "<account_id>"
    }
  ]
}
```

使用 記錄 AWS 目錄服務資料 API 呼叫 AWS CloudTrail

AWS Directory Service Data 與 整合 AWS CloudTrail，此服務提供由使用者、角色或 Directory Service Data 中的 AWS 服務所採取之動作的記錄。CloudTrail 會將 Directory Service Data 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 Directory Service Data 主控台的呼叫，以及對 Directory Service Data API 操作的程式碼呼叫。如果您建立線索，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Directory Service Data 的事件。您可以使用 CloudTrail 所收集的資訊，判斷對 Directory Service Data 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」。

CloudTrail 中的目錄服務資料資訊

當您建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。在 Directory Service Data 中發生支援的事件活動 （管理事件） 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、搜尋和下載過去 90 天的管理事件 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」。檢視事件歷史記錄無需付費。

若要持續記錄 中的事件 AWS 帳戶，包括 Directory Service Data 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。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 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，請參閱下列內容：

- 建立追蹤的概觀

- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有 Directory Service Data 動作，並記錄在 Directory Service Data API 參考中。例如，對 AddGroupMember、DescribeUser 和 SearchGroups 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

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：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

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

了解 Directory Service Data 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件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 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示示範 CreateUser 動作的 CloudTrail 日誌項目。

```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "1234567890abcdef0",
            "arn": "arn:aws:iam::111222333444:role/AdAdmin",
            "accountId": "111222333444",
            "userName": "AdAdmin"
```

```
          },
          "attributes": {
            "creationDate": "2023-05-30T18:22:38Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-05-30T19:17:03Z",
      "eventSource": "ds.amazonaws.com",
      "eventName": "CreateUser",
      "awsRegion": "ap-northeast-2",
      "sourceIPAddress": ": 10.24.34.0",
      "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.create-user",
      "requestParameters": {
        "directoryId": "d-1234567890",
        "sAMAccountName": "johnsmith",
        "clientToken": "example_token"
        "emailAddress": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "surname": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "otherAttributes": {
          "physicalDeliveryOfficeName": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "telephoneNumber": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "streetAddress": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "displayName": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "homePhone": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "postalCode": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "description": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          }
        },
```

```
        "clientToken": "createUserToken4"
      },
      "responseElements": {
        "directoryId": "d-1234567890",
        "sID": "S-1-5-21-1234567890-123456789-123456789-1234",
        "sAMAccountName": "johnsmith"
      },
      "additionalEventData": {
        "SID": "S-1-5-21-1234567890-123456789-123456789-1234"
      },
      "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
      "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
      "readOnly": false,
      "resources": [
        {
          "accountId": "111222333444",
          "type": "AWS::DirectoryService::MicrosoftAD",
          "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
      ],
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111222333444",
      "eventCategory": "Management",
      "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
      }
},
```

下列範例顯示示範 ListUsers 動作的 CloudTrail 日誌項目。

未建立或修改物件的動作會傳回 null 回應。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
```

```
            "sessionIssuer": {
                "type": "Role",
                "principalId": "1234567890abcdef0",
                "arn": "arn:aws:iam::111222333444:role/AdAdmin",
                "accountId": "111222333444",
                "userName": "AdAdmin"
            },
            "attributes": {
                "creationDate": "2023-05-30T18:22:38Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-30T18:22:52Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "ListUsers",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.list-users",
    "requestParameters": {
        "directoryId": "d-1234567890",
        "maxResults": 1
    },
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1244",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111222333444",
            "type": "AWS::DirectoryService::MicrosoftAD",
            "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
```

```
}
```

下列範例顯示示範 ListGroups 動作的 CloudTrail 日誌項目。

> **Note**
>
> NextToken 元素會從所有日誌項目中修訂。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "1234567890abcdef0",
                "arn": "arn:aws:iam::111222333444:role/AdAdmin",
                "accountId": "111222333444",
                "userName": "AdAdmin"
            },
            "attributes": {
                "creationDate": "2023-05-30T18:22:38Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-30T18:29:15Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "ListGroups",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
 command/ds-data.list-groups",
    "requestParameters": {
        "directoryId": "d-1234567890",
        "nextToken": "REDACTED",
        "maxResults": 1
```

```
    },
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111222333444",
            "type": "AWS::DirectoryService::MicrosoftAD",
            "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
}
```

例外狀況錯誤的日誌項目

下列範例顯示拒絕存取錯誤的 CloudTrail 日誌項目。如需此錯誤的協助，請參閱《IAM 使用者指南》中的對存取遭拒錯誤訊息進行故障診斷。

> **Note**
>
> 存取遭拒日誌不會顯示請求參數。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
```

```
            "sessionIssuer": {
                "type": "Role",
                "principalId": "1234567890abcdef0",
                "arn": "arn:aws:iam::111222333444:role/AdAdmin",
                "accountId": "111222333444",
                "userName": "AdAdmin"
            },
            "attributes": {
                "creationDate": "2023-05-31T23:25:49Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-31T23:38:18Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
 command/ds-data.create-user",
    "errorCode": "AccessDenied",
    "errorMessage": "User: arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-
role is not authorized to perform: ds-data:CreateUser on resource: arn:aws:ds:ap-
northeast-2:111222333444:directory/d-1234567890 because no identity-based policy allows
 the ds-data:CreateUser action",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111222333444",
            "type": "AWS::DirectoryService::MicrosoftAD",
            "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
```

```
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
}
```

下列範例顯示找不到資源錯誤的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "1234567890abcdef0",
                "arn": "arn:aws:iam::111222333444:role/AdAdmin",
                "accountId": "111222333444",
                "userName": "AdAdmin"
            },
            "attributes": {
                "creationDate": "2023-05-30T20:41:50Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-30T21:10:16Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "DescribeUser",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
 command/ds-data.describe-user",
    "errorCode": "ResourceNotFoundException",
    "errorMessage": "User not found in directory d-1234567890.",
    "requestParameters": {
        "directoryId": "d-1234567890",
        "sAMAccountName": "nonExistingUser",
        "otherAttributes": [
            "co",
            "givenName",
```

```
            "sn",
            "telephoneNumber"
        ]
    },
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111222333444",
            "type": "AWS::DirectoryService::MicrosoftAD",
            "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444"
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
}
```


的合規驗證 AWS Directory Service

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 AWS Compliance Programs。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源來協助合規：

- 安全合規與治理 - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- HIPAA 合格服務參考 – 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- AWS 合規資源 – 此工作手冊和指南集合可能適用於您的產業和位置。

- AWS 客戶合規指南 – 透過合規的角度了解共同責任模型。本指南摘要說明跨多個架構 （包括國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 保護 AWS 服務和映射指南至安全控制的最佳實務。
- 《AWS Config 開發人員指南》中的使用規則評估資源 – AWS Config 服務會評估資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub – 這 AWS 服務 可讓您全面檢視其中的安全狀態 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱「Security Hub 控制參考」。
- Amazon GuardDuty – 這會監控您的環境是否有可疑和惡意活動，以 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和業界標準的方式。

中的彈性 AWS Directory Service

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置的。 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。

除了 AWS 全球基礎設施之外， AWS Directory Service 還提供隨時手動擷取資料快照的功能，以協助支援您的資料彈性和備份需求。如需詳細資訊，請參閱使用快照還原 AWS Managed Microsoft AD。

中的基礎設施安全性 AWS Directory Service

作為受管服務， AWS Directory Service 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 已發佈的 API 呼叫， AWS Directory Service 透過網路存取 。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。

- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 產生臨時安全憑證來簽署請求。

預防跨服務混淆代理人

混淆代理人問題屬於安全性問題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在 中 AWS，跨服務模擬可能會導致混淆代理人問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況， AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

我們建議在資源政策中使用 aws:SourceArn和 aws:SourceAccount全域條件內容金鑰，以限制 AWS Directory Service Microsoft Active Directory 為資源提供另一項服務的許可。如果 aws:SourceArn 值不包含帳戶 ID (例如 Amazon S3 儲存貯體 ARN)，您必須使用這兩個全域條件內容金鑰來限制許可。如果同時使用這兩個全域條件內容金鑰，且 aws:SourceArn 值包含帳戶 ID，則在相同政策陳述式中使用 aws:SourceAccount 值和 aws:SourceArn 值中的帳戶時，必須使用相同的帳戶 ID。如果您想要僅允許一個資源與跨服務存取相關聯，則請使用 aws:SourceArn。如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，請使用 aws:SourceAccount。

對於下列範例，aws:SourceArn 的值必須是 CloudWatch 日誌群組。

防範混淆代理人問題最有效的方法，是使用 aws:SourceArn 全域條件內容金鑰，以及資源的完整 ARN。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用 aws:SourceArn 全域條件內容金鑰，同時使用萬用字元 (*) 表示 ARN 的未知部分。例如 arn:aws:*servicename*:*:*123456789012*:*。

下列範例顯示如何在 AWS Managed Microsoft AD 中使用 aws:SourceArn和 aws:SourceAccount全域條件內容金鑰，以防止混淆代理人問題。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {
```

```
            "Service": "ds.amazonaws.com"
        },
        "Action": [
            "logs:CreateLogStream",
            "logs:PutLogEvents"
        ],
        "Resource": [
        "arn:aws:logs:us-east-1:111122223333:log-group:/aws/
directoryservice/Log_Group_Name:*"
        ],
        "Condition": {
            "ArnLike": {
                "aws:SourceArn": "arn:aws:ds:us-
east-1:111122223333:directory/Directory_Name"
             },
            "StringEquals": {
                "aws:SourceAccount": "111122223333"
            }
        }
    }
}
```

對於下列範例，aws:SourceArn 的值必須是您帳戶中的 SNS 主題。例如，您可以使用arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f像是「ap-southeast-1」是您的區域、「123456789012」是您的客戶 ID，而「DirectoryMonitoring_d-966739499f」是您建立的 Amazon SNS 主題名稱。

防範混淆代理人問題最有效的方法，是使用 aws:SourceArn 全域條件內容金鑰，以及資源的完整 ARN。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用 aws:SourceArn 全域條件內容金鑰，同時使用萬用字元 (*) 表示 ARN 的未知部分。例如 arn:aws:*servicename*:*:*123456789012*:*。

下列範例顯示如何在 AWS Managed Microsoft AD 中使用 aws:SourceArn和 aws:SourceAccount全域條件內容金鑰，以防止混淆代理人問題。

JSON

```
{
    "Version": "2012-10-17",
```

```
    "Statement": {
        "Effect": "Allow",
        "Principal": {
            "Service": "ds.amazonaws.com"
        },
        "Action": [
            "SNS:GetTopicAttributes",
            "SNS:SetTopicAttributes",
            "SNS:AddPermission",
            "SNS:RemovePermission",
            "SNS:DeleteTopic",
            "SNS:Subscribe",
            "SNS:ListSubscriptionsByTopic",
            "SNS:Publish"
        ],
        "Resource": [
            "arn:aws:sns:us-east-1:111122223333:SNS_TOPIC_NAME"
        ],
        "Condition": {
            "ArnLike": {
                "aws:SourceArn": "arn:aws:ds:us-
east-1:111122223333:directory/EXTERNAL_DIRECTORY_ID"
            },
            "StringEquals": {
                "aws:SourceAccount": "111122223333"
            }
        }
    }
}
```

以下範例顯示了已委派主控台存取權限的角色的 IAM 信任政策。aws:SourceArn 的值必須是您帳戶中的目錄資源。如需詳細資訊，請參閱 定義的資源類型 AWS Directory Service。例如，您可以使用 arn:aws:ds:us-east-1:123456789012:directory/d-1234567890，其中 123456789012 是客戶 ID，d-1234567890 是目錄 ID。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
```

```
        "Principal": {
            "Service": "ds.amazonaws.com"
        },
        "Action": [
            "sts:AssumeRole"
        ],
        "Condition": {
            "ArnLike": {
                "aws:SourceArn": "arn:aws:ds:us-
east-1:111122223333:directory/YOUR_DIRECTORY_ID"
            },
            "StringEquals": {
                "aws:SourceAccount": "111122223333"
            }
        }
    }
}
```

AWS Directory Service 使用 的 API 和界面 Amazon VPC 端點 AWS PrivateLink

您可以使用 AWS PrivateLink 在 VPC 和 AWS Directory Service 和 Directory Service Data APIs之間建立私有連線。這可讓您像在 VPC 中一樣存取 AWS Directory Service 和 Directory Service Data APIs，無需使用網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線。Amazon VPC 中的執行個體不需要公有 IP 地址即可存取 AWS Directory Service 和 Directory Service Data APIs。

若要建立私有連線，您可以建立 AWS PrivateLink 支援的界面 Amazon VPC 端點。我們會在您為介面端點啟用的每個子網中建立端點網路介面。這些是申請者管理的網路介面，可做為目的地為 AWS Directory Service 和 AWS Directory Service Data 之流量的進入點。

如需詳細資訊，請參閱《 AWS PrivateLink 指南》中的AWS 服務 透過 存取 AWS PrivateLink 。

AWS Directory Service 和 Directory Service Data 的考量事項

使用 AWS Directory Service 和 Directory Service Data，您可以透過介面端點呼叫 API 動作。如需建立介面端點之前需要考量的先決條件的相關資訊，請參閱《 AWS PrivateLink 指南》中的AWS 服務 使用介面 Amazon VPC 端點存取 。

AWS Directory Service 和 Directory Service 資料可用性

AWS Directory Service 支援以下介面端點 AWS 區域：

- 美國東部 (維吉尼亞北部)
- AWS GovCloud （ 美國東部 ）
- AWS GovCloud （ 美國西部 ）

Directory Service Data 支援所有 AWS 區域 可用介面端點。如需支援 AWS 區域 AWS Directory Service 和 Directory Service Data 的資訊，請參閱 的區域可用性 AWS Directory Service。

為 AWS Directory Service 和 Directory Service Data 建立介面 Amazon VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 為 AWS Directory Service 和 Directory Service Data APIs 建立介面端點AWS CLI。

範例： AWS Directory Service

使用下列服務名稱建立 AWS Directory Service APIs的介面端點：

```
com.amazonaws.region.ds
```

範例：目錄服務資料

使用下列服務名稱建立 Directory Service Data APIs介面端點：

```
com.amazonaws.region.ds-data
```

如需建立介面端點的詳細資訊，請參閱《 AWS PrivateLink 指南》中的AWS 服務 使用介面 Amazon VPC 端點存取 。

為您的界面 Amazon VPC 端點建立 Amazon VPC 端點政策

端點政策是您連接到介面端點的 IAM 資源政策。

> **Note**
>
> 如果您未將端點政策連接至介面端點，會代表您 AWS PrivateLink 將預設端點政策連接至介面端點。如需詳細資訊，請參閱 AWS PrivateLink 概念。

端點政策會指定以下資訊：

- 可執行動作的委託人 (、IAM AWS 帳戶使用者和 IAM 角色)
- 可執行的動作
- 可以對其執行動作的資源

如需詳細資訊，請參閱「AWS PrivateLink 指南」中的使用端點政策控制對服務的存取。

您可以將自訂端點政策連接至介面端點，以控制從 Amazon VPC 對 APIs 的存取。

範例：適用於 AWS Directory Service API 動作的 Amazon VPC 端點政策

以下是自訂端點政策的範例。當您將此政策連接到介面端點時，它會授予所有資源上所有主體的所列 AWS Directory Service 動作的存取權。

將 *action-1*、 *action-2* 和 *action-3* 取代為您想要包含在政策中的 AWS Directory Service APIs 的必要許可。如需完整清單，請參閱AWS Directory Service API 許可：動作、資源和條件參考。

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds:action-1",
            "ds:action-2",
            "ds:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

範例： Directory Service Data API 動作的 Amazon VPC 端點政策

以下是自訂端點政策的範例。當您將此政策連接到介面端點時，它會授予所有資源上所有主體的列出 Directory Service Data 動作的存取權。

將 *action-1*、 *action-2* 和 *action-3* 取代為您要包含在政策中的 Directory Service Data APIs 的必要許可。如需完整清單，請參閱AWS Directory Service API 許可：動作、資源和條件參考。

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds-data:action-1",
            "ds-data:action-2",
            "ds-data:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

的服務層級協議 AWS Directory Service

AWS Directory Service 是一項高可用性服務，且建置在 AWS受管基礎設施上。它由定義我們服務可用性政策的服務層級 (SLA) 協議提供支援。

- SLA 適用於 AWS Managed Microsoft AD、AD Connector 和 Simple AD。
- SLA 會討論服務額度、SLA 排除項目，並定義「涵蓋目錄」、「每月運作時間百分比」和「請求」等詞彙。
- 如需詳細資訊，請參閱 AWS Directory Service服務水準協議。

的區域可用性 AWS Directory Service

下表列出目錄類型支援哪些區域特定端點。

區域名稱	區域	端點	通訊協定	AWS Manage Microso AD（標準版和企業版）	AWS Manage Microso AD（混合版本）	AD Connec	Simple AD
美國東部(維吉尼亞北部)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	是	是	是	是
美國東部(俄亥俄)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	是	是	是	否
美國西部(加利佛尼亞北部)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	是	是	是	否
美國西部(奧勒岡)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	是	是	是	是

區域名稱	區域	端點	通訊協定	AWS Manage Microso AD（標準版和企業版）	AWS Manage Microso AD（混合版本）	AD Connec	Simple AD
Africa (Cape Town)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	是	是	是	否
亞太區域(香港)	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	是	是	是	否
亞太區域（台北）	ap-east-2	ds.ap-east-2.amazonaws.com	HTTPS	是	否	是	否
亞太區域(海德拉巴)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	是	是	是	否
亞太區域(雅加達)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	是	是	是	否
亞太地區(馬來西亞)	ap-southeast-5	ds.ap-southeast-5.amazonaws.com	HTTPS	是	否	是	否

區域名稱	區域	端點	通訊協定	AWS Manage Microso AD（標準版和企業版）	AWS Manage Microso AD（混合版本）	AD Connec	Simple AD
亞太區域(墨爾本)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	是	是	是	否
亞太區域（泰國）	ap-southeast-7	ds.ap-southeast-7.amazonaws.com	HTTPS	是	否	是	否
亞太區域(孟買)	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	是	是	是	否
亞太區域(大阪)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	是	是	是	否
亞太區域(首爾)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	是	是	是	否
亞太區域(新加坡)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	是	是	是	是

區域名稱	區域	端點	通訊協定	AWS Manage Microso AD（標準版和企業版）	AWS Manage Microso AD（混合版本）	AD Connec	Simple AD
亞太區域 (雪梨)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	是	是	是	是
亞太區域 (東京)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	是	是	是	是
加拿大 (中部)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	是	是	是	否
加拿大西部 (卡加利)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	是	否	是	否
中國 (北京)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	是	否	是	否
中國 (寧夏)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	是	否	是	否

區域名稱	區域	端點	通訊協定	AWS Manage Microso AD（標準版和企業版）	AWS Manage Microso AD（混合版本）	AD Connec	Simple AD
歐洲(法蘭克福)	eu-centra l-1	ds.eu-central-1.amazonaws.com	HTTPS	是	是	是	否
歐洲(愛爾蘭)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	是	是	是	是
歐洲(倫敦)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	是	是	是	否
歐洲(米蘭)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	是	是	是	否
Europe (Paris)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	是	是	是	否
歐洲(西班牙)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	是	是	是	否

區域名稱	區域	端點	通訊協定	AWS Manage Microso AD（標準版和企業版）	AWS Manage Microso AD（混合版本）	AD Connec	Simple AD
Europe (Stockh m)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	是	是	是	否
歐洲 (蘇黎世)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	是	是	是	否
以色列 (特拉維夫)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	是	否	是	否
墨西哥（中部）	mx-central-1	ds.mx-central-1.amazonaws.com	HTTPS	是	否	是	否
Middle East (Bahrair	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	是	是	是	否

區域名稱	區域	端點	通訊協定	AWS Manage Microso AD（標準版和企業版）	AWS Manage Microso AD（混合版本）	AD Connec	Simple AD
中東 (阿拉伯聯合大公國)	me-centra l-1	ds.me-central-1.amazonaws.com	HTTPS	是	是	是	否
南美洲 (聖保羅)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	是	是	是	否
AWS GovClo（美國西部）	us-gov-we st-1	ds.us-gov-west-1.amazonaws.com	HTTPS	是	否	是	否
AWS GovClo（美國東部）	us-gov-east-1	ds.us-gov-east-1.amazonaws.com	HTTPS	是	否	是	否

如需有關 AWS Directory Service 在 AWS GovCloud（美國西部）區域和 AWS GovCloud（美國東部）區域中使用 的資訊，請參閱AWS GovCloud (US) 《使用者指南》中的服務端點。

如需 AWS Directory Service 在北京和寧夏區域使用 的詳細資訊，請參閱中國 Amazon Web Services 的端點和 ARNs 中的 AWS 中國入門。

如需有關 Directory Service Data 支援的 FIPS 端點的資訊，請參閱《 AWS 一般參考 參考指南》中的 Directory Service Data 端點和配額。

AWS 區域 支援 Directory Service Data

下表提供 Directory Service Data 依目錄類型支援的區域特定端點清單。

區域名稱	區域	端點	通訊協定	AWS Managed Microsoft AD	AD Connector	Simple AD
美國東部 (俄亥俄)	us-east-2	ds-data.us-east-2.amazonaws.com	HTTPS	是	否	否
美國東部 (維吉尼亞北部)	us-east-1	ds-data.us-east-1.amazonaws.com	HTTPS	是	否	否
美國西部 (加利佛尼亞北部)	us-west-1	ds-data.us-west-1.amazonaws.com	HTTPS	是	否	否
美國西部 (奧勒岡)	us-west-2	ds-data.us-west-2.amazonaws.com	HTTPS	是	否	否
亞太區域 (香港)	ap-east-1	ds-data.ap-east-1.amazonaws.com	HTTPS	是	否	否

區域名稱	區域	端點	通訊協定	AWS Managed Microsoft AD	AD Connector	Simple AD
亞太區域 (孟買)	ap-south-1	ds-data.ap-south-1.amazonaws.com	HTTPS	是	否	否
亞太區域 (大阪)	ap-northeast-3	ds-data.ap-northeast-3.amazonaws.com	HTTPS	是	否	否
亞太區域 (首爾)	ap-northeast-2	ds-data.ap-northeast-2.amazonaws.com	HTTPS	是	否	否
亞太區域 (新加坡)	ap-southeast-1	ds-data.ap-southeast-1.amazonaws.com	HTTPS	是	否	否
亞太區域 (雪梨)	ap-southeast-2	ds-data.ap-southeast-2.amazonaws.com	HTTPS	是	否	否
亞太區域 (東京)	ap-northeast-1	ds-data.ap-northeast-1.amazonaws.com	HTTPS	是	否	否
加拿大 (中部)	ca-central-1	ds-data.ca-central-1.amazonaws.com	HTTPS	是	否	否

區域名稱	區域	端點	通訊協定	AWS Managed Microsoft AD	AD Connector	Simple AD
歐洲 (法蘭克福)	eu-central-1	ds-data.eu-central-1.amazonaws.com	HTTPS	是	否	否
歐洲 (愛爾蘭)	eu-west-1	ds-data.eu-west-1.amazonaws.com	HTTPS	是	否	否
歐洲 (倫敦)	eu-west-2	ds-data.eu-west-2.amazonaws.com	HTTPS	是	否	否
Europe (Paris)	eu-west-3	ds-data.eu-west-3.amazonaws.com	HTTPS	是	否	否
Europe (Stockholm)	eu-north-1	ds-data.eu-north-1.amazonaws.com	HTTPS	是	否	否
南美洲 (聖保羅)	sa-east-1	ds-data.sa-east-1.amazonaws.com	HTTPS	是	否	否

如需有關 Directory Service Data 支援的 FIPS 端點的資訊，請參閱《 AWS 一般參考 參考指南》中的 Directory Service Data 端點和配額。

的瀏覽器相容性 AWS Directory Service

AWS WorkSpaces、Amazon WorkMail、Amazon Connect、Amazon Chime、WorkDocs 等應用程式和服務 AWS IAM Identity Center 都需要相容瀏覽器的有效登入憑證，才能存取它們。下表僅會說明可供登入的相容瀏覽器與瀏覽器版本。

瀏覽器	版本	相容性
Microsoft Edge	最新的 3 個版本	相容
Mozilla Firefox	最新的 3 個版本	相容
Google Chrome	最新的 3 個版本	相容
Apple Safari	最新的 3 個版本	相容

現在您已驗證您使用的是支援的瀏覽器版本，我們建議您也檢閱以下章節，以確認您的瀏覽器已設定為使用 所需的 Transport Layer Security (TLS) 設定 AWS。

什麼是 TLS？

TLS 是一種通訊協定，可讓 Web 瀏覽器和其他應用程式用來在網路上安全地交換資料。TLS 會透過加密和端點身分驗證機制來確保遠端連線至預期的端點。最新的 TLS 版本為 TLS 1.0、1.1、1.2 和 1.3。

IAM Identity Center 支援哪些 TLS 版本

AWS 應用程式和服務支援 TLS 1.1、1.2 和 1.3 進行安全登入。自 2019 年 10 月 30 日起，TLS 1.0 已不再受支援，因此所有瀏覽器必須全設定為支援 TLS 1.1 或更新版本。這表示在啟用 TLS 1.0 的情況下，您將無法登入存取 AWS 應用程式與服務。如需協助進行此變更，請聯絡您的管理員。

在瀏覽器中啟用受支援 TLS 版本的方法

這取決於您的瀏覽器。通常，您可以在瀏覽器設定的進階設定區域下找到這個設定。例如，在 Internet Explorer 中，您可以在網際網路屬性、進階索引標籤，以及安全性區段下找到各種 TLS 選項。如需特定指示，請參閱您的瀏覽器製造商說明網站。

文件歷史紀錄

下表說明 AWS Directory Service 管理員指南自上次發行後的重要變更。

變更	描述	日期
新的 AWS 服務連結角色	AWS Directory Service 新增 AWS 服務連結角色，AWSServiceRoleForDirectoryService以及 AWS 受管政策 AWSDirectoryServiceServiceRolePolicy。政策允許 AWS 監控客戶受管網域控制站。	2025 年 7 月 30 日
AWS Managed Microsoft AD（混合版本）	AWS Managed Microsoft AD（混合版本）會將自我管理的 Active Directory 與 AWS Directory Service for Microsoft Active Directory 連線，建立跨越基礎設施和 的整合身分環境 AWS 雲端。	2025 年 7 月 30 日
更新記錄和監控主題 - 新章節	在記錄和監控主題中包含 AWS Directory Service 和 AWS Directory Service Data 的區段。	2024 年 9 月 18 日
新目錄服務資料 API 和屬性	AWS Directory Service Data 提供內建的物件管理。您現在可以使用支援的 AD 屬性清單來尋找和更新物件。	2024 年 9 月 18 日
AWS 受管政策 - 新政策	AWS Directory Service Data 新增了新的 AWS 受管政策：AWSDirectoryServiceDataFullAccess和 AWSDirectoryServiceDataReadOnlyAccess。這些	2024 年 9 月 18 日

	政策會授予 Directory Service Data 物件管理的存取權。	
以憑證為基礎的身分驗證設定	新增兩個 AWS Managed Microsoft AD 新安全設定的相關內容。	2023 年 4 月 11 日
AWS PrivateLink	新增有關 AWS PrivateLink的內容。	2023 年 3 月 31 日
Simple AD VPC 端點	新增有關不應設定哪些 VPC 端點的內容。	2021 年 8 月 25 日
AD Connector VPC 端點	新增有關不應設定哪些 VPC 端點的內容。	2021 年 8 月 25 日
智慧卡支援	新增有關 AWS GovCloud (美國西部) 區域支援智慧卡和 Amazon WorkSpaces Application Manager 的內容	2020 年 12 月 1 日
密碼重設	新增如何使用 AWS Management ConsolePowerShell和 重設使用者密碼的內容 AWS CLI。	2019 年 1 月 2 日
目錄共享	新增了有關如何將目錄共用與 AWS Managed Microsoft AD 搭配使用的內容。	2018 年 9 月 25 日
將內容遷移到新的《Amazon 雲端目錄開發人員指南》	將 Amazon 雲端目錄內容從本指南遷移到新的《Amazon 雲端目錄開發人員指南》。	2018 年 6 月 21 日
完成 Admin Guide TOC 全面檢查	重組內容以與更好地滿足客戶需求。還根據需要新增了內容。	2018 年 4 月 5 日

AWS 委派的群組	新增可指派給現場部署使用者的 AWS 委派群組清單。	2018 年 3 月 8 日
修整密碼政策細項	新增有關新密碼政策的內容。	2017 年 7 月 5 日
其他域控制站	新增有關如何向 AWS Managed Microsoft AD 中的目錄新增更多域控制站的內容。	2017 年 6 月 30 日
教學課程	新增測試 AWS Managed Microsoft AD 實驗室環境的新教學課程。	2017 年 6 月 21 日
MFA 搭配 AWS Managed Microsoft AD	新增有關搭配 AWS Managed Microsoft AD 使用 MFA 的內容。	2017 年 2 月 13 日
Amazon 雲端目錄	新增有關新目錄類型的內容。	2017 年 1 月 26 日
結構描述延伸	使用 AWS Directory Service for Microsoft Active Directory 新增有關結構描述延伸的內容。	2016 年 11 月 14 日
AWS Directory Service 管理員指南的主要重組	重組內容以與更好地滿足客戶需求。	2016 年 11 月 14 日
SNS 通知	新增有關 SNS 通知的內容。	2016 年 2 月 25 日
授權與身分驗證	新增了有關如何搭配 使用 IAM 的內容 AWS Directory Service。	2016 年 2 月 25 日
AWS Managed Microsoft AD	在單一指南中新增有關 AWS Managed Microsoft AD 和合併指南的內容。	2015 年 11 月 17 日
允許將 Linux 執行個體加入 Simple AD 目錄	新增如何將 Linux 執行個體加入 Simple AD 目錄的內容。	2015 年 7 月 23 日

指南拆分	將《AWS Directory Service 管理指南》拆分為多份單獨的指南。	2015 年 7 月 14 日
單一登入支援	新增有關單一登入支援的內容。	2015 年 3 月 31 日
新的指南	這是《AWS Directory Service 管理指南》的初版。	2014 年 10 月 21 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。