aws

管理指南

AWS Directory Service

版本 1.0

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Directory Service: 管理指南

Copyright © 2024 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？

AWS Directory Service 提供多種方式與其他 AWS 服務搭配使用 Microsoft Active Directory (AD)。目錄儲存使用者、群組和裝置的相關資訊，而管理員則使用這些目錄來管理資訊和資源的存取。 AWS Directory Service 為想要在雲端中使用現有 Microsoft AD 或輕量型目錄存取通訊協定 (LDAP) 感知應用程式的客戶提供多種目錄選擇。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。

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。請使用下表來協助您判斷哪個 AWS Directory Service 目錄選項最適合您的組織。

您需要執行什麼作業？	推薦 AWS Directory Service 選項
我需要為雲端應用程式使用 Active Directory 或 LDAP	如果您需要支援 Active Directory —aware 工作負載的實際MicrosoftActive Directory AWS 雲端或應用AWS 程式和服務 (例如 Amazon 和 Amazon WorkSpaces)，或者您需要 Linux AWS 應用程式的 LDAP 支援，請使用適用於 Microsoft Active Directory (標準版或企業版) 的 Directory Ser QuickSight vice。 如果您只需要允許內部部署使用者使用其Active Directory認證登入 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 Active Directory 相容應用程式的低規模、低成本的目錄，或者您需要 LDAP 感知應用程式的 LDAP 相容性，請使用 Simple AD。
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，請參閱如何在上選擇Active Directory解決方案 AWS。

AWS Directory Service 選項

AWS Directory Service 包括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

也被稱為 Microsoft AWS 託管 AD， AWS Directory Service 的 Microsoft 活動目錄是由一個實際的 Microsoft Windows ServerActive Directory（AD）供電， AWS 在 AWS 雲中管理。它可讓您將廣泛的使用中目錄感知應用程式遷移到雲端 AWS 。 AWS 受管理的 Microsoft AD 可與Microsoft SharePointMicrosoft SQL Server永遠在可用性群組和許多 .NET 應用程式搭配使用。它還支援 AWS 受管應用程式和服務 WorkSpaces，包括 Amazon WorkDocs QuickSight、Amazon、Amazon 編號、Amazon Connect 和 Amazon Relational Database Service 服務 Microsoft SQL Server（Amazon RDSSQL Server，Amazon RDS 和 PostgreSQL 的亞馬遜 RDS）。Oracle

AWS 當您為目錄啟用合規性時，受到美國 Health 保險可攜性與責任法案 (HIPAA) 或支付卡產業資料安全標準 (PCI DSS) 規範的 AWS 雲端應用程式獲得核准。

所有相容的應用程式都可以使用您存放在 AWS Managed Microsoft AD 中的使用者登入資料，或者您可以透過信任連線至現有 AD 基礎架構，並使用Active Directory執行中的現場部署或 EC2 Windows 上的認證。如果您將 EC2 執行個體加入 AWS 受管 Microsoft AD，您的使用者可以使用與存取現場部署網路中的工作負載相同的 Windows 單一登入 (SSO) 體驗來存取 AWS 雲端中的 Windows 工作負載。

AWS 受管理的 Microsoft AD 也支援使用Active Directory認證的同盟使用案例。單獨, Microsoft AWS 管理 AD 使您能夠登錄到 AWS Management Console. 透過 AWS IAM Identity Center，您也可以取得短期認證以搭配 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) 和選擇性的同Active Directory盟服務 (AD FS)，您可以使用儲存在 AWS 受管理 Microsoft AD 中的認證登入 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 受管理的 Microsoft AD 啟用多重要素驗證 (MFA)，以在使用者從網際網路存取 AWS 應用程式時提供額外的

安全性層級。由於Active Directory是 LDAP 目錄，因此您也可以使用 AWS Linux 安全殼層 (SSH) 驗證和其他啟用 LDAP 的應用程式使用 Microsoft AD。

AWS 提供監視、每日快照和復原作為服務的一部分 — 您可以將使用者和群組新增至 AWS 受管理的 Microsoft AD AD，並使用在加入受管理 Microsoft AD 網域的Windows電腦上執行的熟悉Active Directory工具來 AWS 管理群組原則。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 託管 Microsoft AD 有兩個版本：標準版和企業版。

- 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 如果您需要實際Active Directory功能來支援 AWS 應用程式或Windows工作負載 (包括適用於的 Amazon Relational Database Service)，受管 Microsoft AD 是您的最佳選擇Microsoft SQL Server。這也是最好的，如果你想要一個獨立Active Directory的 AWS 雲支持辦公室 365 或者你需要一個 LDAP 目錄來支持你的 Linux 應用程序。如需詳細資訊，請參閱 AWS 管理 Microsoft AD。

AD Connector

AD 連接器是一種代理服務，可讓您輕鬆將適用於Windows Server執行個體的相容 AWS 應用程式 (例如 Amazon WorkSpaces QuickSight、Amazon 和 Amazon EC2) 連接到現有的現場部署MicrosoftActive Directory。使用 AD Connector，您只需將一個服務帳戶添加到您的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 AWS 應用程式 (例如 Amazon) 時 QuickSight，AD Connector 會讀取您現有的，Active Directory以建立可供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 會將登入要求轉送至您的內部部署Active Directory網域控制站進行驗證。AD Connector 適用於許多 AWS 應用程序和服務 WorkDocs，包括 Amazon WorkSpaces QuickSight，Amazon，Amazon，Amazon Connect 和 Amazon WorkMail。您也可以使用無縫

Active Directory網域加入，透過 AD Connector 將 Windows EC2 執行個體加入現場部署網域。AD Connector 也可讓您的使用者使用現有的Active Directory認證登入，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 將應用程式使用者連接至現有的 Radius 型 MFA 基礎架構，為 AWS 應用程式使用者啟用多重要素驗證 (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Active Directory像現在一樣繼續管理您的。例如，您可以使用內部部署中的標準Active Directory管理工具新增使用者和群組，並更新密碼Active Directory。這可協助您持續強制執行安全性原則，例如密碼到期、密碼歷程記錄和帳戶鎖定，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 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 是一個MicrosoftActive Directory兼容的目錄 AWS Directory Service ，由 Samba 4 供電。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基於 EC2 執行個體、Kerberos 型 SSO 和群組政策。 AWS 作為服務的一部分，提供監控，每日快照和恢復。

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。您可以使用許多需要基本Active Directory功能的熟Active Directory悉應用程式和工具。Simple AD 與以下 AWS 應用程序兼容：Amazon WorkSpaces WorkDocs，Amazon QuickSight，Amazon 和 Amazon WorkMail。您也可以使用 Simple AD 使用者帳戶登入並管理 AWS 資源。 AWS Management Console

Simple AD 不支援多重要素驗證 (MFA)、信任關係、DNS 動態更新、結構描述擴充、透過 LDAPS 的通訊、 PowerShell AD 指令程式或 FSMO 角色傳輸。Simple AD 無法與 RDS SQL Server 相容。如果客戶需要實際功能 MicrosoftActive Directory，或想要使用目錄搭配 RDS SQL Server，則應改為使用 AWS 受管理的 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Windows需要基本Active Directory功能、相容 AWS 應用程式或支援需要 LDAP 服務的 Linux 工作負載的工作負載。如需詳細資訊，請參閱 簡易 AD。

Amazon Cognito

Amazon Cognito 是使用者目錄，可讓您使用 Amazon Cognito 使用者集區，為行動應用程式或 Web 應用程式新增登錄和登入。

使用情況

當您需要建立自訂登錄欄位，並將該中繼資料存放在您的使用者目錄中時，也可以使用 Amazon Cognito。這項全受管的服務可擴展，以支援數億名使用者。如需詳細資訊，請參閱《Amazon Cognito 開發人員指南》中的Amazon Cognito 使用者集區。

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 。

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 Windows 執行個體使用者指南》中的什麼是 Amazon EC2 一節。
- 《Amazon EC2 Windows 執行個體使用者指南》中的啟動 Amazon EC2 執行個體一節。
- 《Amazon EC2 Windows 執行個體使用者指南》中的安全群組一節。
- 《Amazon VPC 使用者指南》中的什麼是 Amazon VPC 一節。
- 《Amazon VPC 使用者指南》中的將硬體虛擬私有閘道新增到您的 VPC 一節。

開始使用 AWS Directory Service

如果您尚未這樣做，您還需要創建一個 AWS 帳戶並使用該 AWS Identity and Access Management 服務來控制訪問權限。

若要使用 AWS Directory Service，您必須符合 AWS Directory Service 的 Microsoft Active Directory、AD 連接器或 Simple AD 的先決條件。如需詳細資訊，請參閱「AWS 管理 Microsoft AD 先決條件」、「AD Connector 事前準備」或「Simple AD 先決條件」。

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為最佳安全實務，將管理存取權指派給管理使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立管理使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

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

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立管理使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，將管理權限授予管理使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以管理員的身分登入

- 若要使用您的 IAM 身分中心使用者登入，請使用建立 IAM 身分中心使用者時傳送至您電子郵件地址的登入 URL。

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

詳細資訊

- 如需如何以 IAM 身分中心使用者身分登入的詳細資訊，請參閱登入 IAM 身分中心存取入口網站。 AWS Management Console
- 如需如何以 IAM 使用者身分登入 AWS Management Console 的詳細資訊，請參閱以 IAM 使用者身分登入。 AWS Management Console
- 如需使用 IAM 政策控制資源存取權的詳細 AWS Directory Service 資訊，請參閱使用以身分為基礎的政策 (IAM 政策) AWS Directory Service。

AWS 管理 Microsoft AD

AWS Directory Service 可讓您以受管理服務的形式執行 Microsoft Active Directory (AD)。 AWS Directory Service Microsoft 活動目錄，也被稱為 AWS 管理 Microsoft AD，是由服務Windows器 2019 年供電。當您選取並啟動此目錄類型時，它會建立為連接到虛擬私有雲 (Amazon VPC) 的高可用性網域控制站組。這些域控制站會在您選擇區域的不同可用區域中執行。為您自動設定和管理主機監控與復原、資料複寫、快照和軟體更新。

使用 AWS 受管理的 Microsoft AD，您可以在 AWS 雲端中執行目錄感知工作負載，包括自訂以 .NET Microsoft SharePoint 和 SQL 伺服器為基礎的應用程式。您也可以設定 AWS 雲端中 AWS 受管理的 Microsoft AD 與現有內部部署之間的信任關係 MicrosoftActive Directory，讓使用者和群組能夠存取任一網域中的資源，使用 AWS IAM Identity Center。

AWS Directory Service 可讓您輕鬆在 AWS 雲端中設定和執行目錄，或將 AWS 資源與現有的內部部署連線MicrosoftActive Directory。目錄建立完成後，您可以使用它處理各種任務：

- 管理使用者和群組
- 提供應用程式和服務的單一登入
- 建立和套用群組政策
- 簡化雲端 Linux 和Microsoft Windows工作負載的部署和管理
- 您可以使用 AWS 受管理的 Microsoft AD 來啟用多因素驗證，方法是與您現有的 Radias 型 MFA 基礎結構整合，以便在使用者存取應用程式時提供額外的安全性層 AWS
- 安全地連接到 Amazon EC2 Linux 和Windows執行個體

> **Note**
>
> AWS 為您管理Windows伺服器執行個體的授權；您只需為使用的執行個體付費即可。另外，您無需購買額外的 Windows Server 用戶端存取授權 (CAL)，因為存取權限的費用已包含在價格中。每個執行個體都提供兩個遠端連線 (僅用於管理目的)。如果您需要兩個以上的連線，或者需要這些連線用於管理以外的目的，您可能需要在 AWS上增加額外的遠端桌面服務 CAL。

請閱讀本節中的主題，以開始建立 AWS 受管理的 Microsoft AD 目錄、在受 AWS 管理的 Microsoft AD 與您的內部部署目錄之間建立信任關係，以及擴充 AWS 受管理的 Microsoft AD 結構描述。

主題

- 開始使用 AWS 受管理 Microsoft AD
- AWS Managed Microsoft AD 重要概念
- AWS 管理 Microsoft AD 的使用案例
- 如何管理 AWS Managed Microsoft AD
- AWS 管理 Microsoft AD 的最佳做法
- AWS Managed Microsoft AD 配額
- AWS 管理 Microsoft AD 的應用程式相容性
- AWS Microsoft AD 測試實驗室託管教程
- 疑難排解 AWS 管理 Microsoft AD

AWS 安全性相關博客文章

- 如何將受管理的 Microsoft AD 目錄的 AWS 管理委派給您的內部部署作用中目錄使用者
- 如何使 AWS Directory Service 用 AWS 受管理的 Microsoft AD 來設定更強大的密碼原則，以協助符合您的安全性標準
- 如何透過新增網域控制站來提 AWS Directory Service 高 AWS 管理 Microsoft AD 的備援和效能
- 如何通過在託管 Microsoft AD 上部署 Microsoft 遠程桌面許可 AWS 管理器來啟用遠程桌面的使用
- 如何 AWS Management Console 使用 AWS 受管理的 Microsoft AD 和您的內部部署認證來存取
- 如何使用 AWS 受管理的 Microsoft AD 和內部部署認證為 AWS 服務啟用多重要素驗證
- 如何輕鬆地登入 AWS 服務，使用您的內部部署作用中目錄

開始使用 AWS 受管理 Microsoft AD

AWS 管理 Microsoft AD 在 AWS 雲中創建了一個完全託管的 Microsoft 活動目錄，並由 Windows 服務器 2019 年供電，並在 2012 R2 森林和域功能級別運行。當您使用 AWS 受管理的 Microsoft AD 建立目錄時， AWS Directory Service 會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 的不同子網路中建立的，此冗餘有助於確保即使發生故障，您的目錄仍可存取。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 部署其他網域控制器。

主題

- AWS 管理 Microsoft AD 先決條件
- 創建您的 AWS 託管 Microsoft AD Active Directory

- 什麼被創建與 AWS 管理 Microsoft AD 活動目錄
- 管理員帳戶的權限

AWS 管理 Microsoft AD 先決條件

要創建 AWS 託管 Microsoft ADActive Directory，您需要一個具有以下內容的 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。
- 您無法使用 198.18.0.0/15 位址空間中的位址在 VPC 中建立 AWS 受管理的 Microsoft AD。

如果您需要將 AWS 受管理的 Microsoft AD 網域與現有的內部部署Active Directory網域整合，您必須將內部部署網域的樹系和網域功能層級設定為 Windows Server 2003 或更新版本。

AWS Directory Service 使用兩個 VPC 結構。構成目錄的 EC2 執行個體在您的 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。

AWS IAM Identity Center 前提

如果您打算使用 IAM 身分中心搭配 AWS 受管理的 Microsoft AD，您必須確保下列條件成立：

- 您的 AWS 受管理 Microsoft AD 目錄是在您 AWS 組織的管理帳戶中設定的。
- 您的 IAM 身分識別中心執行個體位於設定 AWS 受管 Microsoft AD 目錄的相同區域。

如需詳細資訊，請參閱 AWS IAM Identity Center 使用指南中的 IAM 身分中心先決條件。

多重要素驗證先決條件

若要使用受 AWS 管理的 Microsoft AD 目錄支援多因素驗證，您必須以下列方式設定內部部署或雲端架構遠端驗證撥入使用者服務 (RADIUS) 伺服器，以便它可以接受來自中受 AWS 管理 Microsoft AD 目錄的要求。 AWS

1. 在 AWS RADIUS 伺服器上，建立兩個 RADIUS 用戶端來代表中的 AWS 管理 Microsoft AD 網域控制站 (DC)。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)：

- 位址 (DNS 或 IP)：這是其中一個 AWS 受管理的 Microsoft AD DC 的 DNS 位址。您可以在您計劃使用 MFA 之 AWS 受管理 Microsoft AD AWS 目錄的詳細資料頁面上的 Directory Service 主控台中找到這兩個 DNS 位址。顯示的 DNS 位址代表所 AWS使用之兩個受 AWS 管理 Microsoft AD DC 的 IP 位址。

  > **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 受管理的 Microsoft AD DC 和 RADIUS 伺服器之間的驗證通訊協定。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. 設定您現有的網路，以允許從 RADIUS 用戶端 (AWS 受管理 Microsoft AD DC DNS 位址，請參閱步驟 1) 到 RADIUS 伺服器連接埠的輸入流量。
3. 將規則新增至 AWS 受管 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 位址和連接埠號碼的輸入流量。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 搭配使用 AWS 受管理 Microsoft AD 的詳細資訊，請參閱為 AWS Managed Microsoft AD 啟用多重要素驗證。

創建您的 AWS 託管 Microsoft AD Active Directory

若要建立新的目錄，請執行以下步驟：開始此程序之前，請確定您已完成「AWS 管理 Microsoft AD 先決條件」中所示的必要條件。

建立 AWS 受管理的 Microsoft AD 目錄

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)

您可以選擇 AWS 管理 Microsoft AD 的標準版或企業版。如需版本的詳細資訊，請參閱 AWS Directory Service for Microsoft Active Directory。

目錄網域名稱系統 (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 路線 53 用於 DNS，則 AWS 受管 Microsoft AD 的域名必須與您的路由 53 域名不同。如果路由 53 和 AWS 管理 Microsoft AD 共用相同的網域名稱，則可能會發生 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。

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。

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。

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

   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)。

什麼被創建與 AWS 管理 Microsoft AD 活動目錄

當您使用 AWS 受管理的 Microsoft AD 建立作用中目錄時，請代表您 AWS Directory Service 執行下列工作：

- 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 ENI 中的每一個對於 VPC 和 AWS Directory Service 網域控制站之間的連線都是必不可少的，而且永遠不會刪除。您可以 AWS Directory Service 通過以下描述來識別所有保留用於的網絡接口：「為目錄目錄 ID AWS 創建的網絡接口」。如需詳細資訊，請參閱 Amazon EC2 Windows 執行個體使用者指南中的彈性網路界面。 AWS 管理 Microsoft AD 的預設 DNS 伺服器Active Directory是無類別網域間路由 (CIDR) +2 下的 VPC 擬私人雲端 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，網域控制站會部署在區域中的兩個可用區域，並連接到您的 Amazon VPC (VPC)。每天會自動執行一次備份，而 Amazon EBS (EBS) 磁碟區也會加密，以確保靜態資料受到保護。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。

- 在 VPC 中使用兩個網域控制器來佈建 Active Directory，以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 部署其他網域控制器。

> **Note**
>
> AWS 不允許在受管理的 Microsoft AD 網域控制站上安裝監視代 AWS 理程式。

- 建立 AWS 安全群組，藉此確立網路規則，來管理域控制站的出入流量。預設輸出規則允許所有流量 ENI 或連結至建立 AWS 安全群組的執行個體。預設的傳入規則僅允許通過 Active Directory 規定連接埠的流量 (來源不限) (0.0.0.0/0)。0.0.0.0/0 規則不會引入安全性弱點，因為網域控制站的流量僅限於來自 VPC、來自其他對等 VPC 或您使用 AWS Direct Connect、 AWS Transit Gateway 或虛擬私人網路連線的網路的流量。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，唯一可與您 AWS 受管理的 Microsoft AD 通訊的輸入流量是本機 VPC 和 VPC 路由流量。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 管理 Microsoft AD 的最佳做法。依預設會建立下列「 AWS 安全性群組」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	0.0.0.0/0	Ping	LDAP Keep Alive、DFS
TCP 和 UDP	53	0.0.0.0/0	DNS	使用者和電腦身分驗證、名稱解析、信任
TCP 和 UDP	88	0.0.0.0/0	Kerberos	使用者和電腦身分驗證、森林層級信任
TCP 和 UDP	389	0.0.0.0/0	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	0.0.0.0/0	SMB/CIFS	複寫、使用者和電腦身分驗證、群組政策、信任
TCP 和 UDP	464	0.0.0.0/0	Kerberos 更改/設定密碼	複寫、使用者和電腦身分驗證、信任
TCP	135	0.0.0.0/0	複寫	RPC、EPM
TCP	636	0.0.0.0/0	LDAP SSL	目錄、複寫、使用者和電腦身分驗證、群組政策、信任
TCP	1024-65535	0.0.0.0/0	RPC	複寫、使用者和電腦身分驗證、群組政策、信任
TCP	3268-3269	0.0.0.0/0	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	0.0.0.0/0	Windows 時間	Windows 時間、信任
UDP	138	0.0.0.0/0	DFSN & NetLogon	DFS、群組政策
全部	全部	sg-###### ############	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	sg-###### ############	所有流量	

- 如需 Active Directory 使用的連接埠和協定的詳細資訊，請參閱 Microsoft 文件中的 Windows 的服務概述和網路連接埠要求一文。
- 建立含有使用者名稱 Admin 與指定密碼的目錄管理員帳戶。此帳戶位於使用者 OU 下 (例如公司 > 使用者)。您可以使用此帳戶來管理您在 AWS 雲端中的目錄。如需詳細資訊，請參閱 管理員帳戶的權限。

> **Important**
>
> 請務必儲存此密碼。 AWS Directory Service 不儲存此密碼，也無法擷取密碼。不過，您可以從 AWS Directory Service 主控台或使用 ResetUserPasswordAPI 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 委派群組	儲存可用來委派 AWS 特定權限給使用者的所有群組。
AWS 已保留	儲存所有 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 屬於您的所有 AWS相關目錄物件， AWS 並且包含您已獲得「完全控制」的所有目錄物件。此 OU 下預設存在兩個子 OU：Computers (電腦) 和 Users (使用者)。例如： • 公司

OU 名稱	描述
	• 電腦 • 使用者

- 在 AWS 委派群組 OU 中建立下列群組：

Group name (群組名稱)	描述
AWS 委派帳戶運算子	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
AWS 委派作用中目錄啟動管理員	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 委派新增工作站至網域使用者	此安全群組的成員可以將 10 部電腦加入網域。
AWS 委派管理員	這個安全性群組的成員可以 AWS 管理受管理的 Microsoft AD、擁有 OU 中的所有物件的完整控制權，以及管理 AWS 委派群組 OU 中包含的群組。
AWS 允許委派驗證物件	這個安全性群組的成員可以對 AWS 保留的 OU 中的電腦資源進行驗證 (只有啟用了選擇性驗證信任的內部部署物件才需要)。
AWS 允許委派給網域控制站驗證	此安全性群組的成員可以對網域控制器 OU 中的電腦資源進行驗證 (只有已啟用選擇性身分驗證信任的內部部署物件才需要)。
AWS 委派刪除物件存留期管理	這個安全性群組的成員可以修改 msDS-DeletedObjectLifetime 物件，這會定義多久刪除的物件可以從 AD 資源回收筒復原。
AWS 委派分散式檔案系統管理	此安全群組的成員可以新增及移除 FRS、DFS-R 和 DFS 命名空間。

Group name (群組名稱)	描述
AWS 委派網域名稱系統管理員	此安全群組的成員可以管理與 DNS 整合的 Active Directory。
AWS 委派動態主機組態協定管理員	此安全群組的成員可以授權企業中的 Windows DHCP 伺服器。
AWS 委派的企業憑證授權單位	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。
AWS 委派的細緻密碼原則管理員	此安全群組的成員可以修改預先建立的微調密碼政策。
AWS 委派的 FSx 管理員	此安全群組的成員具備 Amazon FSx 資源的管理能力。
AWS 委派群組原則管理員	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 委派 Kerberos 委派系統管理員	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 委派受管理服務帳戶管理	此安全群組的成員可以建立及刪除受管服務帳戶。
AWS 委派的 MS-NPRC 不相容裝置	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 委派遠端存取服務管理員	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 委派複製目錄變更管理員	這個安全性群組的成員可以同步處理 Active Directory 中的設定檔資訊與 SharePoint 伺服器。
AWS 委派伺服器管理	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。

Group name (群組名稱)	描述
AWS 委派的網站和服務管理員	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 委派的系統管理員	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。
AWS 委派的終端機伺服器授權	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 委派使用者主要名稱尾碼管理	此安全群組的成員可以新增及移除使用者主體名稱尾碼。

- 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。這是通過設計，因為它們保留供 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
預設網域政策	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「AWS 委派伺服器管理員」新增為內建\ 系統管理員群組的成員。
AWS 保留政策:使用者	AWS 保留使用者帳戶	針對 AWS 保留的 OU 中的所有使用者帳戶設定建議的安全性設定。

群組政策名稱	適用對象	描述
AWS 受管理的使用中目錄	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。
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)。
預設網域控制站政策	未使用	在網域建立期間佈建， AWS 代替使用受管理的 Active Directory 原則。

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。

管理員帳戶的權限

當您為 Microsoft Active AWS Directory 目錄建立 Directory Service 時， AWS 會建立一個組織單位 (OU) 來儲存所有 AWS 相關的群組和帳戶。如需此 OU 的詳細資訊，請參閱「什麼被創建與 AWS 管理 Microsoft AD 活動目錄」。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 管理 AWS Managed Microsoft AD 中的使用者和群組。
- 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 受管 Microsoft AD 目錄加入權限。
- 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。
- 在活動目錄 Web 服務上運行活動目錄和 DNS Windows PowerShell 模塊。

- 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。

> **Important**
>
> AWS 網域管理員對於託管的所有網域具有完整的管理存取權 AWS。如需有關如何 AWS 處理儲存在 AWS 系統上之內容 (包括目錄資訊) 的詳細資訊，請參閱您的合約 AWS 和資AWS 料保護常見問題集。

> **Note**
>
> 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。

企業和域管理員特殊權限帳戶

AWS 每 90 天自動將內建的管理員密碼轉換為隨機密碼。任何時候要求內置的管理員密碼供人工使用時，都會創建一個 AWS 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，管理員帳戶憑證只能由 AWS Directory Service 管理團隊要求。

若要執行目錄的作業管理， AWS 具有企業系統管理員和網域系統管理員權限的帳戶的專屬控制權。這包括對活動目錄管理員帳戶的獨占控制。 AWS 通過使用密碼保險庫自動化密碼管理來保護此帳戶。在系統管理員密碼的自動輪換期間， AWS 會建立暫時使用者帳戶，並授與其網域管理員權限。此臨時帳戶是管理員帳戶密碼輪換失效時的備用方案。 AWS 成功旋轉管理員密碼後， AWS 刪除臨時管理員帳戶。

通常通過自動化完全 AWS 操作目錄。如果自動化程序無法解決操作問題， AWS 可能需要請支援工程師登入您的網域控制站 (DC) 以執行診斷。在這些罕見的情況下， AWS 實現請求/通知系統來授予訪問權限。在此程序中， AWS Automation 會在您的目錄中建立具有網域管理員權限的時間限制使用者帳戶。 AWS 將使用者帳戶與指派在您目錄上工作的工程師建立關聯。 AWS 在我們的日誌系統中記錄此關聯，並向工程師提供要使用的憑證。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 Security 事件轉寄至您的 CloudWatch系統，在此您可以實作監控解決方案。如需詳細資訊，請參閱 啟用日誌轉發。

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。您可以從加入域的 Windows 電腦使用事件檢視器 Microsoft Management Console (MMC) 檢視每個 DC 的 Windows 安全性事件日誌。您也可以啟用日誌轉發將所有安全事件日誌發送到您帳戶中的 CloudWatch 日誌。

您可能偶爾會看到在 AWS 保留的 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，以及我們未委派您存取和管理權限的任何其他 OU 或容器。您可能會看到該 OU 中的建立和刪除操作。這是因為 AWS Directory Service 使用自動化來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，在極少數情況下需要在 DC 上進行互動式存取以進行疑難排解，會建立一個暫時的使用者帳戶供 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，每次要求目錄的互動式認證時， AWS Directory Service 管理團隊都會收到通知。

AWS Managed Microsoft AD 重要概念

如果您熟悉以下重要概念，將更能充分利用 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。有些使用者類別屬性範例可以包含使用者的名字、姓氏、電話號碼等等。

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，您必須了解這些元素，再開始擴展 AWS Managed Microsoft AD 結構描述的程序。

屬性

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

- 延伸 AWS Managed Microsoft AD 結構描述的時機
- 教學課程：擴充 AWS 受管理的 Microsoft AD 架構

AWS Managed Microsoft AD 修補和維護

AWS Directory Service for Microsoft Active Directory (也稱為適用於 AWS Managed Microsoft AD 的 AWS DS) 實際上是以受管服務形式交付的 Microsoft Active Directory Domain Services (AD DS)。該系統會針對域控制站 (DC) 使用 Microsoft Windows Server 2019，而且 AWS 會將用於管理服務的軟體新增至 DC。AWS 會更新 (修補) DC 以新增功能，並確保 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 DC 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，我們建議部署額外的 DC。 AWS依序修補 DC，在此AWS期間，無法使用主動修補的 DC。如果一或多個 DC 暫時停止服務，AWS 會延遲修補，直到目錄中至少有兩個可運作的 DC。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

為了確保您 DC 上的 Microsoft Windows Server 軟體為最新版本，AWS 會利用 Microsoft Update。當 Microsoft 每月提供 Windows Server 的彙總套件修補程式時，AWS 會盡可能在三個行事曆週內測試彙總套件並套用至所有客戶的 DC。此外，根據 DC 的適用性與急迫性，AWS 會檢閱 Microsoft 在每月彙總套件以外發行的更新。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，您必須新增其帳戶做為 AWS 委派受管服務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 網站上的群組受管理服務帳戶概觀。

相關的 AWS 安全部落格文章

- AWS Managed Microsoft AD 如何協助簡化開發及提升 Active Directory 整合式 .NET 應用程式的安全

Kerberos 限制委派

Kerberos 限制委派是 Windows Server 功能。這項功能可讓服務管理員透過限制範圍來指定及強制執行應用程式信任邊界，其中應用程式服務可代表使用者執行動作。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 登入人力資源應用程式。您希望 SQL Server 套用 jsmith 的資料庫許可。不過，根據預設，SQL Server 會使用套用權限的服務帳戶認證來開啟資料庫連線，而不 hr-app-service 是 jsmith 的設定權限。您必須允許人力資源薪資應用程式使用 jsmith 的登入資料來存取 SQL Server 資料庫。若要這麼做，您可以在中為受AWS管理的 Microsoft AD 目錄上的 hr-app-service 服務帳戶啟用 Kerberos 限制委派。AWS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 Kerberos 票證，因此在開啟資料庫連線時套用 jsmith 特定的權限。

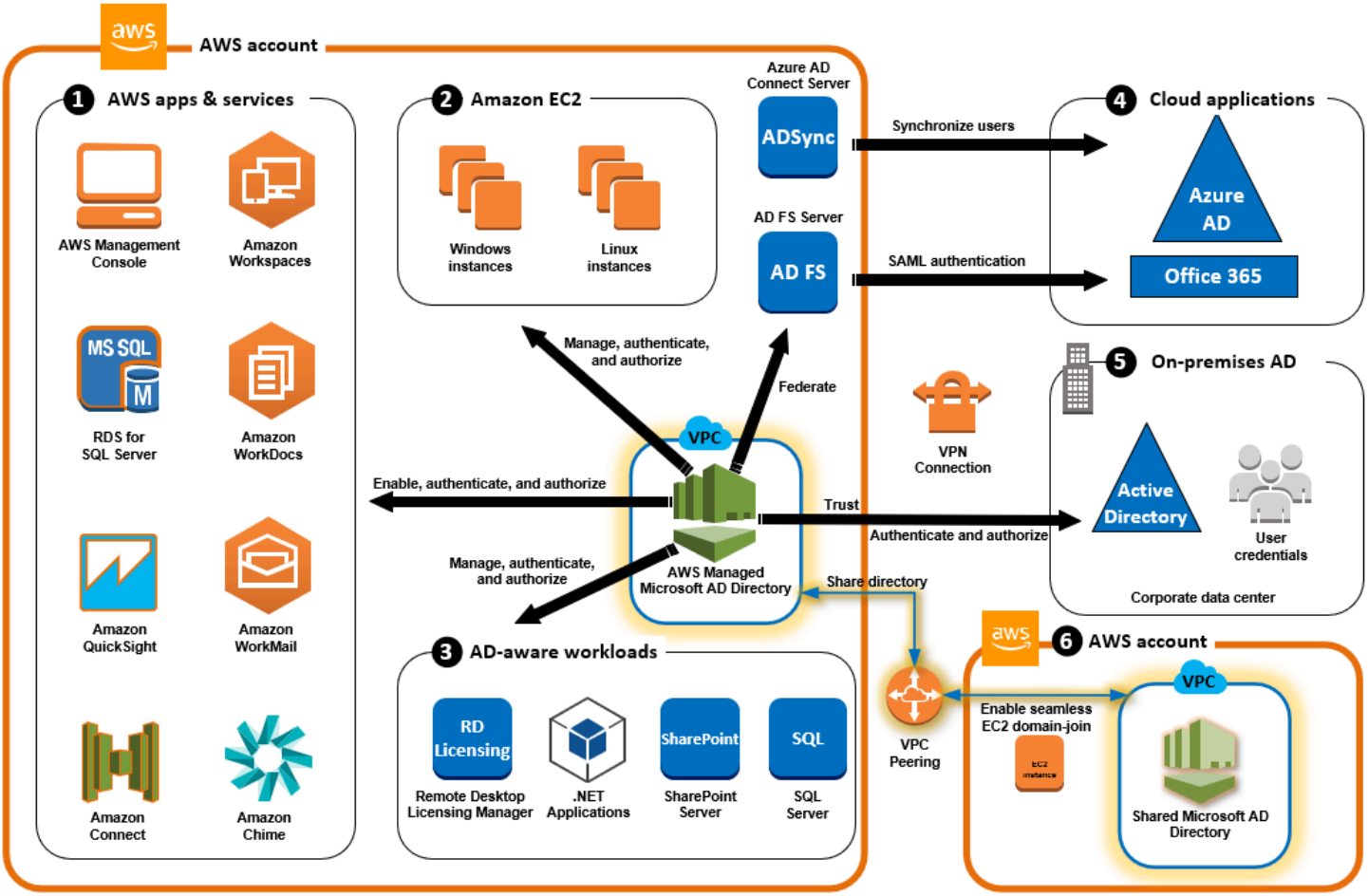
若要授予許可，讓 AWS Managed Microsoft AD 中的使用者可以設定 Kerberos 限制委派，您必須新增其帳戶做為 AWS 委派 Kerberos 委派管理員安全群組的成員。根據預設，管理帳戶是此群組的成員。如需有關 Kerberos 限制委派的詳細資訊，請參閱 Microsoft 網站上的 Kerberos 限制委派概觀。TechNet

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 管理 Microsoft AD 的使用案例

使用 AWS 受管理的 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。

下圖顯示您 AWS 受管理的 Microsoft AD 目錄的一些使用案例。其中包括授與使用者存取外部雲端應用程式的能力，以及允許內部部署 Active Directory 使用者管理和存取 AWS 雲端中的資源。



針對下列其中一個商務使用案例使用 AWS 受管理的 Microsoft AD。

主題

- 使用案例 1：使用作用中目錄認證登入 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：為您的作用中目錄感知工作負載提供目錄服務
- 使用案例 4： AWS IAM Identity Center 到辦公室 365 和其他雲端應用程式
- 使用案例 5：將您的內部部署作用中目錄延伸至 AWS 雲端
- 使用案例 6：共用您的目錄，以便跨 AWS 帳戶將 Amazon EC2 執行個體無縫加入網域

使用案例 1：使用作用中目錄認證登入 AWS 應用程式和服務

您可以啟用多個 AWS 應用程序和服務 AWS Client VPNAWS Management Console，如 AWS IAM Identity Center，，Amazon Chime，Amazon Connect，Amazon FSX，Amazon

QuickSight，AmazonRDS SQL 服務器，Amazon，亞馬遜 WorkDocs WorkMail，並WorkSpaces使用您 AWS 託管的 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 認證來存取應用程式或服務。

例如，您可以讓您的使用者使AWS Management Console 用其 Active Directory 認證登入。若要這麼做，您可以在目錄中啟用 AWS Management Console 作為應用程式，然後將 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，您可以啟用 Amazon 的單一登入功能 WorkDocs，讓您的使用者能夠 WorkDocs 從加入目錄的電腦存取 Amazon，而無需另外輸入其登入資料。

您可以授與目錄或內部部署 Active Directory 中 AWS CLI 使用者帳戶的存取權，以便他們可以登入 AWS Management Console 或透過現有的登入資料和權限來管理 AWS 資源，方法是直接將 IAM 角色指派給現有的使用者帳戶。

FSx FSx for Windows File Server 與 AWS 管理 Microsoft AD 整合

整合 FSx for Windows File Server 與 AWS 管理 Microsoft AD 提供完全受管理的原生 Microsoft 基於 Windows 的伺服器訊息區 (SMB) 通訊協定檔案系統，讓您輕鬆地將您的 Windows 應用程式和用戶端 (利用共用檔案儲存) 移至。 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 Windows 檔案伺服器與 AWS 受管理的 AD 使用案例整合之常見 FSx 資源的參考資源。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：

- 開始使用 AWS 受管理 Microsoft AD
- 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 支持

Amazon AppStream 2.0 是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 搭配 AppStream 2.0 提供使用 Amazon FSx 的個人永久性儲存磁碟機，並可設定為提供共用資料夾以存取常用檔案。

相關項目

- 逐步解說 4：使用 Amazon FSx 與 Amazon 2.0 AppStream
- 使用 Amazon FSx 與 Amazon 2.0 AppStream
- 使用活動目錄 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 可用於將 Active Directory 使用者主資料夾和「我的文件」中的資料儲存在一個集中位置。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
- 將 FSx 與 FSx for Windows File Server 搭配使用 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
- 將 FSx 與 FSx for Windows File Server 搭配使用 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

- How to use Group Policy to remotely install software in Windows Server 2008 and in Windows Server 2003

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 還支持 AWS 託管 Microsoft AD 目錄共享。如需詳細資訊，請參閱：

- 共享您的目錄
- 在不同的 VPC 或帳戶中搭配 AWS 託管 Microsoft AD 使用 Amazon FSx

Amazon RDS 與 AWS 託管 Microsoft AD 集成

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，您首先需要設定基本的 AWS 受管 Microsoft AD 和 Amazon RDS 組態。

- 開始使用 AWS 受管理 Microsoft AD
- Amazon RDS 入門

下面提到的所有使用案例都將從基礎 AWS 託管 Microsoft AD 和 Amazon RDS 開始，並介紹如何將 Amazon RDS 與 AWS 託管 Microsoft AD 集成。

- 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 還支持 AWS 託管 Microsoft AD 目錄共享。如需詳細資訊，請參閱：

- 共享您的目錄
- 在多個帳戶之間將 Amazon RDS 資料庫執行個體加入單一共用域

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 受管理 Microsoft AD 如何協助簡化部署，並改善作用中目錄 — 整合式 .NET 應用程式的安全性

使用案例 2：管理 Amazon EC2 執行個體

使用熟悉的使用中目錄管理工具，您可以套用使用中目錄群組原則物件 (GPO)，藉由將執行個體加入 AWS 受管 Microsoft AD 網域，以集中管理適用於 Windows 或 Linux 執行個體的 Amazon EC2。

此外，您的使用者可以使用其 Active Directory 認證登入您的執行個體。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。這使您可以更輕鬆地使用您已經使用的 Active Directory 用戶管理工具，立即授予或撤消對用戶的訪問權限。

使用案例 3：為您的作用中目錄感知工作負載提供目錄服務

AWS 託管 Microsoft AD 是一個實際的 Microsoft 活動目錄，使您能夠運行傳統的活動目錄感知工作負載，如遠程桌面許可管理器和 Microsoft SharePoint 和 Microsoft SQL 服務器始終在雲中 AWS 。AWS 受管理的 Microsoft AD 也可協助您使用群組受管理服務帳戶 (GMSA) 和 Kerberos 限制委派 (KCD) 來簡化及改善作用中目錄整合 .NET 應用程式的安全性。

使用案例 4： AWS IAM Identity Center 到辦公室 365 和其他雲端應用程式

您可以使用 AWS 受管理的 Microsoft AD 來提 AWS IAM Identity Center 供雲端應用程式。您可以使用 Microsoft Entra Connect (以前稱為Azure Active Directory Connect) 將使用者同步處理至 Microsoft Entra (先前稱為 Azure Active Directory (AzureAD))，然後使用使用中目錄同盟服務 (AD FS)，讓您的使用者可以使用其使用中目錄認證存取 Microsoft Office 365 和其他 SAML 2.0 雲端應用程式。

將AWS 受管 Microsoft AD 與身分識別中心整合，可將 SAML 功能新增至 AWS 受管理的 Microsoft AD 和/或您的內部部署信任網域。整合後，您的使用者就可以將 IAM 身分中心與支援 SAML 的服務搭配使用，包括 Office 365、Concur AWS Management Console 和 Salesforce 等第三方雲端應用程式，而無需設定 SAML 基礎結構。如需允許內部部署使用者使用 IAM 身分中心的程序示範，請參閱下列 YouTube 影片。

> **Note**
>
> AWS 單一登入已重新命名為 IAM 身分中心。

使用案例 5：將您的內部部署作用中目錄延伸至 AWS 雲端

如果您已經擁有 Active Directory 基礎結構，並且想要在將作用中目錄感知工作負載移轉至 AWS 雲端時使用該基礎結構，則 AWS 受管理的 Microsoft AD 可以提供協助。您可以使用活動目錄信任將

AWS 受管理的 Microsoft AD 連接到您現有的活動目錄。這表示您的使用者可以使用其內部部署 Active Directory 認證來存取使用中目錄感知和 AWS 應用程式，而不需要您同步處理使用者、群組或密碼。

例如，您的使用者可以使用其現有的 AWS Management Console Active Directory 使用者名稱和密碼登入和 Amazon WorkSpaces 。此外，當您使用作用中目錄感知應用程式 (例如 SharePoint Microsoft AWS 受管理 AD) 時，登入的 Windows 使用者可以存取這些應用程式，而不需要再次輸入認證。

您也可以移轉您的內部部署 Active Directory 網域， AWS 以免除使用中目錄移轉工具組 (ADMT) 與密碼匯出服務 (PES) 來執行移轉作用中目錄基礎結構的作業負擔。

使用案例 6：共用您的目錄，以便跨 AWS 帳戶將 Amazon EC2 執行個體無縫加入網域

跨多個 AWS 帳戶共用目錄可讓您輕鬆管理 Amazon EC2 等 AWS 服務，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。

當您與其他 AWS 帳戶共用 AWS 受管 Microsoft AD 目錄時，您可以使用 Amazon EC2 主控台，或AWS Systems Manager從帳戶和 AWS 區域內的任何 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。如需更多詳細資訊，請參閱 共享您的目錄。

如何管理 AWS Managed Microsoft AD

本節列出所有操作和維護 AWS Managed Microsoft AD 環境的程序。

主題

- 保護您的 AWS Managed Microsoft AD 目錄
- 監控您的 AWS Managed Microsoft AD
- 多區域複製
- 共享您的目錄
- 將 Amazon EC2 實例加入您的 AWS 受管 Microsoft AD 活動目錄
- 管理 AWS Managed Microsoft AD 中的使用者和群組
- Connect 到您現有的活動目錄基礎結構

- 擴展您的結構描述
- 維護您的 AWS 管理 Microsoft AD 目錄
- 授予 AWS 資源存取權給使用者與群組
- 啟用對應用 AWS 程式和服務的存取
- 啟用 AD 憑證存取 AWS Management Console
- 部署其他網域控制器
- 將使用者從 Active Directory 遷移到 AWS Managed Microsoft AD

保護您的 AWS Managed Microsoft AD 目錄

本節說明保護 AWS Managed Microsoft AD 環境的安全考量。

主題

- 管理 AWS 受管理 Microsoft AD 的密碼原則
- 為 AWS Managed Microsoft AD 啟用多重要素驗證
- 啟用安全的 LDAP 或 LDAP
- 管理 AWS Managed Microsoft AD 的合規性
- 增強您的 AWS Managed Microsoft AD 網路安全組態
- 設定目錄安全設定
- 設定 AD 的 AWS Private CA 連接器

管理 AWS 受管理 Microsoft AD 的密碼原則

AWS 受管理的 Microsoft AD 可讓您針對在受管理的 Microsoft AD 網域中管理的使用者群組，定義並指派不同的密碼和帳戶鎖定原則 (也稱為精細密碼原則)。 AWS 當您建立 AWS 受管理的 Microsoft AD 目錄時，會建立預設網域原則，並將其套用至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 *

政策	設定
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
使用可還原的加密來存放密碼	已停用

* 注意：42 天密碼最長使用期限包括管理員密碼。

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。

以下是深入瞭解MicrosoftActive Directory密碼原則和安全性原則的資源：

- 設定安全性原則設定
- 密碼複雜性需求
- 密碼複雜性安全考量

AWS 在 AWS 受管理的 Microsoft AD 中提供一組精細的密碼原則，您可以設定並指派給群組。若要設定原則，您可以使用標準Microsoft原則工具，例如Active Directory系統管理中心。若要開始使用Microsoft原則工具，請參閱安裝適用於 AWS 受管理 Microsoft AD 的活動目錄管理工具。

如何套用密碼原則

根據密碼重設還是已變更密碼，套用細緻密碼原則的方式會有所不同。網域使用者可以變更自己的密碼。具有必要權限的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

這些差異具有安全隱患。例如，每當重設使用者的密碼時，就不會強制執行密碼歷程記錄和密碼保留天數下限原則。如需詳細資訊，請參閱 Microsoft 說明文件，了解與強制執行密碼歷程記錄和最低密碼保留天數原則相關的安全

主題

- 支援的政策設定
- 委派可管理您密碼政策的人員
- 將密碼政策指派給您的使用者

相關 AWS 安全部落格文章

- 如何使 AWS Directory Service 用 AWS 受管理的 Microsoft AD 來設定更強大的密碼原則，以協助符合您的安全性標準

支援的政策設定

AWS 受管理的 Microsoft AD 包含五個具有不可編輯優先順序值的精細原則。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

下表列出 AWS 受管理 Microsoft AD 目錄中包含的五個原則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。如需有關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：精細密碼原則。如需這些原則的一般資訊，請參閱 Microsoft TechNet 網站上的密碼原則。

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

如需這些原則的一般資訊，請參閱 Microsoft TechNet 網站上的帳戶鎖定原則。

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：精細密碼原則。

委派可管理您密碼政策的人員

您可以將帳戶新增至委派的 F ine Vine 密碼原則系統管理員安全性群組，將管理密碼原則的權限AWS 委派給您在 AWS 受管理的 Microsoft AD 中建立的特定使用者帳戶。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. 從您加入受管 Microsoft AD 網域的任何受管 EC2 執行個體啟動使用中目錄 AWS 管理中心 (ADAC)。
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「什麼被創建與 AWS 管理 Microsoft AD 活動目錄」。
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。

將密碼政策指派給您的使用者

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. 從您加入受管 Microsoft AD 網域的任何受管 EC2 執行個體啟動使用中目錄 AWS 管理中心 (ADAC)。
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。
4. 若要確認密碼原則是否已套用，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 受管理的 Microsoft AD 目錄中設定五個密碼原則中的任何一個，Active Directory 會使用預設的網域群組原則。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。

為 AWS Managed Microsoft AD 啟用多重要素驗證

您可以在 AWS Managed Microsoft AD 目錄啟用多重要素驗證 (MFA)，以在使用者指定其 AD 憑證來存取 支援的 Amazon 企業應用程式 時，提升安全性。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 是一項業界標準的用戶端/伺服器協定，可提供身分驗證、授權與計量管理，讓使用者能夠連線到網路服務。AWSManaged Microsoft AD 包括連線到 RADIUS 伺服器的 RADIUS 用戶端，該伺服器上已實作您的 MFA 解決方案。您的 RADIUS 伺服器驗證使用者名稱和 OTP 代碼。如果您的 RADIUS 服務器成功驗證用戶，Microsoft AWS 管理 AD 然後對活動目錄的用戶進行身份驗證。成功驗證作用中目錄後，使用者就可以存取AWS應用程式。AWS Managed Microsoft AD RADIUS 用戶端和您的 RADIUS 伺服器之間的通訊，需要您設定 AWS 安全群組以啟用連接埠 1812 的通訊。

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。

> **Note**
>
> 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，請參閱為 AD Connector 啟用多重因素認證。

> **Note**
>
> MFA 是 AWS Managed Microsoft AD 的區域功能。如果您使用 多區域複製，則必須在每個區域中單獨執行以下程序。如需詳細資訊，請參閱全域與區域功能。

為 AWS Managed Microsoft AD 啟用多重要素驗證

1. 識別 RADIUS MFA 伺服器的 IP 地址和 AWS Managed Microsoft AD 目錄。
2. 編輯您的 Virtual Private Cloud (VPC) 安全群組，以在您的 AWS Managed Microsoft AD IP 終端節點和 RADIUS MFA 伺服器之間啟用連接埠 1812 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 Amazon 企業應用程式和服務 (例如 WorkSpaces Amazon 或亞馬 Amazon QuickSight Chime) 的存取權。AWS Management Console 它不提供 MFA 給 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，您必須使用執行 MFA 的解決方案， out-of-band 例如用戶的 SMS 文本驗證。在 out-of-band MFA 解決方案中，您必須確定針對您的解決方案適當地設定 RADIUS 逾時值。使用 out-of-band 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 AWS Directory Service 伺服器透過預設 RADIUS 伺服器連接埠 (UDP:1812) 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 。

支援的 Amazon 企業應用程式

所有 Amazon 企業 IT 應用程式 WorkSpaces，包括 Amazon WorkMail、Amazon QuickSight、Amazon 和訪問AWS IAM Identity Center和使用AWS管理 Microsoft AD 和 AD Connector 與 MFA 時AWS Management Console都受到支援。 WorkDocs

如需了解如何使用 AWS Directory Service 設定 Amazon 企業應用程式、AWS 單一登入和 AWS Management Console 的基本使用者存取，請參閱啟用對應用 AWS 程式和服務的存取和啟用 AD 憑證存取 AWS Management Console相關文章。

AWS 安全部落格相關的文章

- 如何使用 AWS Managed Microsoft AD 和內部部署憑證為 AWS 服務啟用多重要素驗證

啟用安全的 LDAP 或 LDAP

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。

為了減輕這種形式的資料暴露， AWS 管理 Microsoft AD 提供了一個選項：您可以啟用 LDAP 透過安全通訊端層 (SSL)/傳輸層安全性 (TLS)，也稱為 LDAPS。您可以使用 LDAPS 改善網路上的安全。您也可以加密已啟用 LDAP 的應用程式與 AWS 受管理的 Microsoft AD 之間的所有通訊，以符合法規要求。

AWS 受管理 Microsoft AD 在下列部署案例中提供 LDAPS 的支援：

- 伺服器端 LDAPS 會加密您的商業或本土開發的 LDAP 感知應用程式 (做為 LDAP 用戶端) 與 AWS 受管理的 Microsoft AD (充當 LDAP 伺服器) 之間的 LDAP 通訊。如需詳細資訊，請參閱 使用 AWS 管理 Microsoft AD 啟用伺服器端 LDAPS。
- 用戶端 LDAPS 會加密 AWS 應用程式之間的 LDAP 通訊，例如 WorkSpaces (做為 LDAP 用戶端) 和您的自我管理 (內部部署) 作用中目錄 (充當 LDAP 伺服器)。如需更多詳細資訊，請參閱 使用 AWS 管理 Microsoft AD 啟用用戶端 LDAPS。

主題

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

使用 AWS 管理 Microsoft AD 啟用伺服器端 LDAPS

伺服器端輕量型目錄存取通訊協定安全通訊端層 (SSL)/傳輸層安全性 (TLS) (LDAPS) 支援加密您的商業或本土開發的 LDAP 感知應用程式與受管理的 Microsoft AD 目錄之間的 LDAP 通訊。 AWS 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

如需如何設定及設定伺服器端 LDAPS 及憑證授權單位 (CA) 伺服器的詳細指示，請參閱 AWS 安全性部落格上如何為您的 AWS 受管理 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。下列步驟會引導您完成在 AWS 雲端中為網域啟用 LDAPS。

如果您想要使用自動化來設定 PKI 基礎結構，您可以使用 Microsoft 公開金鑰基礎結構 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**。如果您使用了 QuickStart 指南，則可以直接跳轉到步驟 3：建立憑證範本。

主題

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 受管理 Microsoft AD 目錄中的系統管理員或 AWS 委派企業憑證授權單位系統管理員群組的成員。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。在此情況下，請將該使用者新增至 AWS 受管理 Microsoft AD 目錄中的「系統管理員」或「 AWS 委派企業憑證授權單位系統管理員」

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。此憑證必須由加入您 AWS 受管理的 Microsoft AD 網域的 Microsoft 企業 CA 伺服器簽發。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**
>
> 伺服器端 LDAPS 與 AWS 受管理的 Microsoft AD 不支援由獨立 CA 所發行的憑證。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：

- 建立從屬 Microsoft 企業 CA — (建議使用) 使用此選項，您可以在雲端部署下屬的 Microsoft 企業 CA 伺服器。 AWS 伺服器可以使用 Amazon EC2，以便與您現有的根 Microsoft CA 使用。如需有關如何設定從屬 Microsoft 企業 CA 的詳細資訊，請參閱步驟 4：將 Microsoft 企業 CA 新增至您的 AWS Microsoft AD 目錄中如何啟用 AWS 受管理的 Microsoft AD 目錄中的伺服器端 LDAPS。
- 建立根 Microsoft 企業 CA — 使用此選項，您可以使用 Amazon EC2 在 AWS 雲端建立根 Microsoft 企業 CA，並將其加入您的 AWS 受管 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 的相關資訊，請參閱如何為您的 AWS 受管理 Microsoft AD 目錄啟用伺服器端 LDAPS 中的步驟 3：安裝及設定離線 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 實例加入您的 AWS 受管 Microsoft AD 活動目錄」。

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. 變更憑證接收者為 Windows 10 / Windows Server 2019。

      > **Note**
      >
      > AWS 託管 Microsoft AD 是由視窗服務器 2019 供電。

   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 的 AWS 安全性群組。
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] 旁邊的方塊中輸入目錄的 AWS 安全性群組 (例如，sg-123456789)。
   - 選擇儲存。
6. 現在，選擇您 AWS 管理的 Microsoft AD 目錄的 AWS 安全性群組。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] 旁邊的方塊中輸入 CA 的 AWS 安全性群組。
   - 選擇儲存。

您可以使用 LDP 工具測試與 AWS 管理 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 安裝適用於 AWS 受管理 Microsoft AD 的活動目錄管理工具。

> **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。

如需有關伺服器端 LDAPS 的其他詳細資訊，以及如何設定它的範例使用案例，請參閱 AWS 安全性部落格上的如何為您的 AWS 受管理 Microsoft AD 目錄啟用伺服器端 LDAPS。

使用 AWS 管理 Microsoft AD 啟用用戶端 LDAPS

管理 Microsoft AD 中的用戶端輕量型目錄存取通訊協定安全通訊端層 (SSL)/傳輸層安全性 (TLS) (LDAPS) 支援加密自我 AWS 管理 (內部部署) Microsoft Active Directory (AD) 和應用程式之間的通訊。 AWS 此類應用程序的示例包括 WorkSpaces AWS IAM Identity Center QuickSight，Amazon 和 Amazon Chime。此加密有助於保護您組織的身分資料並符合您的安全要求。

必要條件

啟用用戶端 LDAPS 前，您必須符合以下要求。

主題

- 在受管理的 Microsoft AD 與自我 AWS 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
- 網路要求

在受管理的 Microsoft AD 與自我 AWS 管理之間建立信任關係 Microsoft Active Directory

首先，您必須在受管理的 Microsoft AD 與自我 AWS 管理之間建立信任關係，才能啟用MicrosoftActive Directory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

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：

- 需要企業憑證授權單位 (CA) 才能啟用用戶端 LDAPS。您可以使用Active Directory憑證服務 (協力廠商商業憑證授權單位)，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 受管理的 Microsoft AD 目錄最多可以儲存五 (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 安全性群組和網路防火牆，以允許在 Microsoft AD 管理 (輸出) 和自我 AWS 管理的 Active Directory (輸入) 中的連接埠 636 上進行 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。您可以使用該 AWS Management Console 方法或方 AWS CLI 法。

> **Note**
>
> 用戶端 LDAPS 是 AWS 管理 Microsoft AD 的區域功能。如果您使用 多區域複製，則必須在每個區域中單獨執行以下程序。如需詳細資訊，請參閱 全域與區域功能。

主題

步驟 1：在中註冊證書 AWS Directory Service

使用下列其中一種方法在中註冊憑證 AWS Directory Service。

方法 1：在 AWS Directory Service （AWS Management Console）中註冊您的證書

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）中註冊您的證書

- 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：在 AWS Directory Service （ AWS Management Console ）中檢查證書註冊狀態

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：在 AWS Directory Service （ AWS CLI ）中檢查證書註冊狀態

- 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 AWS Directory Service一種方法來啟用中的用戶端 LDAPS。

> **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：若要在 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：若要在 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 AWS Directory Service一種方法來檢查中的 LDAPS 狀態。

方法 1：若要在 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：要在 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。您可以使用該 AWS Management Console 方法或方 AWS CLI 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：若要在 AWS Directory Service (AWS Management Console) 中檢視憑證詳細資料

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：若要在 AWS Directory Service (AWS CLI) 中檢視憑證詳細資料

- 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：若要在 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：若要在 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：若要在 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：若要在 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 受管理的 Microsoft AD 網域控制站的程序最多可能需要 30 分鐘的時間。如果您在憑證註冊時遇到問題，而且想要重新啟動 AWS 受管理的 Microsoft AD 網域控制站，您可以連絡 AWS Support。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 的合規性

您可以在 AWS 雲端中，使用 AWS Managed Microsoft AD 來支援符合下列合規需求的 Active Directory 感知應用程式。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，且可當做一部分解決方案使用 (須取得合規認證)。

AWS Managed Microsoft AD 符合美國聯邦風險與授權管理計劃 (FedRAMP) 安全性規定，並已獲得 FedRAMP 聯合授權委員會 (JAB) 依 FedRAMP 中度基準所核發的臨時操作授權 (P–ATO)。如需 FedRAMP 合規的詳細資訊，請參閱 FedRAMP 合規。

AWS Managed Microsoft AD 具備服務供應商第 1 級之支付卡產業 (PCI) 資料安全標準 (DSS) 3.2 版的合規聲明文件。使用 AWS 產品和服務存放、處理或傳輸持卡人資料的客戶，可以使用 AWS Managed Microsoft AD 來管理自己的 PCI DSS 合規認證。

如需 PCI DSS 的詳細資訊，包括如何索取 AWS PCI 合規套裝服務的副本，請參閱 PCI DSS 第 1 級。重要的是，您必須在 AWS Managed Microsoft AD 中設定微調密碼政策，以符合 PCI DSS 3.2 版標準。如需詳細資訊，請參閱下方標題「為您的 AWS Managed Microsoft AD 目錄啟用 PCI 合規」的區段。

AWS 已擴大其健康保險流通與責任法案 (HIPAA) 合規計劃，並加入 AWS Managed Microsoft AD 作為 HIPAA 合格服務。如果您與 AWS 簽署了執行商業夥伴協定 (BAA)，則可以使用 AWS Managed Microsoft AD 協助建立符合 HIPAA 標準的應用程式。

AWS 提供一份以 HIPAA 為主題的白皮書，讓想要進一步了解如何利用 AWS 處理和存放健康資訊的客戶查閱。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 AWS 雲端中執行的應用程式。您必須確保 AWS 服務的使用符合標準。

如需 AWS Managed Microsoft AD 所支援之各種 AWS 合規計劃的完整清單，請參閱 合規計劃的 AWS 服務範圍。

為您的 AWS Managed Microsoft AD 目錄啟用 PCI 合規

若要為您的 AWS Managed Microsoft AD 目錄啟用 PCI 合規，您必須依照 AWS Artifact 所提供之「PCI DSS 合規聲明 (AOC) 與責任摘要」文件中的指定，來設定微調密碼政策。

如需使用微調密碼政策的詳細資訊，請參閱「管理 AWS 受管理 Microsoft AD 的密碼原則」。

增強您的 AWS Managed Microsoft AD 網路安全組態

針對 AWS Managed Microsoft AD 目錄佈建的 AWS 安全群組會設定為支援 AWS Managed Microsoft AD 目錄所有已知使用案例所需的最小傳入網路連接埠。如需已佈建的 AWS 安全群組的詳細資訊，請參閱 什麼被創建與 AWS 管理 Microsoft AD 活動目錄。

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。

主題

- AWS 應用程式僅支援
- 僅具有信任支援的 AWS 應用程式
- AWS 應用程式和原生 Active Directory 工作負載支援
- AWS 應用程式和具有信任支援的原生 Active Directory 工作負載支援

AWS 應用程式僅支援

所有使用者帳戶僅佈建於您的 AWS Managed Microsoft AD 中，以便和支援的 AWS 應用程式搭配使用，例如：

- Amazon Chime
- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center

- Amazon 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 AWS Managed Microsoft AD 域控制器的所有非必要流量。

> **Note**
>
> - 下列項目與此 AWS 安全性群組組態不相容：
>   - 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。

僅具有信任支援的 AWS 應用程式

所有使用者帳戶佈建於您的 AWS Managed Microsoft AD 或信任的 Active Directory 中，以便和支援的 AWS 應用程式搭配使用，例如：

- Amazon Chime

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

您可以修改佈建的 AWS 安全群組組態來封鎖 AWS Managed Microsoft AD 域控制器的所有非必要流量。

> **Note**
>
> - 下列項目與此 AWS 安全性群組組態不相容：
>   - 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「內部部署 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	內部部署 CIDR	DNS	使用者和電腦身分驗證、名稱解析、信任
TCP 和 UDP	88	內部部署 CIDR	Kerberos	使用者和電腦身分驗證、森林層級信任
TCP 和 UDP	389	內部部署 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	內部部署 CIDR	Kerberos 更改/設定密碼	複寫、使用者和電腦身分驗證、信任
TCP	445	內部部署 CIDR	SMB/CIFS	複寫、使用者和電腦身分驗證群組政策、信任
TCP	135	內部部署 CIDR	複寫	RPC、EPM
TCP	636	內部部署 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	內部部署 CIDR	RPC	複寫、使用者和電腦身分驗證、群組政策、信任
TCP	3268-3269	內部部署 CIDR	LDAP GC 和 LDAP GC 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
UDP	123	內部部署 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	內部部署 CIDR	所有流量	

AWS 應用程式和原生 Active Directory 工作負載支援

使用者帳戶僅佈建於您的 AWS Managed Microsoft AD 中，以便和支援的 AWS 應用程式搭配使用，例如：

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

- AWS Client VPN
- AWS Management Console

您可以修改佈建的 AWS 安全群組組態來封鎖 AWS Managed Microsoft AD 域控制器的所有非必要流量。

> **Note**
>
> - 無法在您的 AWS Managed Microsoft AD 目錄和內部部署域之間，建立和維護使用中的目錄信任。
> - 它要求您確保「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。
> - 如果您想要使用具有此組態的企業 CA，則必須建立傳出規則「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	用戶端 CIDR	DNS	使用者和電腦身分驗證、名稱解析、信任
TCP 和 UDP	88	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	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	用戶端 CIDR	SMB/CIFS	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	464	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	用戶端 CIDR	複寫	RPC、EPM
TCP	636	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	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	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	用戶端 CIDR	SOAP	AD DS 網路服務
UDP	123	用戶端 CIDR	Windows 時間	Windows 時間、信任
UDP	138	用戶端 CIDR	DFSN 和 NetLogon	DFS、群組政策

傳出規則

無。

AWS 應用程式和具有信任支援的原生 Active Directory 工作負載支援

所有使用者帳戶佈建於您的 AWS Managed Microsoft AD 或信任的 Active Directory 中，以便和支援的 AWS 應用程式搭配使用，例如：

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

您可以修改佈建的 AWS 安全群組組態來封鎖 AWS Managed Microsoft AD 域控制器的所有非必要流量。

> **Note**
>
> - 它要求您確保「內部部署 CIDR」和「用戶端 CIDR」網路是安全的。
> - 具有「內部部署 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「用戶端 CIDR」的 TCP 445 應該保持開啟狀態，因為這是群組政策處理所需。
> - 只有在使用透過 SSL 的 LDAP 時，才需要 TCP 636。
> - 如果您想要使用具有此組態的企業 CA，則必須建立傳出規則「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	內部部署 CIDR	DNS	使用者和電腦身分驗證、名稱解析、信任
TCP 和 UDP	88	內部部署 CIDR	Kerberos	使用者和電腦身分驗證、森林層級信任
TCP 和 UDP	389	內部部署 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	內部部署 CIDR	Kerberos 更改/設定密碼	複寫、使用者和電腦身分驗證、信任
TCP	445	內部部署 CIDR	SMB/CIFS	複寫、使用者和電腦身分驗證群組政策、信任
TCP	135	內部部署 CIDR	複寫	RPC、EPM
TCP	636	內部部署 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	內部部署 CIDR	RPC	複寫、使用者和電腦身分驗證、群組政策、信任
TCP	3268-3269	內部部署 CIDR	LDAP GC 和 LDAP GC 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
UDP	123	內部部署 CIDR	Windows 時間	Windows 時間、信任
TCP 和 UDP	53	用戶端 CIDR	DNS	使用者和電腦身分驗證、名稱解析、信任
TCP 和 UDP	88	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	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	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	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	用戶端 CIDR	複寫	RPC、EPM
TCP	636	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

通訊協定	連接埠範圍	來源	流量類型	Active Directory 用量
TCP	49152 - 65535	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	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	用戶端 CIDR	SOAP	AD DS 網路服務
UDP	123	用戶端 CIDR	Windows 時間	Windows 時間、信任
UDP	138	用戶端 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	內部部署 CIDR	所有流量	

設定目錄安全設定

您可以為 AWS Managed Microsoft AD 設定精細的目錄設定，以滿足合規和安全要求，而無需增加任何操作工作負載。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，您可以靈活地分別停用舊式加密方式 (例如 RC4 或 DES) 以及協定 (例如 SSL 2.0/3.0 和 TLS 1.0/1.1)。AWS然後，Managed Microsoft AD 會將組態部署到目錄中的所有域控制站，管理域控制站會重新啟動，並在您橫向擴展或部署更多 AWS 區域 時維護此組態。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，然後在 https://console.aws.amazon.com/directoryservicev2/ 開啟 AWS Directory Service 主控台。
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。完成所需並確認變更後，請選擇更新設定。然後，您將返回目錄 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。

類型	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。 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。

類型	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 (預設)：即便憑證無法強式地對應到使用者，亦允許進行身分驗證。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。 • 完整強制執行：如果憑證無法強式地對應到使用者，則不允許進行身分驗證。如果您選擇此強制執行類型，則無法設定憑證回溯認證。

類型	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。

類型	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。

類型	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。

類型	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 AD 的 AWS Private CA 連接器

您可以將 AWS 受管理的 Microsoft AD 與 AWS Private Certificate Authority (CA) 整合，以便為您的 Active Directory 網域加入的使用者、群組和機器發行及管理憑證。 AWS Private CA Active Directory 的連接器可讓您為自我管理的企業 CA 使用完全受控的 AWS Private CA 嵌入式替代方案，而不需要部署、修補或更新本機代理程式或 Proxy 伺服器。

> **Note**
>
> 不支援使用中目錄 AWS Private CA 連接器的 AWS 受管理 Microsoft AD 網域控制站的伺服器端 LDAPS 憑證註冊。若要為您的目錄啟用伺服器端 LDAPS，請參閱如何為 AWS 受管理的 Microsoft AD 目錄啟用伺服器端 LDAPS。

您可以透過 Directory Service 主控台、使用中目錄的 AWS Private CA 連接器主控台或呼叫 `CreateTemplate`API 來設定與目錄的 AWS Private CA 整合。若要透過使用中目錄的 AWS Private CA 連接器主控台設定私有 CA 整合，請參閱建立連接器範本。請參閱以下有關如何從 AWS Directory Service 主控台設定此整合的步驟。

若要設定 AD 的 AWS Private CA 連接器

1. 登入 AWS Management Console 並開啟 AWS Directory Service 主控台，位於https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 [網路與安全性] 索引標籤下的 [ADAWS Private CA 連接器] 下，選擇 [設定 AD 的 AWS Private CA 連接器]。此時會顯示「建立私人 CA 憑證 Active Directory」頁面。依照主控台上的步驟，為 Active Directory連接器建立私人 CA，以便在私人 CA 中註冊。如需詳細資訊，請參閱建立連接器。
4. 建立連接器後，請按照以下步驟檢視詳細資訊，包括連接器的狀態和關聯的私有 CA 的狀態。

若要檢視 AD 的 AWS Private CA 連接器

1. 登入 AWS Management Console 並開啟 AWS Directory Service 主控台，位於https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在網路與安全性中的適用於 AD 的AWS Private CA 連接器下，您可以檢視私有 CA 連接器和關聯的私有 CA。依預設，您會看到下列欄位：

    a. AWS Private CA 連接器 ID — 連接 AWS Private CA 器的唯一識別碼。按一下它會導致該 AWS Private CA 連接器的詳細資料頁面。

    b. AWS Private CA 主旨 — 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 — 以 AWS Private CA 連接器和的狀態檢查為基礎 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 — 建立 AWS Private CA 連接器的日期。

如需詳細資訊，請參閱檢視連接器詳細資訊。

監控您的 AWS Managed Microsoft AD

您可以使用以下方法來監控您的 AWS Managed Microsoft AD 目錄：

主題

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 Support 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 疑難排解 AWS 管理 Microsoft AD、AD Connector 疑難排

解、Simple AD 疑難排解。對於一般維護相關問題，請在 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 Support 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 建立目錄快照或還原目錄。

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

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 Support 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 SNS 設定目錄狀態通知

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。使用以下步驟，您可以將 AWS Directory Service 作為發佈者新增至 Amazon SNS 主題。當 AWS Directory Service 偵測到目錄狀態變更時，會將訊息發佈到該主題，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？」。

> **Note**
>
> 目錄狀態通知是 AWS 受管理的 Microsoft AD 的區域功能。如果您使用 多區域複製，則必須在每個區域中單獨執行以下程序。如需詳細資訊，請參閱 全域與區域功能。

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. 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**
   >
   > 如果您使用僅具有DirectoryServiceFullAccess受管政策的 IAM 使用者或角色登入，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. 選擇建立。

如果您想要指定其他 SNS 訂閱者 (例如其他電子郵件地址、Amazon SQS 佇列) AWS Lambda，或者，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. 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。如果要刪除整個主題，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，請將您的目錄與其他 Amazon SNS 主題建立關聯。

檢閱您的 AWS Managed Microsoft AD 目錄日誌

AWS Managed Microsoft AD 域控制站執行個體中的安全日誌會封存一年。您也可以設定 AWS Managed Microsoft AD 目錄，以近乎即時的方式轉發域控制器日誌至 Amazon CloudWatch Logs。如需更多詳細資訊，請參閱 啟用日誌轉發。

AWS 會記錄下列合規事件。

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
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	Success (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	Success (成功)
	稽核登入	成功、失敗
	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

監控類別	政策設定	稽核狀態
	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	Success (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

啟用日誌轉發

您可以使用 AWS Directory Service 主控台或 API 來轉發域控制器安全事件日誌至 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 還可以將這些事件轉寄到其他 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**
>
> 日誌轉發是 AWS Managed Microsoft AD 的區域功能。如果您使用 多區域複製，則必須在每個區域中單獨執行以下程序。如需更多詳細資訊，請參閱 全域與區域功能。

啟用日誌轉發

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 選擇您要共享之 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。如需更多詳細資訊，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)。

停用日誌轉發

1. 在 AWS Directory Service 主控台導覽窗格中，選擇 Directories (目錄)。
2. 選擇您要共享之 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。如需更多詳細資訊，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. 讀取資訊之後，請在 Disable log forwarding (停用日誌轉發) 對話方塊中，選擇 Disable (停用)。

透過 CLI 來啟用日誌轉發

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。若要透過 CLI 啟用日誌轉發，請完成下列所有步驟。

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 命令範例

```
aws logs create-log-group --log-group-name '/aws/directoryservice/
d-9876543210'
```

POWERSHELL 命令範例

```
New-CWLLogGroup -LogGroupName '/aws/directoryservice/d-9876543210'
```

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 資源政策授權 AWS Directory Service 將日誌增加至您在步驟 1 所建立的新日誌群組。您可以指定確切的 ARN 至該日誌群組，藉以限制 AWS Directory Service 存取其他日誌群組的權限；或使用萬用字元來納入所有日誌群組。以下範例政策針對目錄所在的 AWS 帳戶，使用萬用字元方法來識別所有開頭為 `/aws/directoryservice/` 的日誌群組。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ds.amazonaws.com"
            },
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER: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 命令範例

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

POWERSHELL 命令範例

```
$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 命令範例

```
aws ds create-log-subscription --directory-id 'd-9876543210' --log-group-name '/aws/directoryservice/d-9876543210'
```

POWERSHELL 命令範例

```
New-DSLogSubscription -DirectoryId 'd-9876543210' -LogGroupName '/aws/directoryservice/d-9876543210'
```

透過效能指標監控域控制站

AWS Directory Service 與 Amazon 整合，協 CloudWatch 助您為. 中的每個網域控制站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 主題起始自動化 (例如 AWS Lambda 功能)，以增加您的網域控制站數目Active Directory。

如需監控域控制站的詳細資訊，請參閱 判斷何時新增含 CloudWatch 量度的網域控制站。

有與 Amazon 相關的費用 CloudWatch。如需詳細資訊，請參閱CloudWatch帳單與費用。

> **Important**
>
> 加拿大西部 (卡加利) 區域無法使用的網域控制站效能指標。 CloudWatch

尋找網域控制站效能指標 CloudWatch

在 Amazon 主 CloudWatch 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 受管理 Microsoft AD 網域控制站度量所需的正確命名空間和從屬度量。

在 CloudWatch 主控台中尋找網域控制站度量

1. 請登入 AWS Management Console 並開啟 CloudWatch 主控台，網址為 https://console.aws.amazon.com/cloudwatch/。
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站指標的指示，請參閱 AWS 安全性部落格中的如何根據使用率指標自動化 AWS 受管 Microsoft AD 擴展。

判斷何時新增含 CloudWatch 量度的網域控制站

所有網域控制站的負載平衡對於您的Active Directory. 若要協助您最佳化 Microsoft AWS 受管理 AD 中的網域控制站效能，建議您先監視中 CloudWatch 的重要指標，以形成基準。在此過程中，您會分析Active Directory隨著時間的推移，以確定您的平均使用率和尖峰Active Directory使用率。決定基準之後，您可以定期監視這些指標，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。如需中可用網域控制站度量的完整清單 CloudWatch，請參閱AWS 受管理 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 受管理的 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站指標的指示，請參閱 AWS 安全性部落格中的如何根據使用率指標自動化 AWS 受管 Microsoft AD 擴展。有關中指標的一般資訊 CloudWatch，請參閱 Amazon 使用者指南中的使 CloudWatch 用 Amazon 指 CloudWatch 標。

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

AWS 受管理 Microsoft AD 效能計數器

下表列出 Amazon 中可用來追蹤 AWS 受管 Microsoft AD 中 CloudWatch 的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 (元)	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

指標類別	指標名稱
	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
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

指標類別	指標名稱
	NTLM 身分驗證

多區域複製

多區域複寫可用於跨多個 AWS AWS 區域管理的 Microsoft AD 目錄資料自動複寫。此複寫可以改善分散地理位置的使用者和應用程式的效能。 AWS 受管理的 Microsoft AD 會使用原生作用中目錄複寫，將目錄的資料安全地複寫到新的區域。

只有 AWS 受管理 Microsoft AD 的企業版才支援多區域複寫。

您可以在提供 AWS Managed Microsoft AD 的大多數區域中使用自動多區域複寫功能。

Important

在下列選擇加入區域中無法使用多區域複寫：

- 非洲 (開普敦) af-south-1
- 亞太區域 (香港) ap-east-1
- 亞太區域 (海德拉巴) ap-south-2
- 亞太區域 (雅加達) ap-southeast-3
- 亞太區域 (墨爾本) ap–southeast–4
- 加拿大西部 (卡加利) CA-西 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）中部 -1
- 中東 (巴林) me-south-1
- 中東 (阿拉伯聯合大公國) me-central-1

如需有關選擇加入區域以及如何啟用這些區域的詳細資訊，請參閱指AWS Account Management 南中的指定 AWS 區域 您的帳戶可以使用的項目。

優勢

使用 AWS 受管理 Microsoft AD 中的多區域複寫時，使用中的目錄感知應用程式會在本機使用目錄以取得高效能，並使用多區域功能來提供復原能力。您可以將多區域複寫與作用中的目錄感知應用程式 (例如 SharePoint 和 SQL Server 永遠開啟)，以及適用於 SQL 伺 AWS 服器的 Amazon RDS 和 FSx for Windows File Server 等服務一起使用。以下是多區域複寫的其他優勢。

- 它可讓您快速地在全域部署單一 AWS 受管理的 Microsoft AD 執行個體，並免除自我管理全域 Active Directory 基礎結構的繁重工作。
- 它可讓您在多個 AWS 區域中部署和管理 Windows 和 Linux 工作負載，更輕鬆且更具成本效益。自動化的多區域複寫可讓您的全域使用中目錄感知應用程式達到最佳效能。部署在 Windows 或 Linux 執行個體中的所有應用程式都會使用區域中的本機 AWS 管理 Microsoft AD，以便能夠回應來自最近區域的使用者要求。
- 它提供多區域彈性。 AWS 受管理的 Microsoft AD 部署在高可用性 AWS 受管理的基礎結構中，可處理所有區域的自動化軟體更新、監視、復原，以及基礎 Active Directory 基礎結構的安全性。這使您可以專注於建立應用程式。

主題

全域與區域功能

使用多區域複寫將 AWS 區域新增至目錄時，會 AWS Directory Service 增強所有功能的範圍，使其成為區域感知功能。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 受管理 Microsoft AD 的企業版才支援多區域複寫。

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

透過多區域複寫， AWS 受管理的 Microsoft AD 會使用下列兩種類型的區域來區分應如何在您的目錄中套用全域或區域功能。

主要區域

您首次建立目錄的初始區域稱為主要區域。您只能從主要區域執行全域目錄層級的操作，例如建立 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。

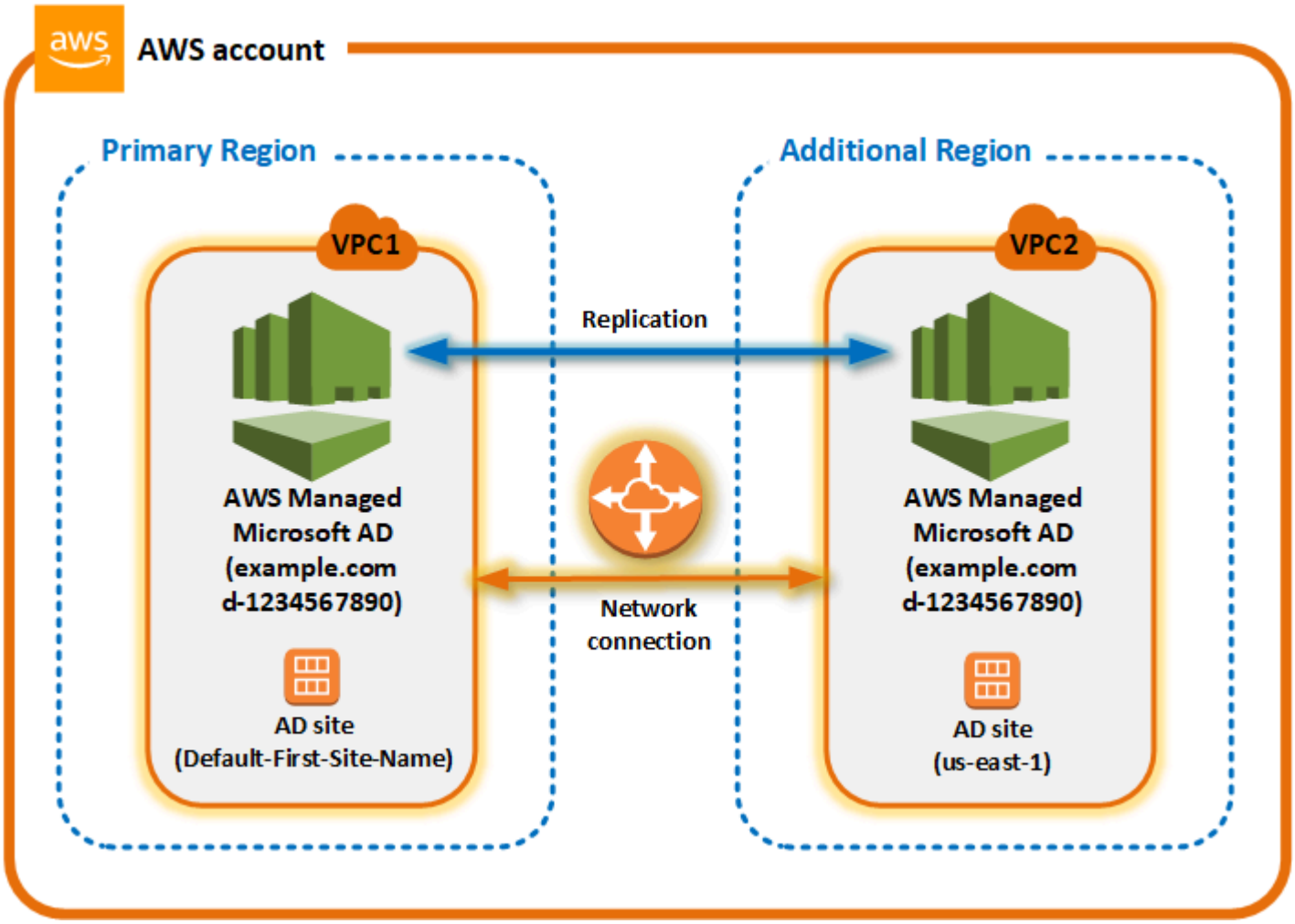
選取其他區域時對 區域功能 所做的任何變更將僅套用於相應區域。

多區域複寫的運作方式

透過多區域複寫功能， AWS 受管理的 Microsoft AD 可免除管理全域 Active Directory 基礎結構的無差別繁重工作。設定完成後，會跨多個 AWS 區域 AWS 複寫所有客戶目錄資料，包括使用者、群組、群組原則和結構描述。

新增區域後，將自動發生以下操作，如圖所示：

- AWS 受管理的 Microsoft AD 會在選取的 VPC 中建立兩個網域控制站，並將它們部署到相同 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 受管理的 Microsoft AD 會設定主要區域與新區域之間的網路連線。
- AWS 管理 Microsoft AD 創建一個新的活動目錄網站，並給它相同的名稱為區域，如美國東部 -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 受管理的 Microsoft AD 會將所有 Active Directory 物件和組態複寫到新的區域，包括使用者、群組、群組原則、使用中目錄信任、組織單位和使用中目錄結構描述。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，Microsoft AWS 受管理 AD 會讓所有功能感知多區域。如需詳細資訊，請參閱 全域與區域功能。



Active Directory 站台

多區域複寫支援多個作用中目錄站台 (每個區域一個作用中目錄站台)。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 站台及服務工具對其進行重新命名。

AWS 服務

AWS 適用於 SQL 伺服器的 Amazon RDS 和亞馬遜 FSx 等服務會連接到全域目錄的本機執行個體。這可讓您的使用者一次登入執行的作用中目錄感知應用程式， AWS 以及任何 AWS 區域中的 Amazon RDS for SQL Server 等 AWS 服務。若要這麼做，當您與受 AWS 管理的 Microsoft AD 信任時，使用者需要來自受 AWS 管理的 Microsoft AD 或內部部署 Active Directory 的認證。

您可以搭配多區域複寫功能使用下列 AWS 服務。

- Amazon EC2
- FSx for Windows File Server

- Amazon RDS 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已關閉， AWS Managed 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。

新增複寫區域

使用此多區域複製功能新增區域時， AWS 受管 Microsoft AD 會在選取的 AWS 區域、Amazon Virtual Private Cloud (VPC) 和子網路中建立兩個網域控制站。 AWS 受管理的 Microsoft AD 也會建立相關的安全性群組，讓 Windows 工作負載連線至新區域中的目錄。它也會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。

只有 AWS 受管理 Microsoft AD 的企業版才支援多區域複寫。

必要條件

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。

- 確認您在要將目錄複寫到的新區域中具有必要的 AWS Identity and Access Management (IAM) 許可、Amazon VPC 設定和子網路設定。
- 如果您想要使用現有的內部部署 Active Directory 認證來存取和管理中的使用中目錄感知工作負載 AWS，您必須在 AWS 受管理的 Microsoft AD 和您的內部部署 AD 基礎結構之間建立 Active Directory 信任。如需信任的詳細資訊，請參閱 Connect 到您現有的活動目錄基礎結構。
- 如果現場部署 Active Directory 之間有現有的信任關係，而且想要新增複寫區域，則需要確認您在要複寫目錄的新區域中具有必要的 Amazon VPC 和子網路設定。

新增區域

請使用下列程序，為您的 AWS 受管理 Microsoft AD 目錄新增複寫的區域。

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 受管理的 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 新增或移除其他域控制站。
- 每個區域與更多 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 共享您的目錄。
- 啟用日誌轉送功能，使用 Amazon 日誌從新區域擷取目錄的安全 CloudWatch 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 啟用日誌轉發。
- 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 SNS 設定目錄狀態通知。

刪除複寫區域

請使用下列程序來刪除 AWS 受管理 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。

共享您的目錄

AWS Managed Microsoft AD 能緊密結合 AWS Organizations，並讓多個 AWS 帳戶能夠流暢進行目錄共享。您可以與相同組織內的其他可信任 AWS 帳戶共享單一目錄，或者與您組織以外的其他 AWS 帳戶共享該目錄。您也可以在 AWS 帳戶目前不是組織成員時，共享您的目錄。

> **Note**
>
> AWS 會額外收取目錄共享的費用。若要進一步了解，請參閱 AWS Directory Service 網站上的定價頁面。

運用目錄共享，AWS Managed Microsoft AD 就能以更符合成本效益的整合方法，操作多個帳戶及 VPC 的 Amazon EC2。目錄共享適用於所有的 AWS 區域，此類區域當中會提供 AWS Managed Microsoft AD。

> **Note**
>
> 在 AWS 中國 (寧夏) 區域中，這項功能只能在使用 AWS Systems Manager (SSM) 流暢加入 Amazon EC2 執行個體時有效運作。

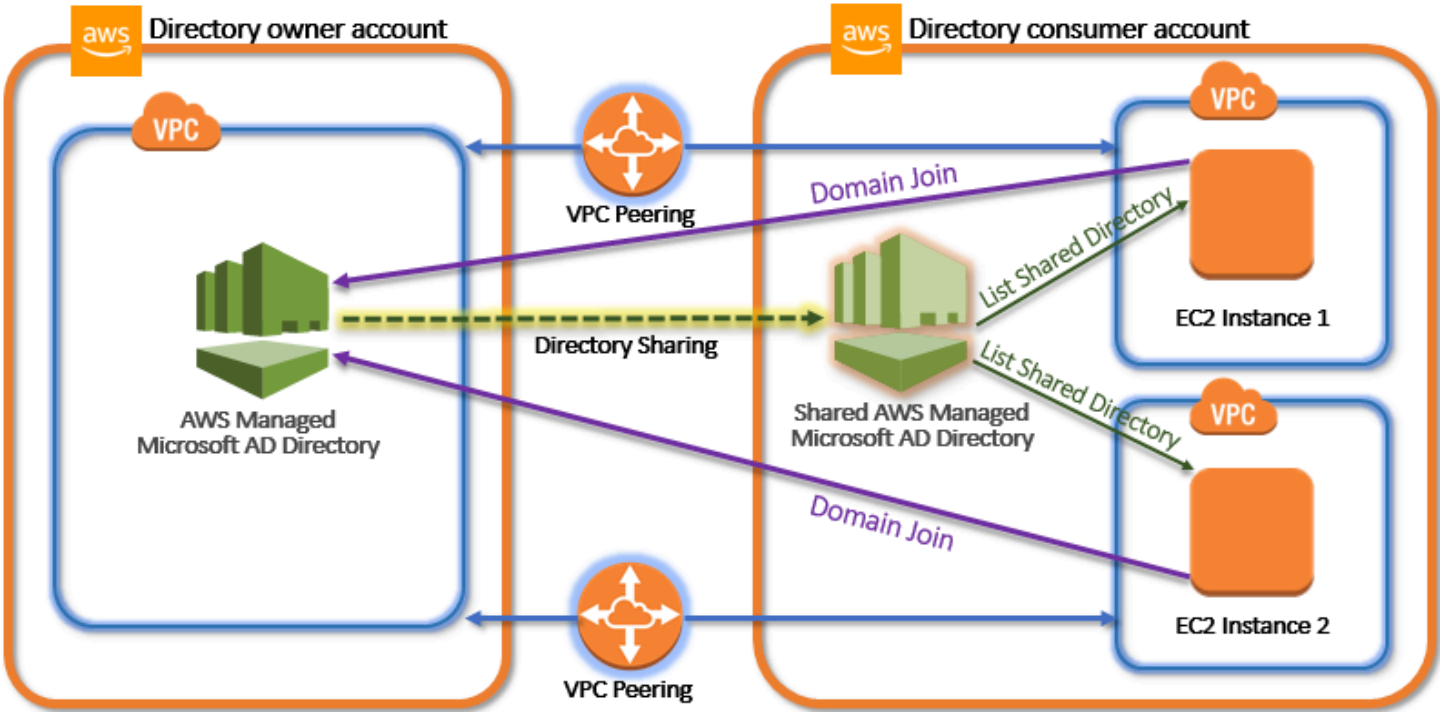
如需有關目錄共享及如何在 AWS 帳戶邊界處推廣 AWS Managed Microsoft AD 目錄的詳細資訊，請參閱下列主題。

主題

- 重要的目錄共享概念
- 教學課程：共用您的 AWS 受管 Microsoft AD 目錄以進行無縫 EC2 網域加入
- 取消目錄的共用

重要的目錄共享概念

如果您熟悉以下重要概念，將更能充分利用目錄共享功能。



目錄擁有者帳戶

目錄擁有者是 AWS 帳戶 持有者，其擁有共享目錄關係中的發起目錄。這個帳戶中的管理員可透過指定要共享其目錄的 AWS 帳戶，進而啟動目錄共享工作流程。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 提供以下兩種目錄共享方法：

- 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。這種共享方法可以簡化您的設定過程，因為它不會要求目錄消費者帳戶接受您的目錄共享請求。在主控台中，此方法稱為與組織內的 AWS 帳戶 共用此目錄。
- 交握 – 這種方法可讓您在未使用 AWS Organizations 時啟用目錄共享。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

網路連線能力是使用跨 AWS 帳戶 目錄共享關係的先決條件。AWS 支援許多連線您 VPC 的解決方案，其中包括 VPC 對等連線、Transit Gateway 和 VPN。若要開始使用，請參閱 教學課程：共用您的 AWS 受管 Microsoft AD 目錄以進行無縫 EC2 網域加入。

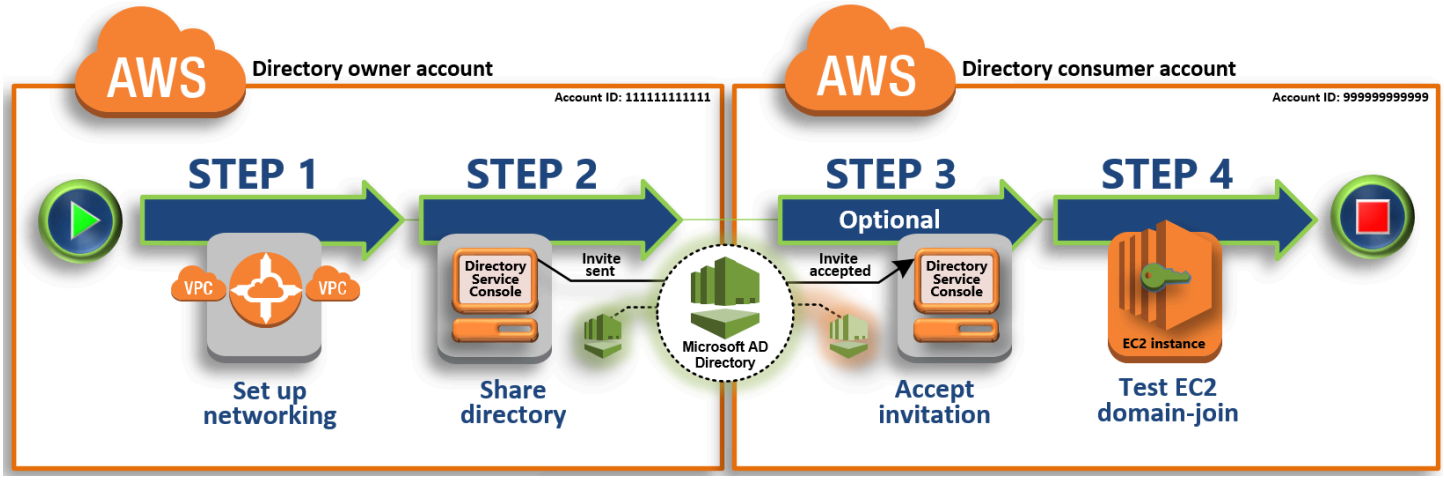
教學課程：共用您的 AWS 受管 Microsoft AD 目錄以進行無縫 EC2 網域加入

本教學課程說明如何與另一個 (目錄用戶帳戶) 共用 AWS 受管理的 Microsoft AD 目錄 AWS 帳戶 (目錄擁有者帳戶)。完成網路必要條件之後，您將在兩者之間共用一個目錄 AWS 帳戶。然後，您將能夠了解如何將 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與同一組織 AWS 帳戶 中的其他人共用目錄，還是與 AWS 組織外部的帳戶共用目錄而有所不同。 AWS 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：接受共享目錄邀請-可選

使用目錄用戶管理員認證登入時，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 VPC 加入單一 AWS 受管 Microsoft AD 目錄

步驟 1：設定聯網環境

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：

- 在同一個區域中創建兩個用 AWS 帳戶 於測試目的的的新。當您創建一個時 AWS 帳戶，它會自動在每個帳戶中創建一個專用的虛擬私有雲（VPC）。記下每個帳戶內的 VPC ID。後續操作將會用到這份資料。
- 使用這個步驟的程序，在每個帳戶的兩個 VPC 之間建立 VPC 對等連線。

> **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. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。確定在目錄擁有者帳戶中，使用管理員登入資料登入為使用者。
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)。

由於這兩個 VPC 都位於相同區域，所以送出 VPC 對等請求的目錄擁有者帳戶也可以代表目錄消費者帳戶接受該對等請求。

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。
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。

務必設定您的目錄消費者 VPC 的安全群組，才能在向外規則表格中新增 Active Directory 通訊協定和連接埠，啟用向外流量。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 管理 Microsoft AD 的區域功能。如果您使用 多區域複製，則必須在每個區域中單獨執行以下程序。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. 在目錄擁有者帳戶中 AWS Management Console 使用管理員憑據登錄，然後在 https://console.aws.amazon.com/directoryservicev2/ 打開AWS Directory Service 控制台。
2. 在導覽窗格中，選擇目錄。
3. 選擇您要共用的 AWS 受管理 Microsoft AD 目錄的目錄識別碼。
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 [選擇分享 AWS 帳戶 對象] 頁面上，根據您的業務需求，選擇下列其中一種分享方法：
   a. 與組織 AWS 帳戶 內部共用此目錄 — 使用此選項，您可以從顯示組 AWS 織內部所有 AWS 帳戶 內容的清單中選取要共用目錄的目錄。 AWS 帳戶 您必須 AWS Directory Service 先啟用受信任的存取權，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 在您的組織中，選取您 AWS 帳戶 要與其共用目錄的對象，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。因為所有組織 AWS 帳戶 都在同一個組織中，因此您不需要遵循步驟 3。

b. 與其他人共享此目錄 AWS 帳戶-使用此選項，您可以與 AWS 組織內部或外部的帳戶共享目錄。當您的目錄不是組織的成員，而且您想要與其他組 AWS 織共用時，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：接受共享目錄邀請-可選

步驟 3：接受共享目錄邀請-可選

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 [與組織 AWS 帳戶 內部共用此目錄] 選項，請略過此步驟並繼續執行步驟 4。

接受共享目錄邀請

1. 在目錄 AWS Management Console 用戶帳戶中使用管理員憑據登錄，然後在 https://console.aws.amazon.com/directoryservicev2/ 打開AWS Directory Service 控制台。
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 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 在導航欄中，選擇與現有目錄 AWS 區域 相同的目錄。
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。

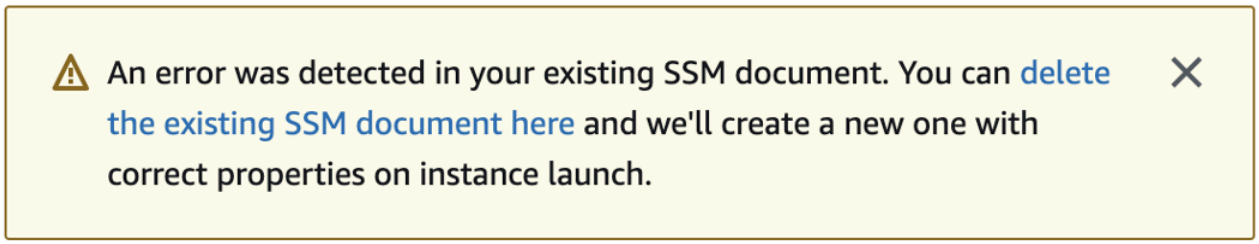
e. 您的瀏覽器會自動下載私有金鑰檔案。將私有金鑰檔案存放在安全的地方。

> **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 地址的詳細資訊，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的 Amazon EC2 執行個體 IP 地址一節。
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 啟動精靈識別具有未預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
>
> - 如果您之前已編輯過 SSM 文件，且預期會有屬性，請選擇 [關閉] 並繼續啟動 EC2 執行個體而不進行任何變更。
> - 選取此處刪除現有 SSM 文件連結以刪除 SSM 文件。這將允許創建具有正確屬性的 SSM 文檔。SSM 文件會在您啟動 EC2 執行個體時自動建立。

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已DirectoryServiceAccess附加 AWS 受管政策 AmazonSSM ManagedInstanceCore 和 AmazonSSM 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 [新增權限] 下方的原則清單中，選取 [亞馬遜 SSM] ManagedInstanceCore 和 [亞馬遜 SSM] 原則。DirectoryServiceAccess在搜尋方塊中，輸入 **SSM** 以篩選政策。選擇下一步。

        > **Note**
        >
        > AmazonSSM DirectoryServiceAccess 提供將執行個Active Directory體加入至管理的權限。 AWS Directory Service亞馬遜 SSM ManagedInstanceCore 提供了使用該服務所需的最低權限。 AWS Systems Manager 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：使用測試網域加入 AWS Systems Manager

在目錄消費者帳戶中執行這些步驟。若要完成此程序，您需要有關目錄擁有者帳戶的一些資訊，例如目錄 ID、目錄名稱和 DNS IP 地址。

先決條件

- 安裝程式 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。

- 您希望加入 AWS 受管 Microsoft 活動目錄域的實例必須具有附加的 IAM 角色，其中包含亞馬遜 SSM ManagedInstanceCore 和亞馬遜 SSM 託管政策。DirectoryServiceAccess
  - 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。

如需有關使用 Systems Manager 將 EC2 執行個體加入到 AWS 受管 Microsoft Active Directory 網域的詳細資訊，請參閱如 AWS Systems Manager 何使用將執行中的 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，來尋找目錄 ID、目錄名稱和 DNS IP 位址。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。

   - 針對目錄識別碼，輸入 AWS 受管理的 Microsoft 作用中目錄的名稱。
   - 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)。
   - 對於 DNS IP 位址，請在 AWS 受管理的 Microsoft 活動目錄中輸入 DNS 伺服器的 IP 位址 (針對目錄擁有者帳戶)。
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。完成此操作之後，您就可以使用遠端桌面通訊協定 (RDP) 用戶端使用 AWS 受管理 Microsoft AD 使用者帳戶的認證登入執行個體。

取消目錄的共用

使用以下程序來取消 AWS Managed Microsoft AD 目錄的共用。

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。如需更多詳細資訊，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：共享您的目錄，以便將 Amazon EC2 執行個體無縫加入跨 AWS 帳戶的域
- AWS 安全部落格文章：如何從多個帳戶及 VPC 將 Amazon EC2 執行個體加入單一 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 Amazon EC2 實例加入您的 AWS 受管 Microsoft AD 活動目錄

啟動執行個體時，您可以順暢地將 Amazon EC2 執行個體加入您的Active Directory網域。如需詳細資訊，請參閱 將 Amazon EC2 Windows 執行個體無縫加入您的 AWS 受管 Microsoft AD Active Directory。您也可以使用自動化功能直接從 AWS Directory Service 主控台啟AWS Systems Manager 動 EC2 執行個體並將其加入Active Directory網域。

如果您需要手動將 EC2 執行個體加入網Active Directory域，則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

- 在受管理的 Microsoft AD 中啟動目錄 AWS 管理執行個體 Active Directory
- 將 Amazon EC2 Windows 執行個體無縫加入您的 AWS 受管 Microsoft AD Active Directory
- 手動將 Amazon EC2 Windows 實例加入到您的 AWS 受管 Microsoft AD 活動目錄
- 將 Amazon EC2 Linux 執行個體無縫加入您的 AWS 受管 Microsoft AD 活動目錄
- 手動將 Amazon EC2 Linux 執行個體加入您的 AWS 受管 Microsoft AD 活動目錄
- 使用 Winbind 手動將 Amazon EC2 Linux 執行個體加入您的 AWS 受管 Microsoft AD 活動目錄
- 手動將 Amazon EC2 Mac 執行個體加入您的 AWS 受管 Microsoft AD 活動目錄
- 委派 AWS 受管 Microsoft AD 目錄加入權限
- 建立 DHCP 選項集

在受管理的 Microsoft AD 中啟動目錄 AWS 管理執行個體 Active Directory

此程序會在使用自動化管理目錄時啟 AWS Management Console AWS Systems Manager 動目錄管理 EC2 Windows 執行個體。您也可以直接ManagementInstance在自動化主控台中執行自動化 AWS-CreateD 來完成此操作。 AWS Systems Manager

必要條件

若要從主控台啟動目錄管理 EC2 執行個體，您必須在帳戶中啟用下列許可。

- `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`

若要啟動目錄管理 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. 選擇您要在其中啟動作用中目錄管理 EC2 執行個體的目錄識別碼。
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。
7. (選擇性) 選擇 [檢視] AWS CLI 命令以查看您在中用 AWS CLI 來執行此自動化操作的範例。
8. 選擇提交。
9. 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。

若要檢視目錄管理 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 執行個體無縫加入您的 AWS 受管 Microsoft AD Active Directory

此程序可將 Amazon EC2 視窗執行個體無縫連接到您的 AWS 受管 Microsoft AD。如果您需要跨多個進行無縫網域加入 AWS 帳戶，請參閱教學課程：共用您的 AWS 受管 Microsoft AD 目錄以進行無縫 EC2 網域加入。如需 Amazon EC2 的詳細資訊，請參閱什麼是 Amazon EC2？。

無縫加入 Windows EC2 執行個體

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 在導航欄中，選擇與現有目錄 AWS 區域 相同的目錄。

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。

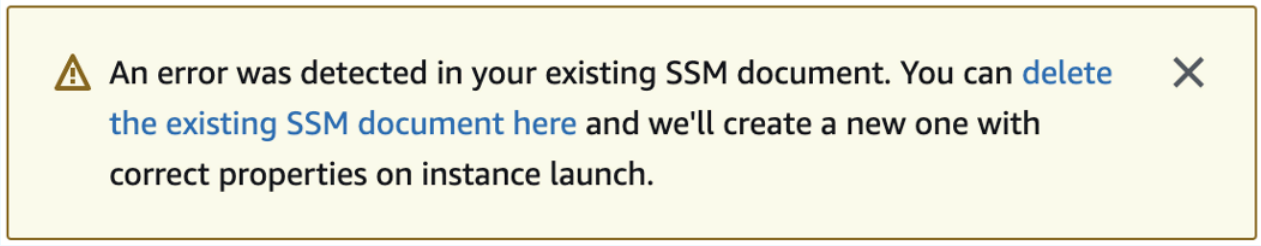
   a. 若要建立新的金鑰對，請選擇建立新金鑰對。
   b. 輸入金鑰對的名稱，然後選取金鑰對類型和私有金鑰檔案格式的選項。
   c. 若要將私有金鑰儲存為可與 OpenSSH 搭配使用的格式，請選擇 .pem。若要將私有金鑰儲存為可與 PuTTY 搭配使用的格式，請選擇 .ppk。
   d. 選擇建立金鑰對。
   e. 您的瀏覽器會自動下載私有金鑰檔案。將私有金鑰檔案存放在安全的地方。

   > **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 地址的詳細資訊，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的 Amazon EC2 執行個體 IP 地址一節。
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 啟動精靈識別具有未預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
>
> - 如果您之前已編輯過 SSM 文件，且預期會有屬性，請選擇 [關閉] 並繼續啟動 EC2 執行個體而不進行任何變更。
> - 選取此處刪除現有 SSM 文件連結以刪除 SSM 文件。這將允許創建具有正確屬性的 SSM 文檔。SSM 文件會在您啟動 EC2 執行個體時自動建立。

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已DirectoryServiceAccess附加 AWS 受管政策 AmazonSSM ManagedInstanceCore 和 AmazonSSM 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 [新增權限] 下方的原則清單中，選取 [亞馬遜 SSM] ManagedInstanceCore 和 [亞馬遜 SSM] 原則。DirectoryServiceAccess在搜尋方塊中，輸入 **SSM** 以篩選政策。選擇下一步。

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess 提供將執行個Active Directory體加入至管理的權限。 AWS Directory Service亞馬遜 SSM ManagedInstanceCore 提供了使用該服務所需的最低權限。 AWS Systems Manager 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。

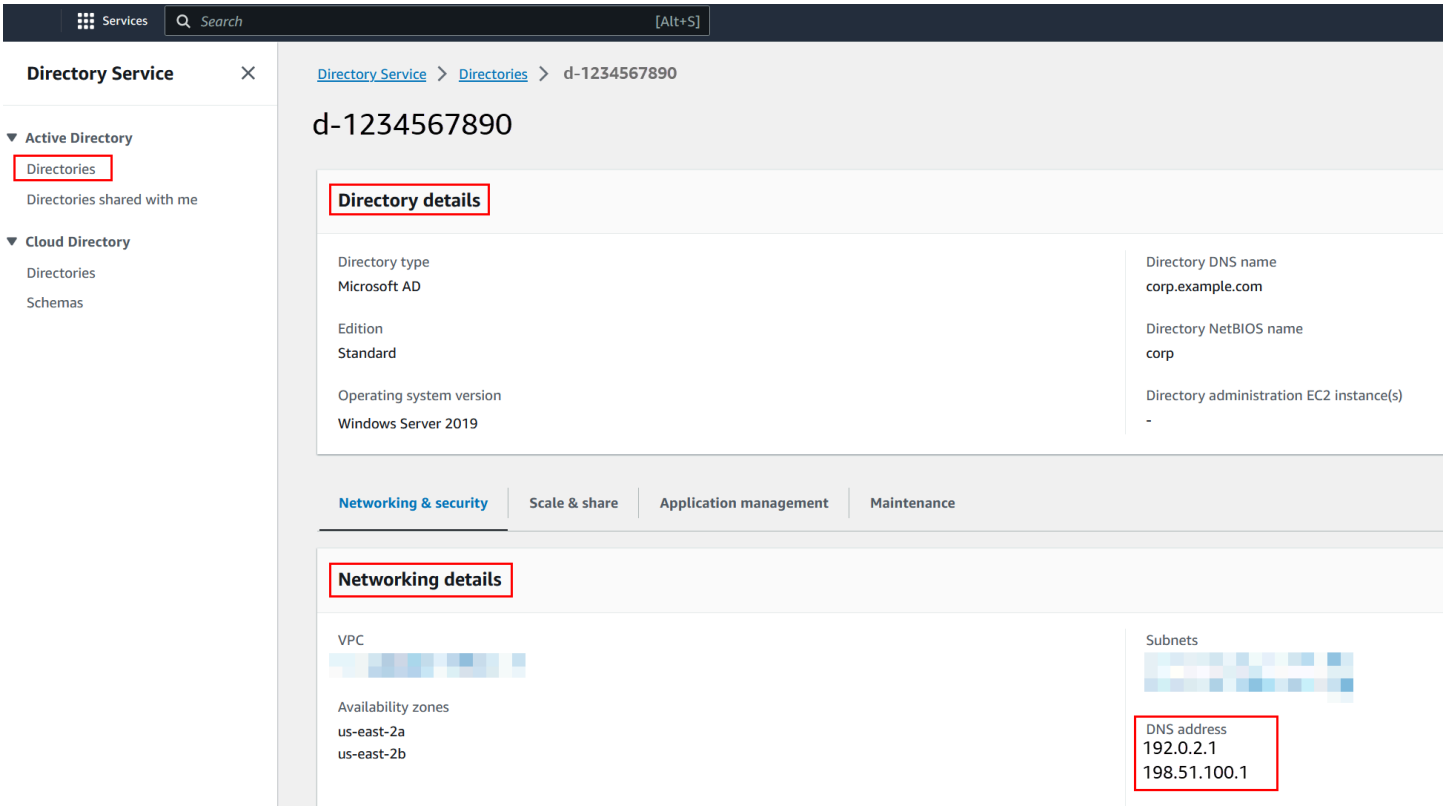
5. 在命名、檢閱和建立頁面上，針對角色名稱輸入角色名稱。您將需要此角色名稱來連接到 EC2 執行個體。
6. (選用) 您可以在描述欄位中提供 IAM 執行個體設定檔的描述。
7. 選擇建立角色。
8. 返回啟動執行個體頁面，然後選擇 IAM 執行個體設定檔旁的重新整理圖示。剛剛建立的 IAM 執行個體設定檔應顯示在 IAM 執行個體設定檔下拉式清單中。選擇這個新的設定檔並將其餘設定保留為預設值。

16. 選擇啟動執行個體。

手動將 Amazon EC2 Windows 實例加入到您的 AWS 受管 Microsoft AD 活動目錄

若要將現有的 Amazon EC2 執行個體手動加入 AWS 受管 Microsoft ADActive Directory，必須使用中指定的參數啟動執行個體[將 Amazon EC2 Windows 執行個體無縫加入您的 AWS 受管 Microsoft AD Active Directory](#)。

您將需要 AWS 管理 Microsoft AD DNS 伺服器的 IP 位址。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。



將視窗執行個體加入 AWS 管理 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。

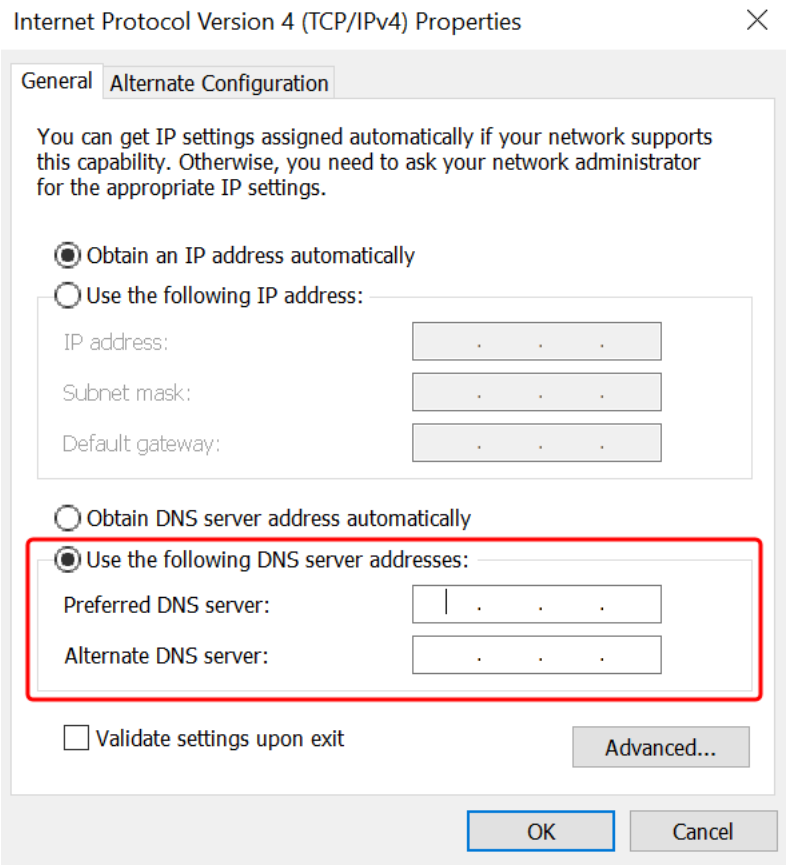
   a. 開啟 Network Connections (網路連線)。

   > **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 [使用下列 DNS 伺服器位址]，將 [慣用的 DNS 伺服器] 和 [替代 DNS 伺服器位址] 變更為您 AWS 受管理的 Microsoft AD 提供的 DNS 伺服器的 IP 位址，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 [成員屬於] 欄位中，選取 [網域]，輸入 AWS 受管理的 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之帳戶的使用者名稱和密碼。如需委派這些權限的詳細資訊，請參閱「委派 AWS 受管 Microsoft AD 目錄加入權限」。

> **Note**
>
> 您可以輸入網域的完整名稱或 NetBIOS 名稱，接著輸入反斜線 (\)，然後輸入使用者名稱。用戶名將是管理員。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 受管理的 Microsoft AD Active Directory 網域，您可以從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。使用中的目錄管理工具可用來建立使用者和群組。如需詳細資訊，請參閱 安裝適用於 AWS 受管理 Microsoft AD 的活動目錄管理工具。

> **Note**
>
> 您也可以使用亞馬遜路線 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，請參閱將目錄服務的 DNS 解析與整合 Amazon Route 53 Resolver和將輸出 DNS 查詢轉送至您的網路。

將 Amazon EC2 Linux 執行個體無縫加入您的 AWS 受管 Microsoft AD 活動目錄

此程序將 Amazon EC2 Linux 執行個體無縫連接到您的 AWS 受管 Microsoft AD 活動目錄。如果您需要跨多個 AWS 帳戶執行無縫網域加入，您可以選擇性地選擇啟用目錄共用。

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 之前的發行版不支援無縫域加入功能。

如需將 Linux 執行個體無縫加入 AWS 管理 Microsoft AD 活動目錄的程序示範，請參閱下列 YouTube 影片。

Amazon EC2 for Linux 無縫 AD 域加入示範

必要條件

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

您可以無縫加入 Linux 電腦到 AWS 管理 Microsoft AD 活動目錄域。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。

若要將電腦加入網域所需的最低權限委派帳戶，您可以執行下列 PowerShell 命令。您必須從已加入域並安裝了 安裝適用於 AWS 受管理 Microsoft AD 的活動目錄管理工具 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。此命 PowerShell 令會設定權限，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。

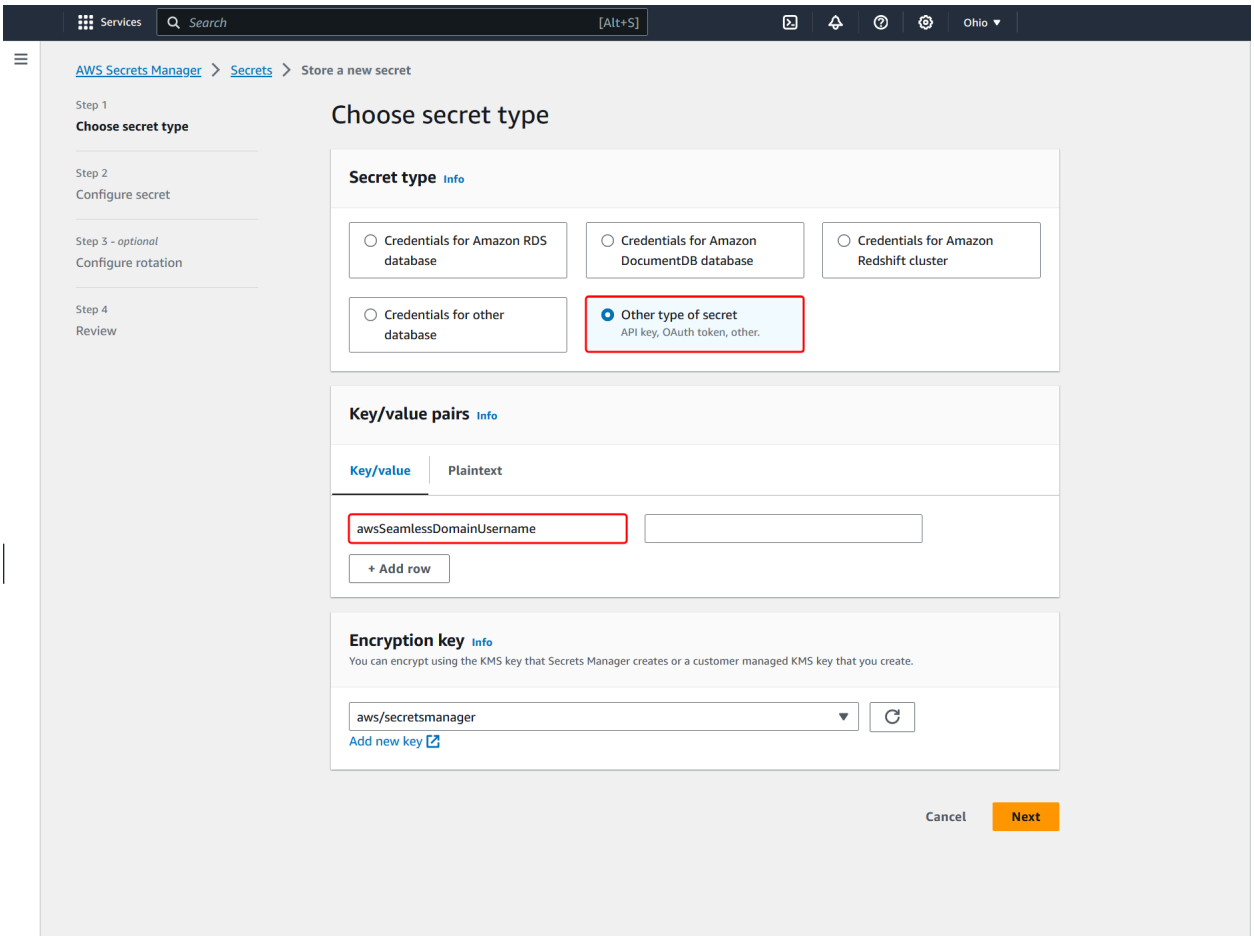
建立儲存域服務帳戶的機密

您可以用 AWS Secrets Manager 來儲存網域服務帳戶。

建立機密並儲存域服務帳戶資訊

1. 請登入 AWS Management Console 並開啟 AWS Secrets Manager 主控台，網址為 https://console.aws.amazon.com/secretsmanager/。
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「其他類型的機密」。
   b. 在「鍵/值配對」下，執行下列操作：
      i. 在第一個方塊中，輸入 **awsSeamlessDomainUsername**。在同一列的下一個方塊中，輸入服務帳戶的使用者名稱。例如，如果您之前使用了該 PowerShell 命令，則服務帳戶名稱將是**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] 底下，保留預設值`aws/secretsmanager`。 AWS Secrets Manager 當您選擇此選項時，一律會加密密碼。您也可以選擇您建立的金鑰。

> **Note**
>
> 有相關的費用 AWS Secrets Manager，具體取決於您使用的秘密。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/secretsmanager`的 AWS 受管理金鑰來免費加密您的密鑰。如果您建立自己的 KMS 金鑰來加密密碼，請按照目前的 AWS 費 AWS KMS 率向您收費。如需詳細資訊，請參閱 AWS Key Management Service 定價。

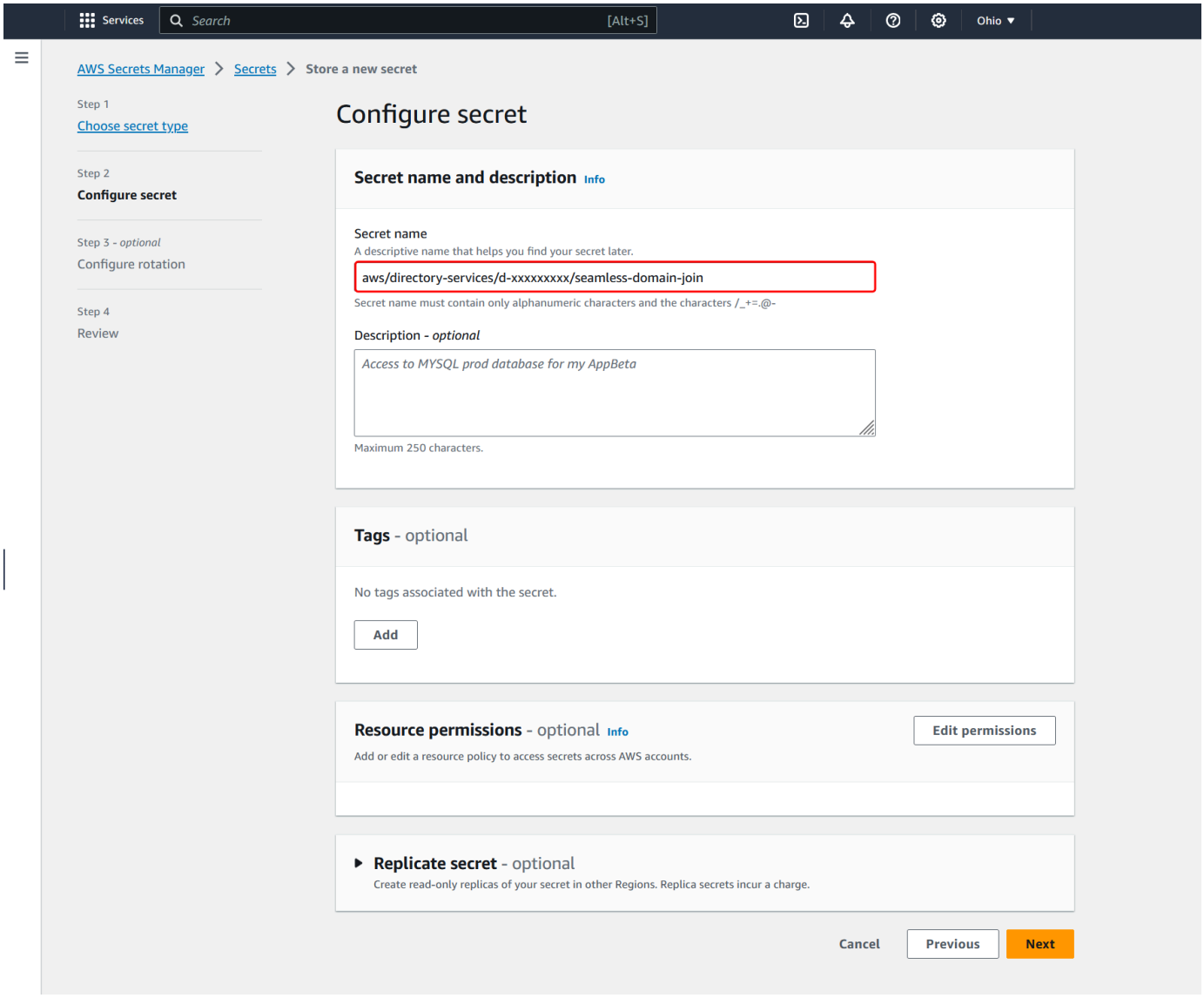
v. 選擇下一步。

4. 在密碼名稱下，使用下列格式輸入包含您目錄 ID 的密碼名稱，並以您的目錄識別碼取代 *d-xxxxxxxxx*：

```
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-xxxxxxxxx* 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。
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。

建立必要的 IAM 政策和角色

使用下列先決條件步驟來建立自訂政策，允許您的 Secrets Manager 無縫網域加入密碼 (您之前建立) 的唯讀存取權限，以及建立新的 LinuxEC2 DomainJoin 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 政策權限的使用者身分登入。 AWS Management Console 前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在功能窗格的 [存取管理] 中，選擇 [原則]。
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**
>
> 請確定您將 [區域] 和 [資源 ARN] 取代為您先前建立的密碼的實際 [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。

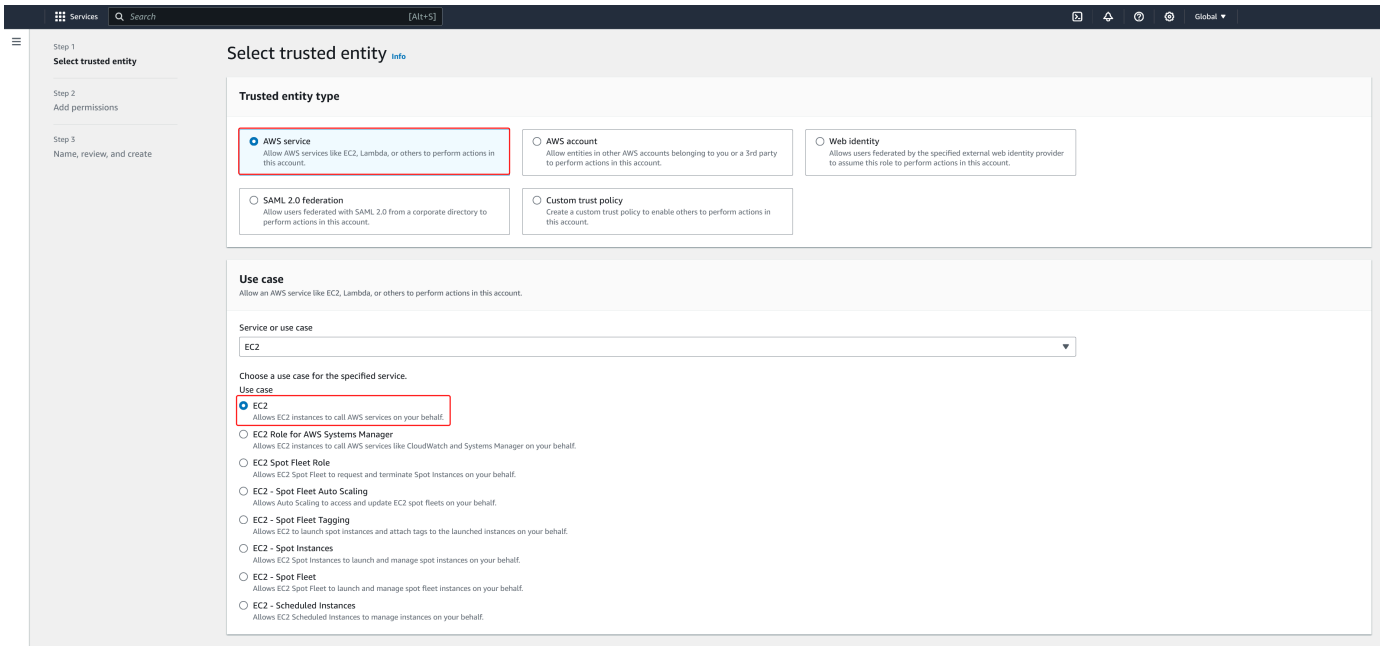
> **Note**
>
> 我們建議您為每個機密建立一個政策。這樣做可以確保執行個體只能存取適當的機密，並在執行個體受到入侵時將影響降至最低。

建立角色 DomainJoin

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。

若要建立 Linux 角DomainJoin 色

1. 以具有建立 IAM 政策權限的使用者身分登入。 AWS Management Console 前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在功能窗格的 [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] 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. 新增上面列出的三個策略之後，選取 [建立角色]。

> **Note**
>
> AmazonSSM DirectoryServiceAccess 提供將執行個Active Directory體加入至管理的權限。 AWS Directory Service亞馬遜 SSM ManagedInstanceCore 提供了使用該服務所需的最低權限。 AWS Systems Manager 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. 輸入新角色的名稱，例如**LinuxEC2DomainJoin**，在「角色名稱」欄位中輸入您偏好的名稱。
8. (選用) 針對 Role description (角色描述)，輸入描述。
9. (選擇性) 在「步驟 3：新增標籤」下方選擇「新增標籤」以新增標籤。標籤鍵值配對用於組織、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

現在您已經設定了所有先決條件任務，您可以使用下列程序順暢地加入 EC2 Linux 執行個體。

無縫加入您的 Linux 執行個體

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 從導覽列的 [區域] 選取器中，選擇與現有目錄 AWS 區域 相同的選項。
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，輸入您想要用於 Linux 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 機器映像) 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 代理程式) 2.3.1644.0 或更高版本。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 會在將 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格式為 EC2AMAZ-*XXXXXX* 格式。如需有關的詳細資訊`aws:domainJoin`，請參閱AWS Systems Manager 使用指南中的指AWS Systems Manager 令文件外掛程式參考。

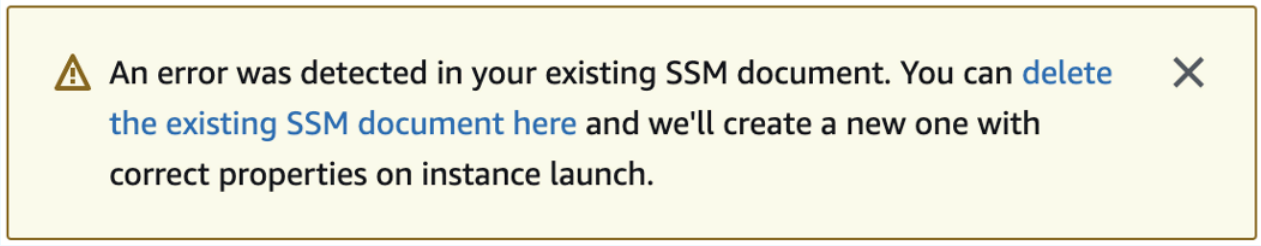
7. 在執行個體類型區段中，從執行個體類型下拉式清單中選擇您要使用的執行個體類型。
8. 在金鑰對 (登入) 區段中，您可以選擇建立新金鑰對或從現有金鑰對中進行選擇。若要建立新的金鑰對，請選擇建立新金鑰對。輸入金鑰對的名稱，然後選取金鑰對類型和私有金鑰檔案格式的選項。若要將私有金鑰儲存為可與 OpenSSH 搭配使用的格式，請選擇 .pem。若要將私有金鑰儲存為可與 PuTTY 搭配使用的格式，請選擇 .ppk。選擇建立金鑰對。您的瀏覽器會自動下載私有金鑰檔案。將私有金鑰檔案存放在安全的地方。

> **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 地址的詳細資訊，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的Amazon EC2 執行個體 IP 地址一節。
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 啟動精靈識別具有未預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
>
> - 如果您之前已編輯過 SSM 文件，且預期會有屬性，請選擇 [關閉] 並繼續啟動 EC2 執行個體而不進行任何變更。
> - 選取此處刪除現有 SSM 文件連結以刪除 SSM 文件。這將允許創建具有正確屬性的 SSM 文檔。SSM 文件會在您啟動 EC2 執行個體時自動建立。

15. 對於 IAM 執行個體設定檔，請在先決條件部分步驟 2：建立 LinuxEC2 DomainJoin 角色中選擇先前建立的 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 AWS 受管 Microsoft AD 活動目錄

除了 Amazon EC2 Windows 執行個體之外，您還可以將某些 Amazon EC2 Linux 執行個體加入您的 AWS 受管 Microsoft AD 活動目錄。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
- 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 執行個體加入您的 AWS 管理 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. 將 Linux 執行個體設定為使用 AWS Directory Service提供之 DNS 伺服器的 DNS 伺服器 IP 位址。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 受管 Microsoft AD 目錄加入權限」。

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，請透過任何安全殼層用戶端連線至該執行個體，然後執行下列步驟將 AWS 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. 將 Linux 執行個體設定為使用 AWS Directory Service提供之 DNS 伺服器的 DNS 伺服器 IP 位址。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 受管 Microsoft AD 目錄加入權限」。

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，請透過任何安全殼層用戶端連線至該執行個體，然後執行下列步驟將 AWS 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. 將 Linux 執行個體設定為使用 AWS Directory Service提供之 DNS 伺服器的 DNS 伺服器 IP 位址。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

example.com 網域中具有網域加入權限之帳戶的 SAM AccountName。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 受管 Microsoft AD 目錄加入權限」。

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，請透過任何安全殼層用戶端連線至該執行個體，然後執行下列步驟將 AWS 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，請參閱如何將靜態 DNS 伺服器指派給 AWS 知識中心中的私有 Amazon EC2 執行個體，以取得針對特定 Linux 發行版和版本設定永久性 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

.com 網域AccountName 中具有網域加入權限的 SAM。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 受管 Microsoft AD 目錄加入權限」。

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. 重新啟動執行個體之後，請透過任何安全殼層用戶端連線至該執行個體，然後執行下列步驟將 AWS 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. 將 Linux 執行個體設定為使用 AWS Directory Service提供之 DNS 伺服器的 DNS 伺服器 IP 位址。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

example.com 網域中具有網域加入權限之帳戶的 SAM AccountName。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 受管 Microsoft AD 目錄加入權限」。

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，請透過任何安全殼層用戶端連線至該執行個體，然後執行下列步驟將 AWS 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
```

識別碼對應

識別碼對應可以透過兩種方法執行，以維持 UNIX/Linux 使用者識別碼 (UID) 與群組識別碼 (GID) 與視窗與Active Directory安全性識別碼 (SID) 身分之間的統一體驗。

1. 集中式
2. 分散式

> **Note**
>
> 中的集中式使用者身分對應Active Directory需要可攜式作業系統介面或 POSIX。

集中使用者身分對應

Active Directory或其他輕量型目錄存取通訊協定 (LDAP) 服務提供 UID 和 GID 給 Linux 使用者。在中 Active Directory，這些識別碼會儲存在使用者屬性中：

- UID-使用者名稱 (字串)
- UID 號碼-Linux 使用者識別碼編號 (整數)
- GID 號碼-Linux 群組識別碼 (整數)

若要將 Linux 執行個體設定為使用來源的 UID 和 GIDActive Directory，請在 sssd.conf 檔案`ldap_id_mapping = False`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

分佈式用戶身份映射

如果Active Directory沒有 POSIX 擴充功能，或者您選擇不集中管理身分對應，Linux 可以計算 UID 和 GID 值。Linux 會使用使用者的唯一安全性識別碼 (SID) 來維持一致性。

若要設定分散式使用者識別碼對應，請`ldap_id_mapping = True`在 sssd.conf 檔案中進行設定。

Connect 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，回應會類似下列內容：

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 執行個體加入您的 AWS 受管 Microsoft AD 活動目錄

您可以使用 Winbind 服務手動將您的 Amazon EC2 Linux 執行個體加入到 AWS 受管 Microsoft AD 活動目錄網域。這可讓您現有的內部部署作用中目錄使用者在存取加入您 AWS 受管理的 Microsoft AD 活動目錄的 Linux 執行個體時，使用他們的作用中目錄認證。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
- 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 執行個體加入您的 AWS 管理 Microsoft AD 活動目錄

> **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，請參閱如何將靜態 DNS 伺服器指派給 AWS 知識中心中的私有 Amazon EC2 執行個體，以取得針對特定 Linux 發行版和版本設定永久性 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
```

填寫您的活動目錄域環境信息，如下面的例子所示：

```
[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 受管 Microsoft AD 目錄加入權限」。

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，請參閱如何將靜態 DNS 伺服器指派給 AWS 知識中心中的

私有 Amazon EC2 執行個體，以取得針對特定 Linux 發行版和版本設定永久性 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

.com 網域AccountName 中具有網域加入權限的 SAM。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 受管 Microsoft AD 目錄加入權限」。

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，請參閱如何將靜態 DNS 伺服器指派給 AWS 知識中心中的私有 Amazon EC2 執行個體，以取得針對特定 Linux 發行版和版本設定永久性 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
   ```

   ```
   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 受管 Microsoft AD 目錄加入權限」。

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。)

Connect 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，回應會類似下列內容：

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%
```

手動將 Amazon EC2 Mac 執行個體加入您的 AWS 受管 Microsoft AD 活動目錄

此程序以手動方式將 Amazon EC2 Mac 執行個體加入您的 AWS 受管 Microsoft AD 活動目錄。

必要條件

- 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 Linux 執行個體使用者指南中的啟動 Mac 執行個體。
- 我們建議您為 AWS 管理 Microsoft AD 活動目錄創建一個 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 伺服器來解析其網域名稱。如需詳細資訊，請參閱建立 DHCP 選項集。

> **Note**
>
> 專用主機的定價會因您選取的付款選項而有所不同。如需詳細資訊，請參閱 Amazon EC2 Linux 執行個體使用者指南中的定價和計費。

手動加入 Mac 執行個體

1. 使用下列 SSH 指令連線至您的 Mac 執行個體。如需連線至 Mac 執行個體的詳細資訊，請參閱：Connect 至 Mac 執行個體。

   ```
   ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
   ```

2. 連線到 Mac 執行個體後，請使用下列指令為 *ec2 ###*帳戶建立密碼：

   ```
   sudo passwd ec2-user
   ```

3. 在指令列中出現提示時，請提供 *ec2 #####*的密碼。您可以按照 Amazon EC2 Linux 執行個體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* 指令，將您的 Mac 執行個體加入 AWS 管理 Microsoft AD 活動目錄網域。請務必將網域名稱、電腦名稱和組織單位取代為 AWS 受管理的 Microsoft AD Active Directory 網域資訊。如需詳細資訊，請參閱在 Apple 網站上的 Mac 上「目錄工具程式」中設定網域存取。

   > **Warning**
   >
   > 電腦名稱不應包含連字號。連字號可能會阻止綁定到 AWS 受管理的 Microsoft AD 活動目錄。

   ```
   sudo dsconfigad -add domainName -computer computerName -username Username -
   ou "Your-AWS-Delegated-Organizational-Unit"
   ```

   下列範例是在名為**example.com**網域的 Mac 執行個體上加入系統管理使用者時，命令**myec2mac01**的外觀應如下：

   ```
   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受 AWS 管理的 Microsoft AD 活動目錄網域加入成功：

   ```
   dsconfigad -show
   ```

您已成功加入您的 Mac 執行個體到 AWS 管理 Microsoft AD 活動目錄。您現在可以使用 AWS 管理 Microsoft AD 活動目錄憑據登錄到 Mac 實例。

當您第一次登入 Mac 執行個體時，應該會提供您以「其他」使用者身分登入的選項。此時，您可以使用活動目錄網域認證登入 Mac 執行個體。如果您在完成這些步驟後，在登入畫面上沒有提供「其他」，請以 ec2-user 身分登入，然後登出。

若要透過網域使用者使用圖形化使用者介面登入，請依照 Amazon EC2 Linux 執行個體使用者指南中的 Connect 到執行個體的圖形化使用者介面 (GUI) 中的步驟進行操作。

委派 AWS 受管 Microsoft AD 目錄加入權限

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 Microsoft Active AWS Directory 的 Directory Service，系統管理員和AWS 委派伺服器系統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。

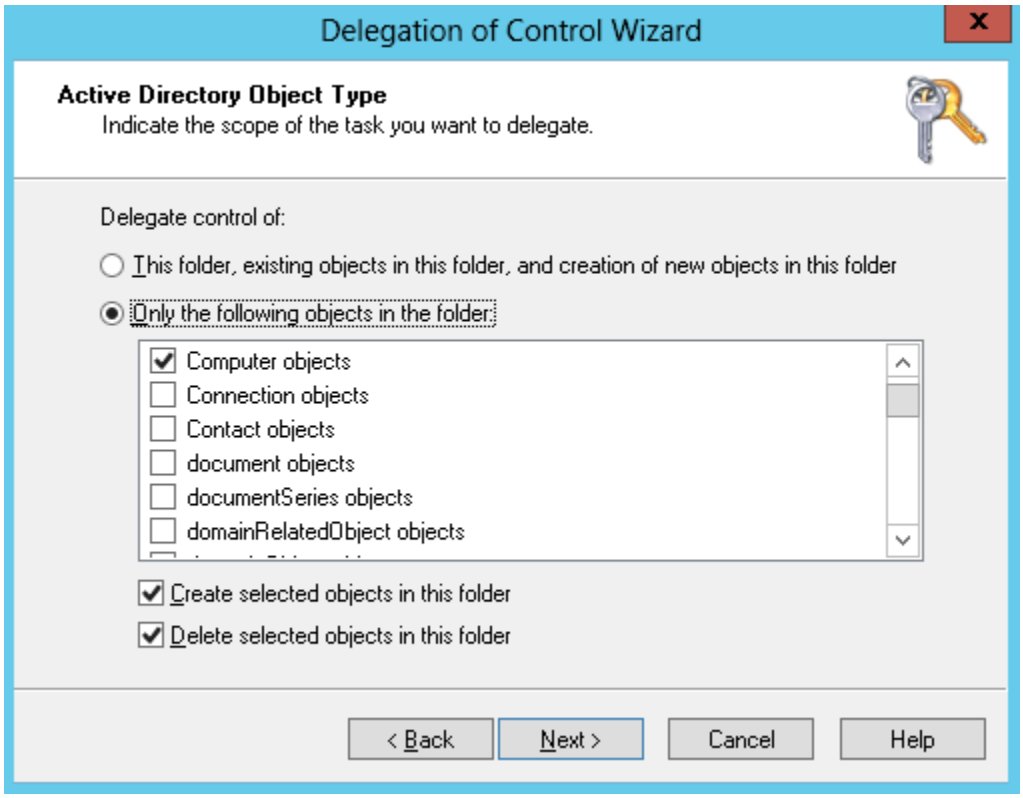
委派 AWS 受管理 Microsoft AD 的加入權限

1. 開啟 Active Directory User and Computers (Active Directory 使用者和電腦)，在導覽樹狀目錄中選取具有您 NetBIOS 名稱的組織單位 (OU)，然後選取 Users (使用者) OU。

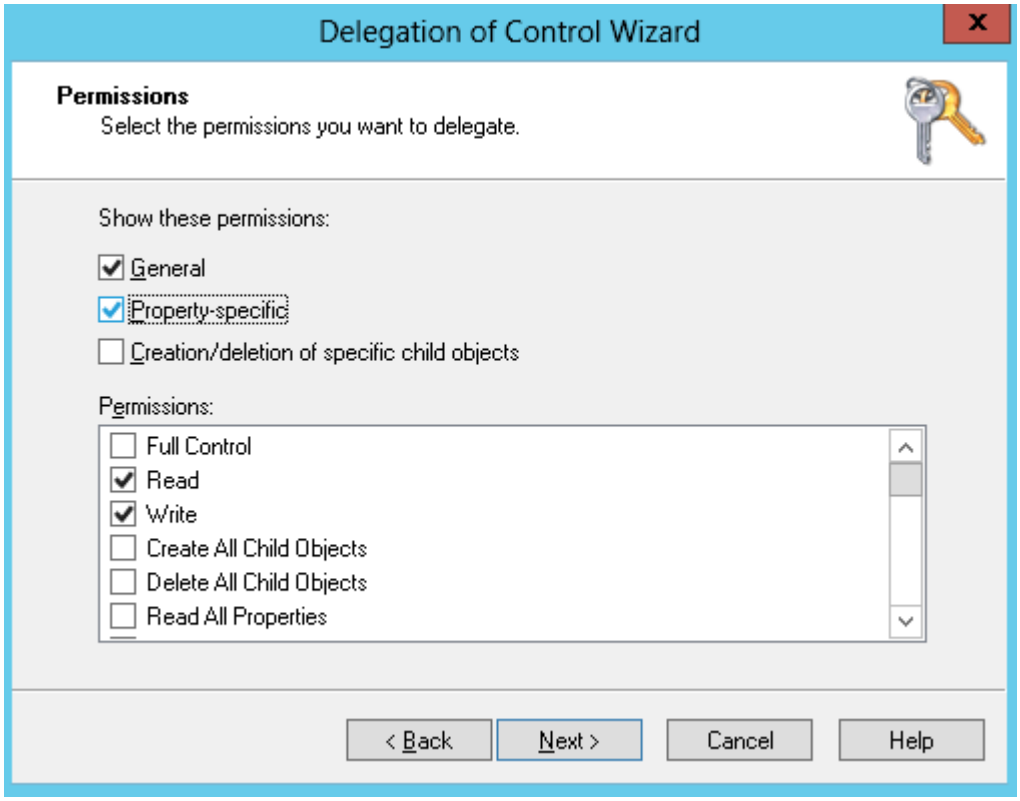
   > **Important**
   >
   > 當您啟動 Microsoft Active AWS Directory 的 Directory Service 時， AWS 會建立包含所有目錄物件的組織單位 (OU)。此 OU 有您在建立目錄時所輸入的 NetBIOS 名稱，位於根網域中。網域根目錄擁有及管理 AWS。您不能變更根網域本身；因此，您必須在具有您 NetBIOS 名稱的 OU 內建立 **`Joiners`** 群組。

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 DHCP 選項集

AWS 建議您為 AWS Directory Service 目錄建立 DHCP 選項集，並將 DHCP 選項設定指派給目錄所在的 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. 前往 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所提供目錄之 DNS 伺服器的 IP 位址。

> **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. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇您的 VPC
3. 選取 VPC，然後選擇動作、編輯 DHCP 選項集。

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。

管理 AWS Managed Microsoft AD 中的使用者和群組

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，您必須使用已加入您 AWS Directory Service 目錄的執行個體 (來自內部部署或 EC2)，並以具有建立使用者和群組之權限的使用者身分登入。您還需要在 EC2 執行個體上安裝 Active Directory 工具，才可在 Active Directory 使用者和電腦嵌入的狀態下，新增您的使用者和群組。

您可以從 AWS Directory Service 管理主控台使用預先安裝的 Active Directory 管理工具部署預先設定的 EC2 執行個體。如需更多詳細資訊，請參閱 在受管理的 Microsoft AD 中啟動目錄 AWS 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 受管 Microsoft AD 活動目錄。

> **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

- 安裝適用於 AWS 受管理 Microsoft AD 的活動目錄管理工具
- 建立使用者
- 刪除使用者
- 重設使用者密碼
- 建立群組
- 將使用者新增至群組

安裝適用於 AWS 受管理 Microsoft AD 的活動目錄管理工具

若要從 Amazon EC2 Windows 伺服器執行個體管理您的作用中目錄，您需要在執行個體上安裝活動目錄網域服務和使用中目錄輕量型目錄服務工具。請使用下列程序在 EC2 Windows 伺服器執行個體上安裝這些工具。

必要條件

開始此程序之前，請先完成下列步驟：

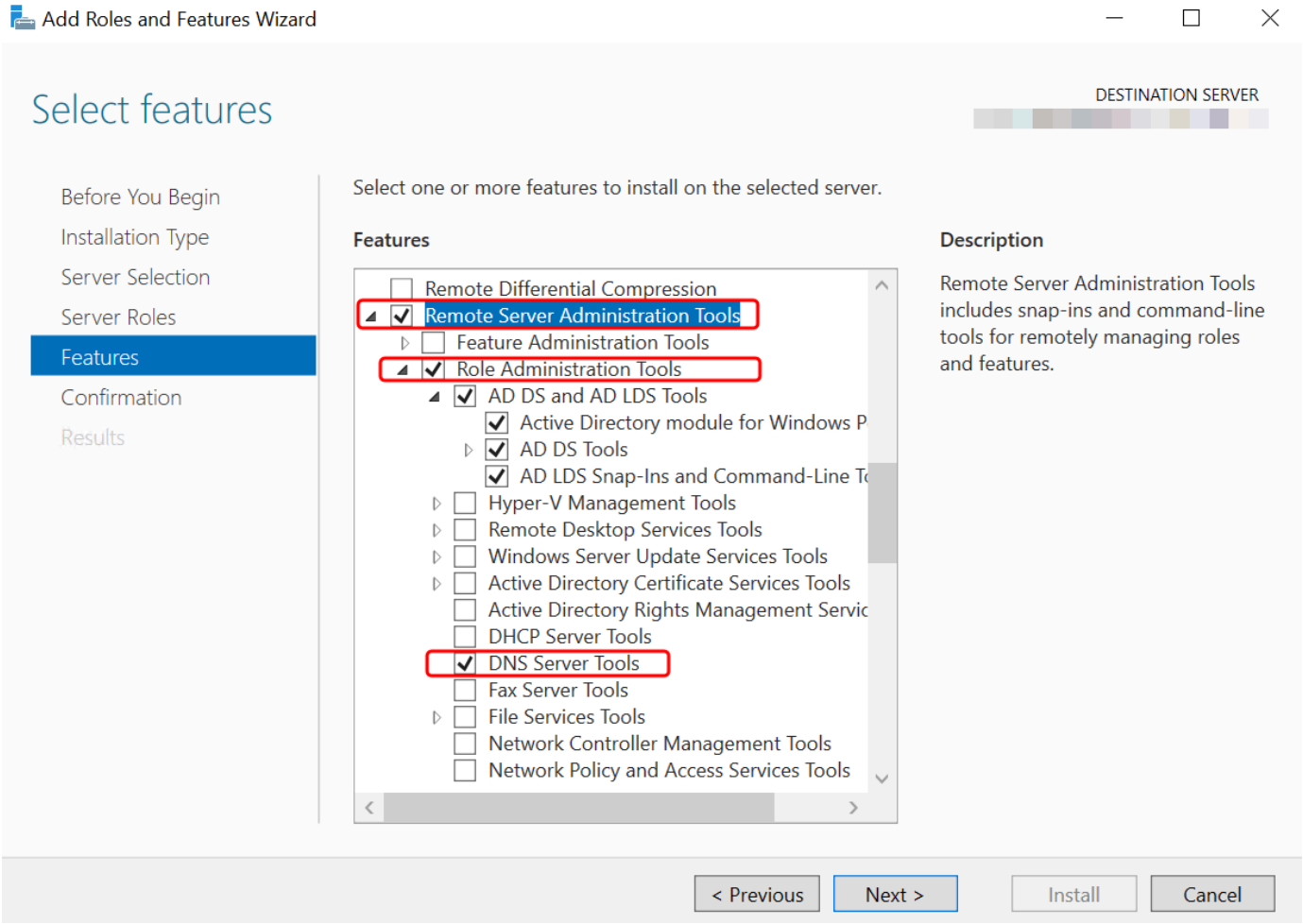
1. 創建一個 AWS 託管 Microsoft AD 活動目錄。如需詳細資訊，請參閱 創建您的 AWS 託管 Microsoft AD Active Directory。
2. 啟動並加入 EC2 視窗伺服器執行個體到您的 AWS 受管 Microsoft AD 活動目錄。EC2 執行個體需要下列政策來建立使用者和群組：**AWSSSMManagedInstanceCore**和**AmazonSSMDirectoryServiceAccess**。如需詳細資訊，請參閱 在受管理的 Microsoft AD 中啟動目錄 AWS 管理執行個體 Active Directory 及 將 Amazon EC2 Windows 執行個體無縫加入您的 AWS 受管 Microsoft AD Active Directory。
3. 您將需要您的活動目錄域管理員的憑據。這些認證是在建立受 AWS 管理的 Microsoft AD 時建立的。如果您遵循中的程序創建您的 AWS 託管 Microsoft AD Active Directory，您的管理員使用者名稱會包含您的 NetBIOS 名稱、**corp\admin**。

在 EC2 Windows 伺服器執行個體上安裝作用中目錄管理工具

若要在 EC2 Windows 伺服器執行個體上安裝作用中目錄管理工具

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 安全性」對話方塊中，複製 Windows 伺服器電腦的本機系統管理員身分證明以進行登入。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，則**corp\admin**會是使用者名稱創建您的 AWS 託管 Microsoft AD Active Directory。
7. 登入 Windows Server 執行個體之後，請選擇 [伺服器管理員]，從 [開始] 功能表中開啟 [伺服器管理員]。

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，會選取用於Windows PowerShell、AD DS 工具和 AD LDS 嵌入式管理單元和命令列工具的Active Directory模組。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。

在 EC2 Windows 伺服器執行個體上安裝活動目錄管理工具的替代方法

- 以下是安裝活動目錄管理工具的其他一些方法：
  - 您可以選擇使用安裝活動目錄管理工具Windows PowerShell。例如，您可以使用 PowerShell 提示安裝 Active Directory 遠端管理工具`Install-WindowsFeature RSAT-ADDS`。如需詳細資訊，請參閱 Microsoft 網站WindowsFeature上的安裝。
  - 您也可以啟動已安裝 Active Directory 網域服務和 Active Directory 輕量型目錄服務工具的目錄管理 EC2 執行個體，請遵循中的程序在受管理的 Microsoft AD 中啟動目錄 AWS 管理執行個體 Active Directory。 AWS Management Console

建立使用者

請使用下列步驟以在加入您 AWS Managed Microsoft AD 目錄的 EC2 執行個體上建立使用者。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。

您可以使用下列任何一種方法來建立使用者：

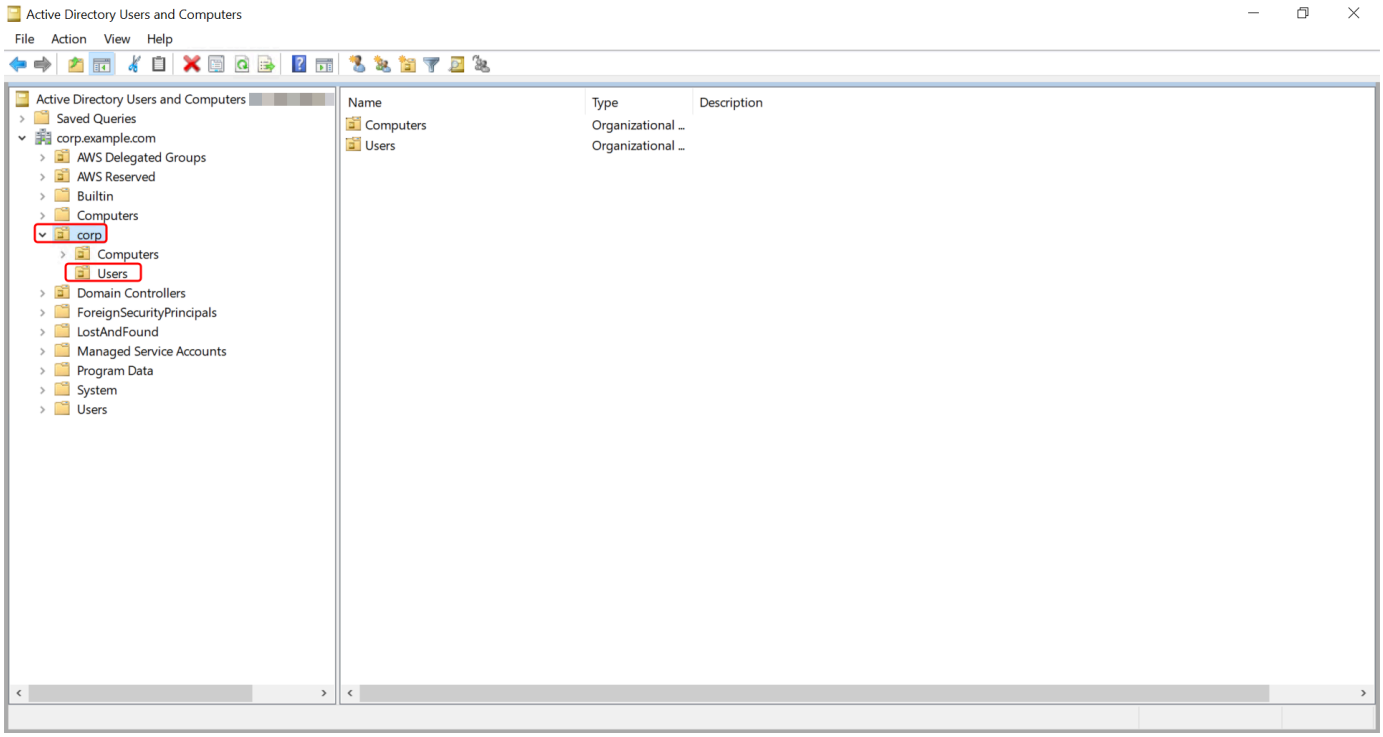
- Active Directory管理工具
- Windows PowerShell

使用Active Directory管理工具建立使用者

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「使用中目錄使用者和電腦」工具。在 Windows 系統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. 在目錄樹狀結構中，選取您要儲存使用者的目錄 NetBIOS 名稱 OU 下的 OU (例如，**corp\Users**)。如需中目錄所使用 OU 結構的詳細資訊 AWS，請參閱什麼被創建與 AWS 管理 Microsoft AD 活動目錄。



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。

在中建立使用者 Windows PowerShell

1. 以系統管理員身分 Connect 至加入您Active Directory網域的Active Directory執行個體。
2. 打開 Windows PowerShell.
3. 輸入以下指令，將使**`jane.doe`**用者名稱取代為您要建立的使用者名稱。系統會提示您Windows PowerShell提供新使用者的密碼。如需Active Directory密碼複雜性需求的詳細資訊，請參閱Microsoft文件。有關 New AdUser 命令的更多信息，請參閱Microsoft文檔。

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

刪除使用者

請使用下列程序來刪除加入 AWS 受管理 Microsoft AD 的使用者Active Directory。

您可以使用下列任何一種方法來刪除使用者：

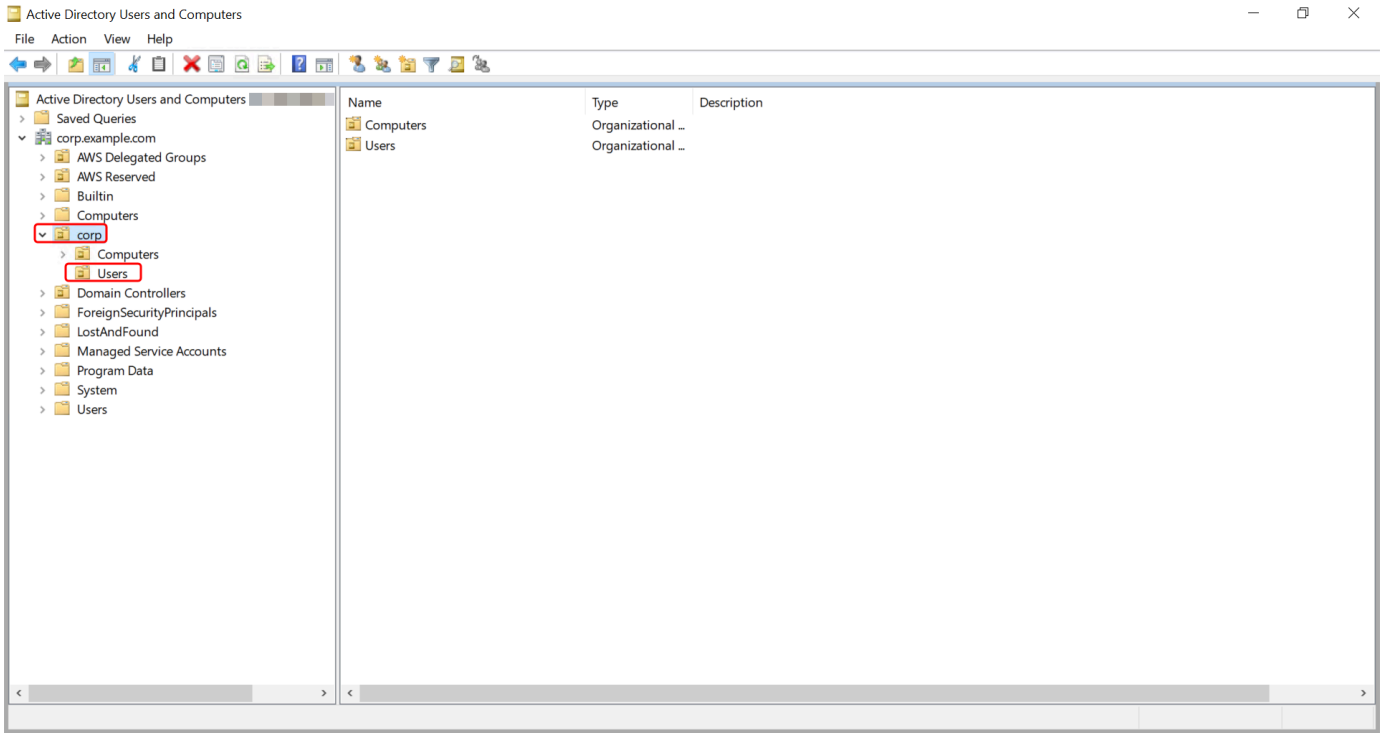
- Active Directory管理工具
- Windows PowerShell

使用Active Directory管理工具刪除使用者

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「使用中目錄使用者和電腦」工具。在 Windows 系統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. 在目錄樹狀結構中，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。

刪除中的使用者 Windows PowerShell

1. 以系統管理員身分 Connect 至加入您Active Directory網域的Active Directory執行個體。
2. 打開 Windows PowerShell.
3. 輸入以下指令，以您要刪除的使**jane.doe**用者名稱取代使用者名稱的使用者名稱。有關刪除 AdUser 命令的更多信息，請參閱文檔。Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

AD 資源回收筒考量

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 AD 資源回收筒：瞭解、實作、最佳做法和疑難排解Microsoft的詢問目錄服務小組部落格。

重設使用者密碼

使用者必須遵守中定義的密碼策略Active Directory。有時候，這可以得到最好的用戶，包括Active Directory管理員，他們忘記了他們的密碼。發生這種情況時，如果使用者位於 AWS 受管理的 Microsoft AD，您可以 AWS Directory Service 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「管理資 AWS Directory Service 源存取權限概觀」。

您可以為您Active Directory的任何使用者重設密碼，但下列情況例外：

- 您可以在組織單位 (OU) 內重設任何使用者的密碼，這些使用者是以您Active Directory建立時所使用的 NetBIOS 名稱為基礎。例如，如果您遵循 NetBIOS 名稱中的程序將是 CORP，而創建您的 AWS 託管 Microsoft AD Active Directory您可以重設的使用者密碼將是公司/使用者 OU 的成員。
- 您無法重設 OU 以外的任何使用者的密碼，該使用者的密碼是根據您Active Directory在建立時使用的 NetBIOS 名稱。例如，您無法在AWS 保留的 OU 中重設使用者的密碼。如需 AWS 受管理 Microsoft AD 之 OU 結構的詳細資訊，請參閱什麼被創建與 AWS 管理 Microsoft AD 活動目錄。

如需有關在 AWS 受管理 Microsoft AD 中重設密碼時如何套用密碼原則的詳細資訊，請參閱如何套用密碼原則。

您可以使用下列任何一種方法來重設使用者密碼：

- AWS Management Console
- AWS CLI
- Windows PowerShell

重設中的使用者密碼 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Active Directory在清單中選取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] 對話方塊的 [使用者名稱] 中，輸入需要變更密碼之使用者的使用者名稱。
4. 在新密碼和確認密碼中輸入密碼，然後選擇重設密碼。

重設使用者密碼 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，並以您的目錄 ID 和所需的認證取代Active Directory目錄 ID **jane.doe**、使用者名稱和密碼**P@ssw0rd**。如需更多資訊，請參閱〈AWS CLI 指令參考〉reset-user-password中的〈

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

重設使用者密碼 Windows PowerShell

1. 以系統管理員身分 Connect 至加入您Active Directory網域的Active Directory執行個體。
2. 打開 Windows PowerShell.
3. 輸入下列指令**jane.doe**，以您的目錄 ID 和所需的認證取代使用者名稱、Active Directory目錄 ID 和密碼**P@ssw0rd**。如需詳細資訊，請參閱重設-DS UserPassword 指令程式。

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

建立群組

使用下列程序建立安全群組，其中包含加入 AWS 受管 Microsoft AD 目錄的 EC2 執行個體。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。

您也可以使用Windows PowerShell指令建立群組。如需詳細資訊，請參閱新 AD群組中的視窗伺服器 2022 PowerShell 文件。

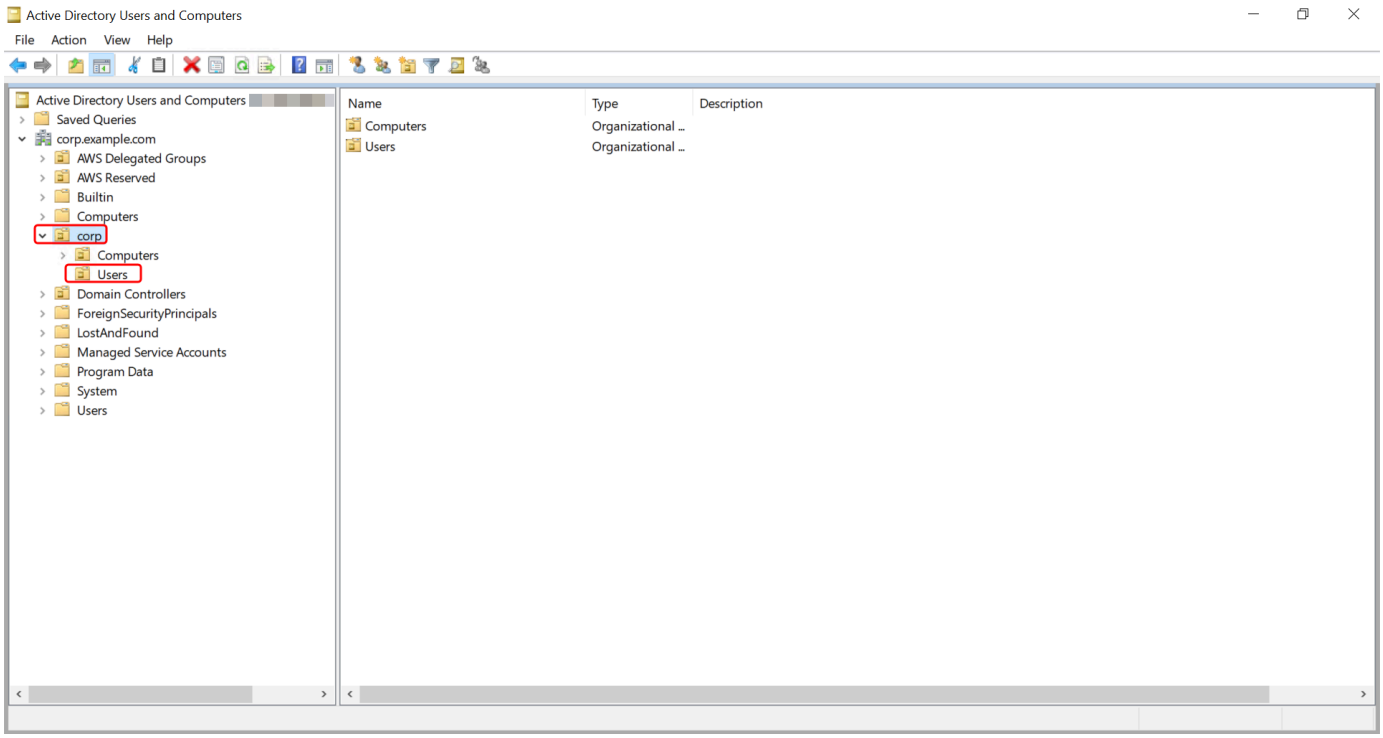
建立群組

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")。如需中目錄所使用 OU 結構的詳細資訊 AWS，請參閱什麼被創建與 AWS 管理 Microsoft AD 活動目錄。



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。

將使用者新增至群組

請使用下列步驟以在加入您 AWS Managed Microsoft AD 目錄的 EC2 執行個體上將使用者新增至安全群組。

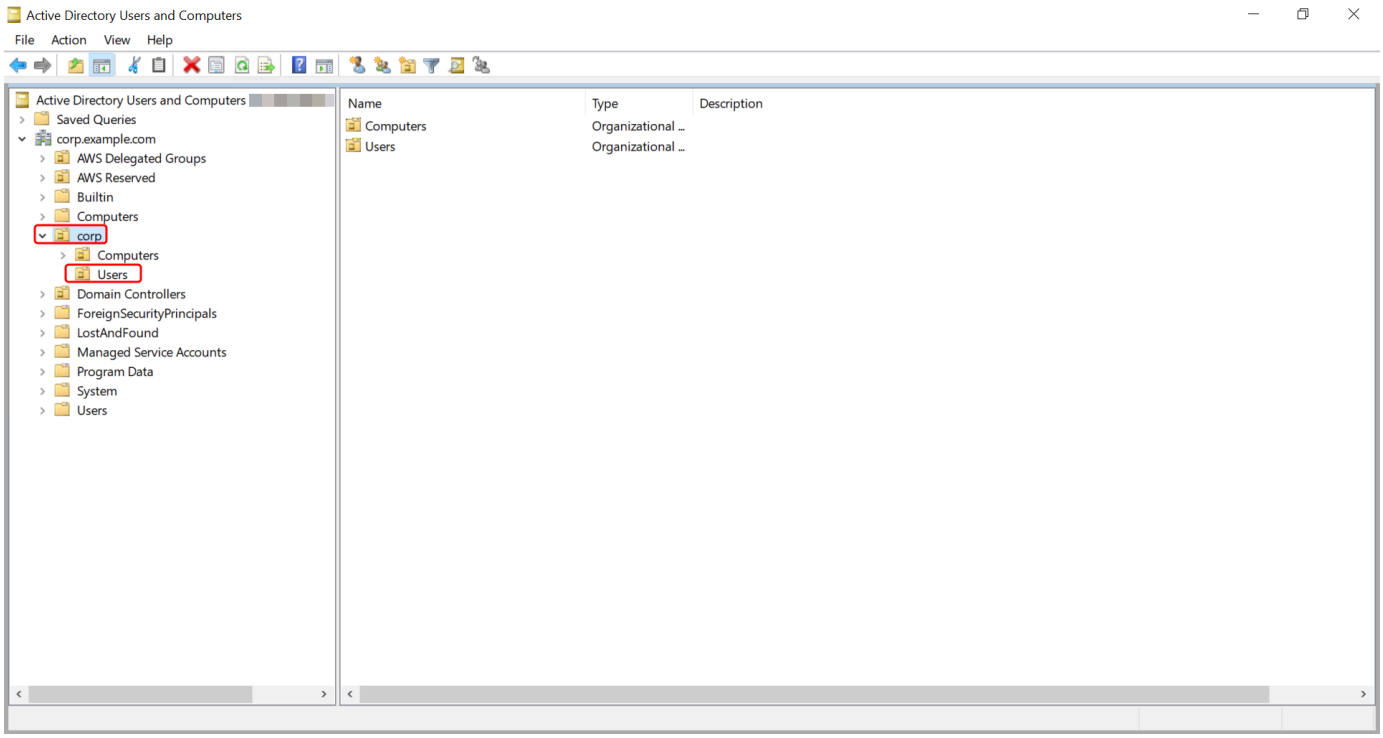
將使用者新增至群組

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. 在 [輸入要選取的物件名稱] 中，輸入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。

Connect 到您現有的活動目錄基礎結構

本節說明如何設定AWS受管理的 Microsoft AD 與您現有的使用中目錄基礎結構之間的信任關係。

主題

建立信任關係

您可以設定 Microsoft Active Directory 的 AWS Directory Service 與自我管理 (內部部署) 目錄，以及 AWS 雲端中多個 AWS 受管理 Microsoft AD 目錄之間的一個和雙向外部和樹系信任關係。 AWS 受管理的 Microsoft AD 支援所有三個信任關係方向：傳入、傳出和雙向 (雙向)。

如需有關信任關係的詳細資訊，請參閱您想要瞭解的有關 AWS 受管理 Microsoft AD 信任的一切。

> **Note**
>
> 設定信任關係時，您必須確定您的自我管理目錄與 AWS Directory Service s 保持相容。如需您責任的詳細資訊，請參閱我們的「共同的責任模型」。

AWS 受管理的 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。

AWS 企業應用程序需要雙向信任，例如 Amazon Chime QuickSight，Amazon Connect AWS IAM Identity Center WorkDocs，Amazon WorkMail，Amazon WorkSpaces，Amazon 和. AWS Management Console AWS 受管理的 Microsoft AD 必須能夠查詢您自我管理Active Directory中的使用者和群組。

Amazon EC2、Amazon RDS 和 Amazon FSx 將使用單向或雙向信任。

必要條件

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 受管理的 Microsoft AD 不支援單一標籤網域的信任。

連線到 VPC

如果您要使用自我管理的目錄建立信任關係，則必須先將自我管理網路連線到包含受 AWS 管 Microsoft AD 的 Amazon VPC。您自我管理和 AWS 受管理的 Microsoft AD 網路的防火牆必須開啟的網路連接埠，這些連接埠都必須在Windows伺服器 2008 及更新版本的Microsoft說明文件中列出。

若要使用 NetBIOS 名稱而非完整網域名稱來驗證您的 AWS 應用程式 (例如 Amazon WorkDocs 或 Amazon) QuickSight，您必須允許連接埠 9389。如需有關 Active Directory 連接埠和通訊協定的詳細資訊，請參閱Microsoft說明文件Windows中的服務概觀和網路連接埠需求。

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 受管理 Microsoft AD 的 VPC 人雲端必須具有適當的輸出和輸入規則。

設定您的 VPC 輸出規則

1. 在AWS Directory Service 主控台的 [目錄詳細資料] 頁面上，記下您 AWS 受管理的 Microsoft AD 目錄識別碼。
2. 前往 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 AWS 管理的 Microsoft AD 目錄識別碼。在搜索結果中，選擇描述為「為目錄 ID 目錄控制器AWS 創建安全組」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 瞭解目錄的 AWS 安全性群組組態和使用方式。

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。如需有關此設定的詳細資訊，請檢閱 Microsoft TechNet 上的預先驗證。

為您的自我管理域設定 DNS 條件式轉寄站

您必須在自我管理域上設定 DNS 條件式轉寄站。如需有關條件式轉寄站的詳細資訊，請參閱在 Microsoft 上指派網域名稱 TechNet 的條件式轉寄站。

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，您必須獲取有關 AWS 託管 Microsoft AD 的一些信息。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 管理 Microsoft AD 的目錄識別碼。
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 AWS 受管理的 Microsoft AD 的完整網域名稱 (FQDN)，這是您先前提到的。

11. 選擇主要伺服器的 IP 位址，然後輸入 AWS 受管理的 Microsoft AD 目錄的 DNS 位址，這是您先前提到的。

    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 受管理的 Microsoft AD 上設定信任關係時，您將需要使用這個相同的密碼。如需詳細資訊，請參閱管理 Microsoft 上的信任 TechNet。

您現在已準備好在 AWS 受管理的 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 管理 Microsoft AD 的全域功能。如果您使用 多區域複製，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。

與 AWS 管理 Microsoft AD 建立信任關係

1. 開啟 AWS Directory Service 主控台。
2. 在 [目錄] 頁面上，選擇您的 AWS 受管理 Microsoft AD 識別碼。
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. (選擇性) 如果您想要只允許授權的使用者存取 AWS 受管理 Microsoft AD 目錄中的資源，您可以選擇性地選擇性驗證核取方塊。如需有關選擇性驗證的一般資訊，請參閱 Microsoft 上信任的安全性考量 TechNet。
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 受管理的 Microsoft AD 和各種活動目錄域之間創建多個信任。不過，每對一次只能存在一個信任關係。例如，如果您已有「連入方向」的單向信任，之後想要設定「連出方向」的另一個信任關係，您將需要刪除現有信任關係，再建立新的「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 受管理 Microsoft AD 識別碼。
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)。

這個過程只驗證雙向信任的傳出方向。 AWS 不支援驗證傳入的信任。如需有關如何驗證與您自我管理的 Active Directory 之間的信任的詳細資訊，請參閱驗證 Microsoft TechNet 上的信任。

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 受管理 Microsoft AD 識別碼。
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。

使用公有 IP 地址時新增 IP 路由

您可以使用 AWS Directory Service for Microsoft Active Directory 利用許多強大的 Active Directory 功能，包括建立與其他目錄的信任關係。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「建立信任關係」。

同樣地，當您將流量從 AWS 上的 AWS Managed Microsoft AD 路由到對等的 AWS VPC 時，如果 VPC 使用公有 IP 範圍，您也必須輸入 IP 地址資訊。

當您如「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。如需更多詳細資訊，請參閱 瞭解目錄的 AWS 安全性群組組態和使用方式。

教學：在 AWS Managed Microsoft AD 和自我管理的 Active Directory 域之間建立信任關係

此教學會帶您演練設定 AWS Directory Service for Microsoft Active Directory 與自我管理 (內部部署) Microsoft Active Directory 之間信任關係所需的所有步驟。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

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 不支援信任單一標籤域。

- 在 AWS 上建立 AWS Managed Microsoft AD 目錄。如果您需要協助來執行此作業，請參閱「開始使用 AWS 受管理 Microsoft AD」。
- 執行 Windows 並已新增至該 AWS Managed Microsoft AD 的 EC2 執行個體。如果您需要協助來執行此作業，請參閱「手動將 Amazon EC2 Windows 實例加入到您的 AWS 受管 Microsoft AD 活動目錄」。

> **Important**
>
> 您的 AWS Managed Microsoft AD 管理員帳戶必須具備此執行個體的管理存取權。

- 已在該執行個體上安裝下列 Windows Server 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「安裝適用於 AWS 受管理 Microsoft AD 的活動目錄管理工具」。
- 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。此目錄也必須能夠使用以上所列的相同 Windows Server 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 建立信任關係。

教學組態

在本教學中，我們已經建立了一個 AWS Managed Microsoft AD 和一個自我管理域。該自我管理網路連線至該 AWS Managed Microsoft AD 的 VPC。以下是這兩個目錄的屬性：

在 AWS 上執行的 AWS Managed Microsoft AD

- 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

該 AWS Managed Microsoft AD 位於 VPC ID：vpc-12345678。

自我管理或 AWS Managed Microsoft AD 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的防火牆，以便針對包含受管理 Microsoft AD 的 VPC 所使用的所有子網路，開放下列連接埠供 CIDR 使用。 AWS 在本教程中，我們允許來自 10.0.0/16（我們 AWS 託管 Microsoft AD VPC 的 CIDR 塊）的傳入和傳出流量在以下端口上：

- 網域名稱系統 (DNS)
- TCP/UDP 88 - Kerberos 身分驗證
- 輕量型目錄存取通訊協定
- 伺服器訊息區 (SMB)
- TCP 9389-使用中目錄 Web 服務 (ADWS) (選用-如果您想要使用 NetBIOS 名稱而不是完整的網域名稱進行身份驗證，如 Amazon WorkDocs 或 Amazon AWS 應用程式，則需要開啟此連接埠。) QuickSight

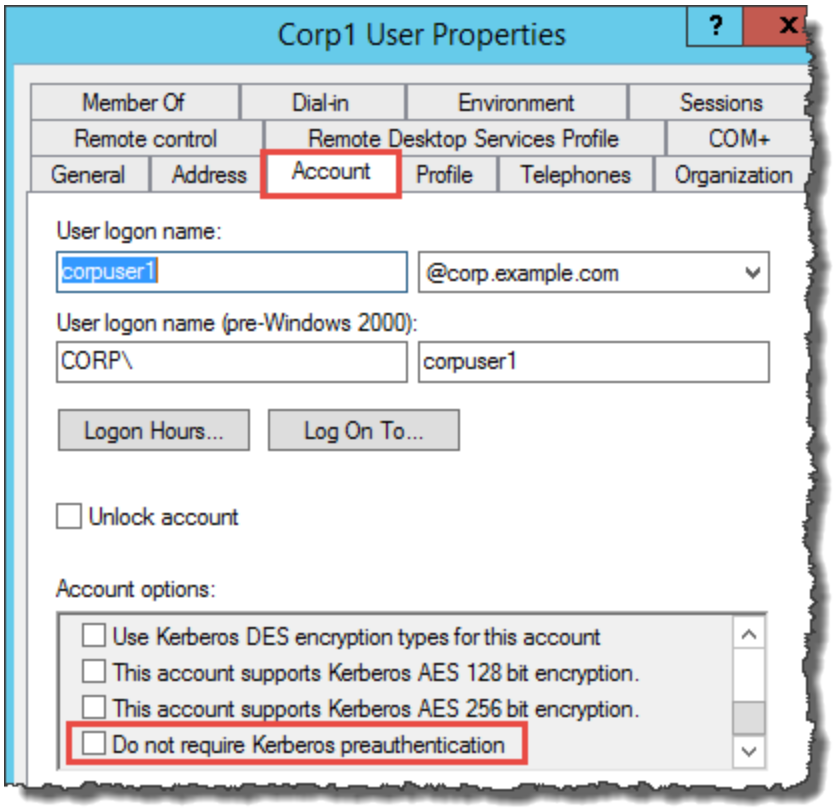
> **Note**
>
> 不再支援 SMBv1。
> 您至少需要這些連接埠，才可將 VPC 連線到自我管理目錄。您特定的組態可能需要開啟其他連接埠。

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。

若要檢視使用者的 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。



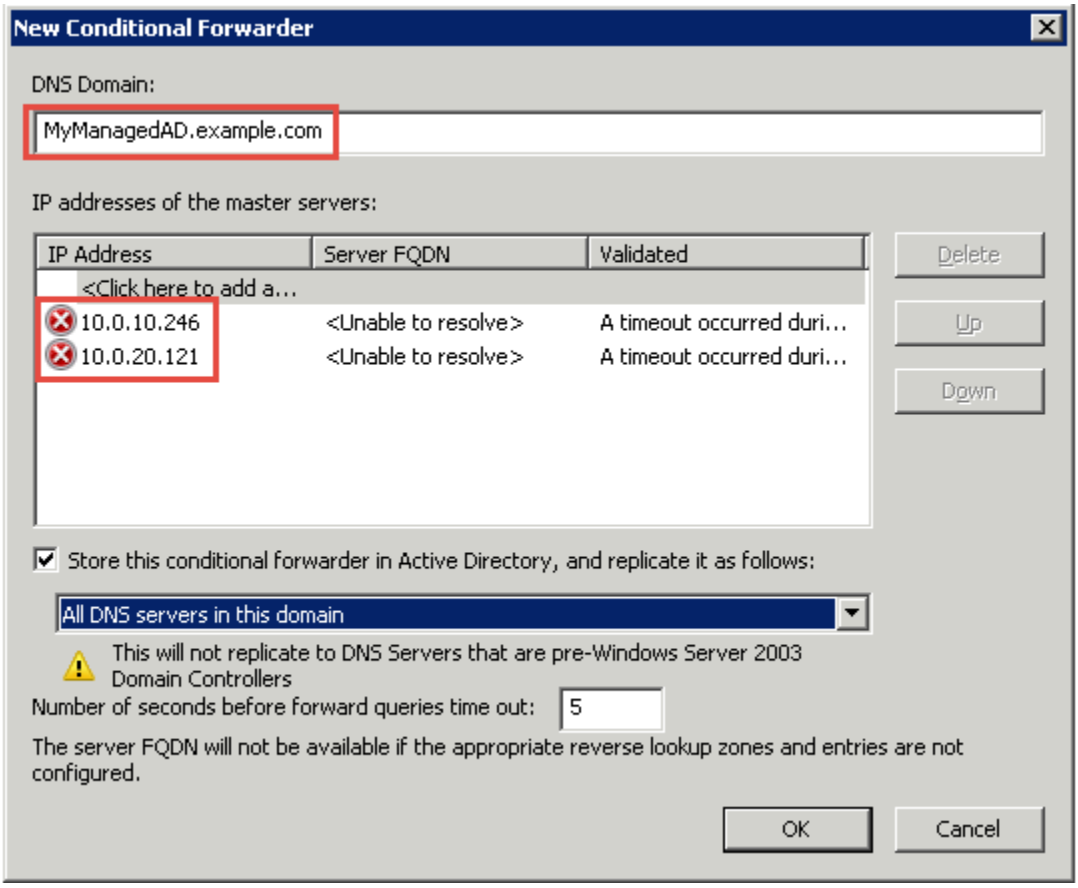
為您的自我管理域設定 DNS 條件式轉寄站

您必須在每個網域上設定 DNS 條件式轉寄站。在您的自我管理網域上執行這項操作之前，您會先取得有關 AWS 受管理 Microsoft AD 的一些資訊。

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 管理 Microsoft AD 的目錄識別碼。
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 AWS 受管理的 Microsoft AD 的完整網域名稱 (FQDN)，這是您先前提到的。在此範例中，FQDN 為 MyManaged廣告。
11. 選擇主要伺服器的 IP 位址，然後輸入 AWS 受管理的 Microsoft AD 目錄的 DNS 位址 (您先前所述)。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

現在讓我們為建立信任關係準備您的 AWS Managed Microsoft AD。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。只是這次是處理 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。若要執行此操作，您需確保域控制站上，ACL 已關聯至您用以部署 AWS Managed Microsoft AD 和安全群組規則的子網路，兩者允許先決流量以支援信任。

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

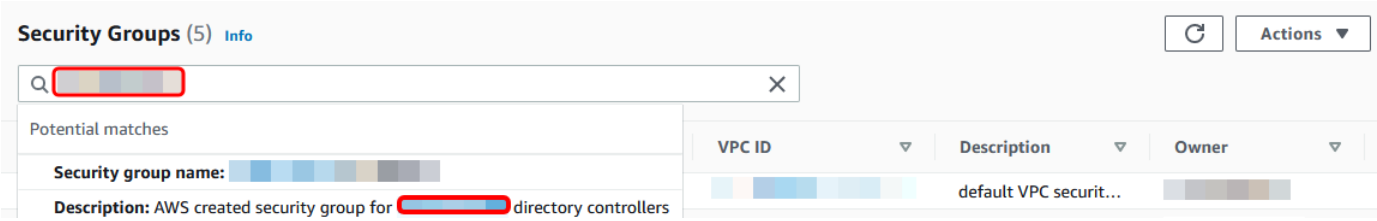
- ALL

> **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 域控制站的傳出和傳入規則

1. 返回 AWS Directory Service 主控台。目錄清單中，請記錄 AWS Managed Microsoft AD 目錄為您的目錄 ID。
2. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
3. 在導覽窗格中，選擇安全群組。

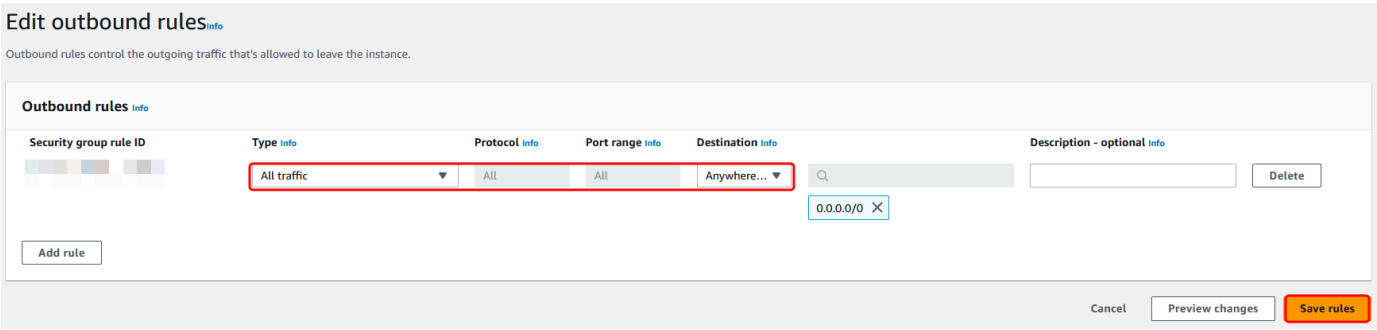
4. 使用搜尋方塊搜尋您的 AWS Managed Microsoft AD 目錄 ID。在搜尋結果中，選取包含說明的「安全性群組」**AWS created security group for *yourdirectoryID* directory controllers**。



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，請參閱瞭解目錄的 AWS 安全性群組組態和使用方式。

6. 選取儲存規則。



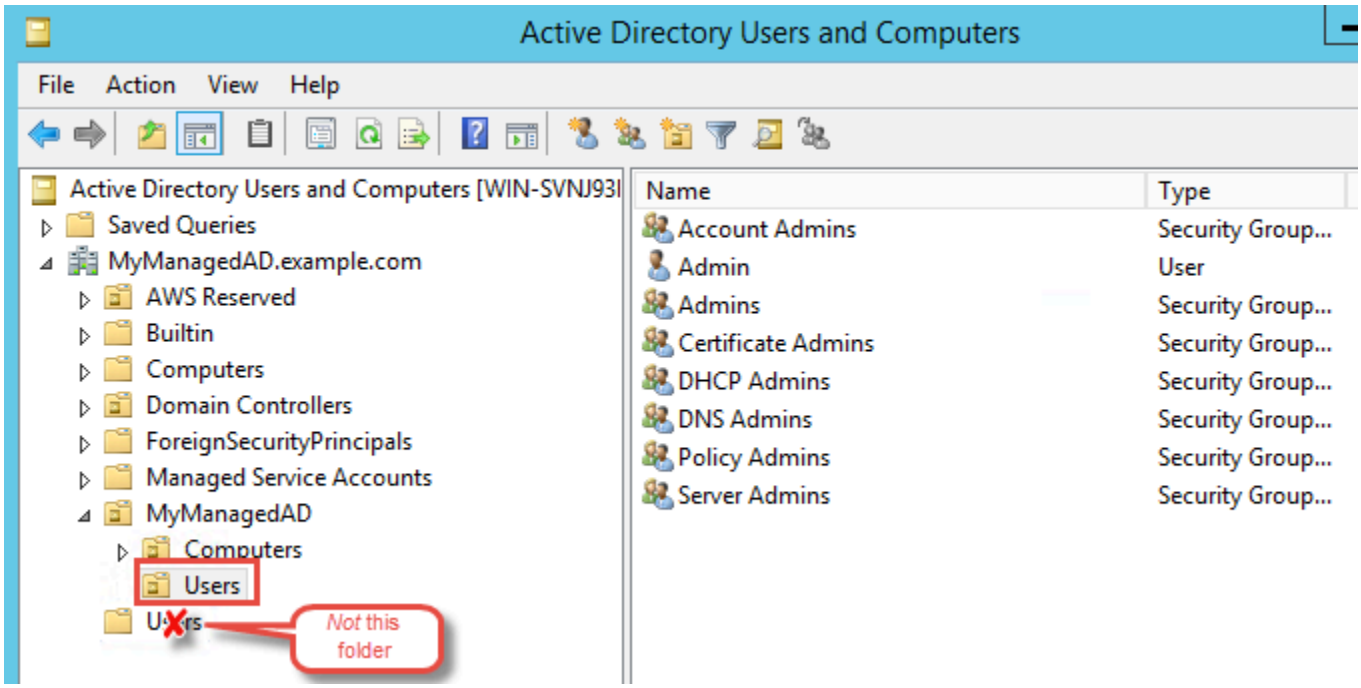
確定已啟用 Kerberos 預先驗證

現在您要確認 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. 使用域的 管理員帳戶的權限 或已獲委派管理域使用者許可的帳戶，登入屬於 AWS Managed Microsoft AD 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，請參閱安裝適用於 AWS 受管理 Microsoft AD 的活動目錄管理工具。
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，您要建立自我管理域的信任，最後再建立 AWS Managed Microsoft AD 的信任。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，如果您建立了自我管理域的單向傳出信任，就需要建立 AWS Managed Microsoft AD 的單向傳入信任。

> **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。

若要在您的自我管理作用中目錄中設定信任

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)。選擇下一步。
5. 選擇 Two-way (雙向)。選擇下一步。
6. 選擇 This domain only (僅限此網域)。選擇下一步。
7. 選擇 Forest-wide authentication (全森林身分驗證)。選擇下一步。
8. 輸入 Trust password (信任密碼)。請務必記住此密碼，因為您設定 AWS Managed Microsoft AD 的信任時，會需要該密碼。
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)。選擇下一步。
11. 選擇 No, do not confirm the incoming trust (否，不要確認傳入信任)。選擇下一步。

在您的 AWS Managed Microsoft AD 目錄中設定信任

最後，您需要設定 AWS Managed Microsoft AD 目錄的林信任關係。因為您已建立自我管理域的雙向林信任，所以也要使用 AWS Managed Microsoft AD 目錄來建立雙向信任。

> **Note**
>
> 信任關係是 AWS Managed Microsoft AD 的全域功能。如果您使用 多區域複製，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。

在您的 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 Add (新增)。

恭喜您。您現在在自我管理的網域 (Corp.example.com) 和受管理的 Microsoft AD (Ad.example.com) 之間有信任關係。AWS MyManaged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 建立信任關係。

教學：在兩個 AWS Managed Microsoft AD 域之間建立信任關係

此教學會帶您演練設定兩個 AWS Managed Microsoft AD 域之間建立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：建立與另一個 AWS Managed Microsoft AD 域的信任關係

另請參閱

建立信任關係

步驟 1：準備您的 AWS Managed Microsoft AD

在本節中，您將準備 AWS Managed Microsoft AD，讓其能夠與另一個 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，這次您將設定不同的 AWS Managed Microsoft AD 環境以讓它們之間可以搭配使用。

設定您的 VPC 子網路和安全群組

您必須允許從一個 AWS Managed Microsoft AD 網路到包含另一個 AWS Managed Microsoft AD 的 VPC 的流量。若要執行此操作，您需確保域控制站上，ACL 已關聯至您用以部署 AWS Managed Microsoft AD 和安全群組規則的子網路，兩者允許先決流量以支援信任。

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

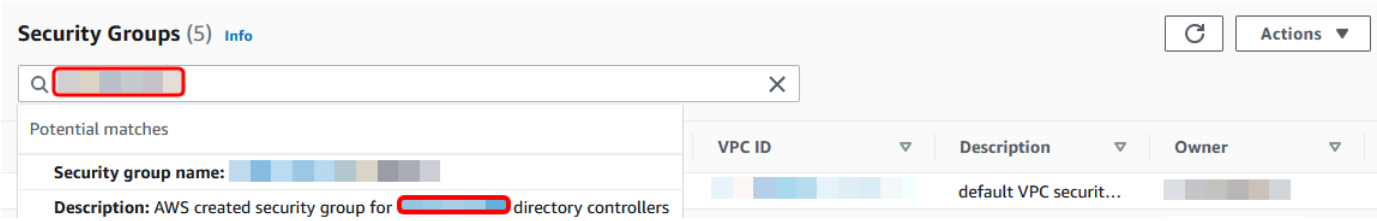
- ALL

> **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 域控制站的傳出規則

> **Note**
>
> 對每個目錄重複下面的步驟 1-6。

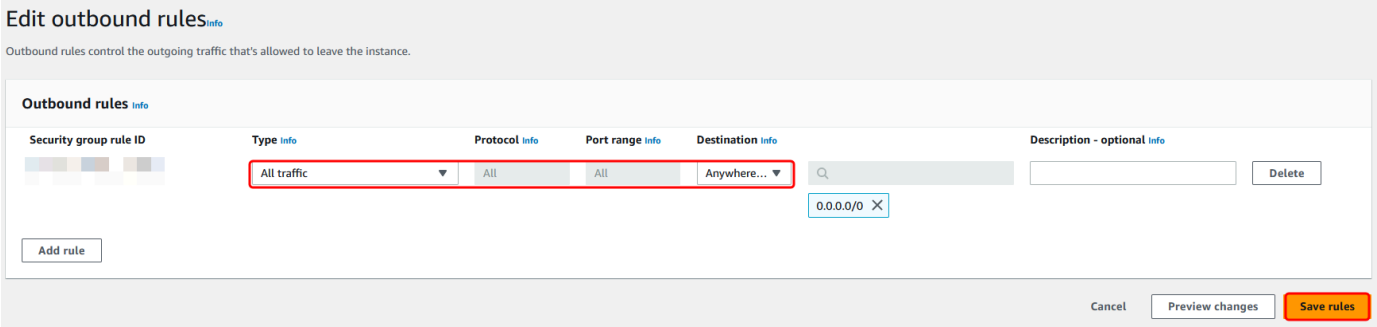
1. 前往 AWS Directory Service 主控台。目錄清單中，請記錄 AWS Managed Microsoft AD 目錄為您的目錄 ID。
2. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
3. 在導覽窗格中，選擇安全群組。
4. 使用搜尋方塊搜尋您的 AWS Managed Microsoft AD 目錄 ID。請在搜索結果中選擇包含描述的物件**`AWS created security group for yourdirectoryID directory controllers`**。



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，請參閱瞭解目錄的 AWS 安全性群組組態和使用方式。

6. 選取 Save (儲存)。

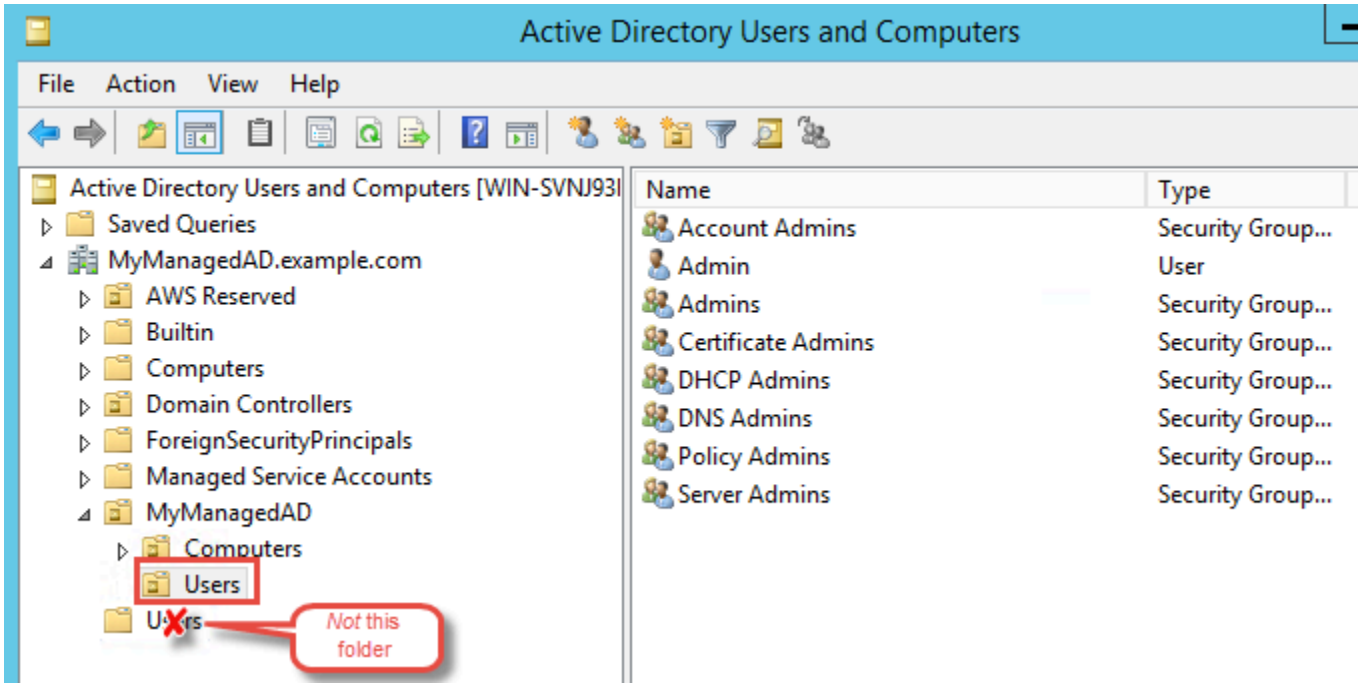


確定已啟用 Kerberos 預先驗證

現在您要確認 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. 使用域的 管理員帳戶的權限 或已獲委派管理域使用者許可的帳戶，登入屬於 AWS Managed Microsoft AD 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，請參閱安裝適用於 AWS 受管理 Microsoft AD 的活動目錄管理工具。
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：建立與另一個 AWS Managed Microsoft AD 域的信任關係

步驟 2：建立與另一個 AWS Managed Microsoft AD 域的信任關係

既然準備工作已完成，最後步驟便要建立兩個 AWS Managed Microsoft AD 域之間的信任。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 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，如果您在第一個 AWS Managed Microsoft AD 域中建立了單向傳出信任，那麼就需要在第二個中建立單向傳入信任。

> **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 域中設定信任

1. 開啟 AWS Directory Service 主控台。
2. 在目錄頁面上，選擇第一個 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。如需更多詳細資訊，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，鍵入第二個 AWS Managed Microsoft AD 域的 FQDN。請務必記住此密碼，因為您設定第二個 AWS Managed Microsoft AD 的信任時，會需要該密碼。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，然後輸入第二個 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 Add (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 域中設定信任

現在，您需要設定第二個 AWS Managed Microsoft AD 目錄的林信任關係。由於您在第一個 AWS Managed Microsoft AD 域中建立了雙向林信任，因此您同樣需要在此 AWS Managed Microsoft AD 域中建立雙向信任。

在第二個 AWS Managed Microsoft AD 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。如需更多詳細資訊，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，鍵入第一個 AWS Managed Microsoft AD 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，然後輸入第一個 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 Add (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 域之間建立了信任關係。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。

擴展您的結構描述

AWS Managed Microsoft AD 使用結構描述來組織及強制執行目錄資料的存放方式。將定義新增至結構描述的程序稱為「延伸結構描述」。結構描述延伸讓您能夠使用有效的 LDAP 資料交換格式 (LDIF) 檔案，修改您 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。

主題

- 延伸 AWS Managed Microsoft AD 結構描述的時機
- 教學課程：擴充 AWS 受管理的 Microsoft AD 架構

延伸 AWS Managed Microsoft AD 結構描述的時機

您可以透過新增物件類別和屬性，來延伸您的 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。當您需要將依賴 AWS Managed Microsoft AD 的企業應用程式遷移到 AWS 雲端時，這可能會特別有用。

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 ID 稱為 AD 物件識別符 (OID) 並會存放在 AWS Managed Microsoft AD 中。

若要開始使用，請參閱 教學課程：擴充 AWS 受管理的 Microsoft AD 架構。

相關主題

- 擴展您的結構描述
- 結構描述元素

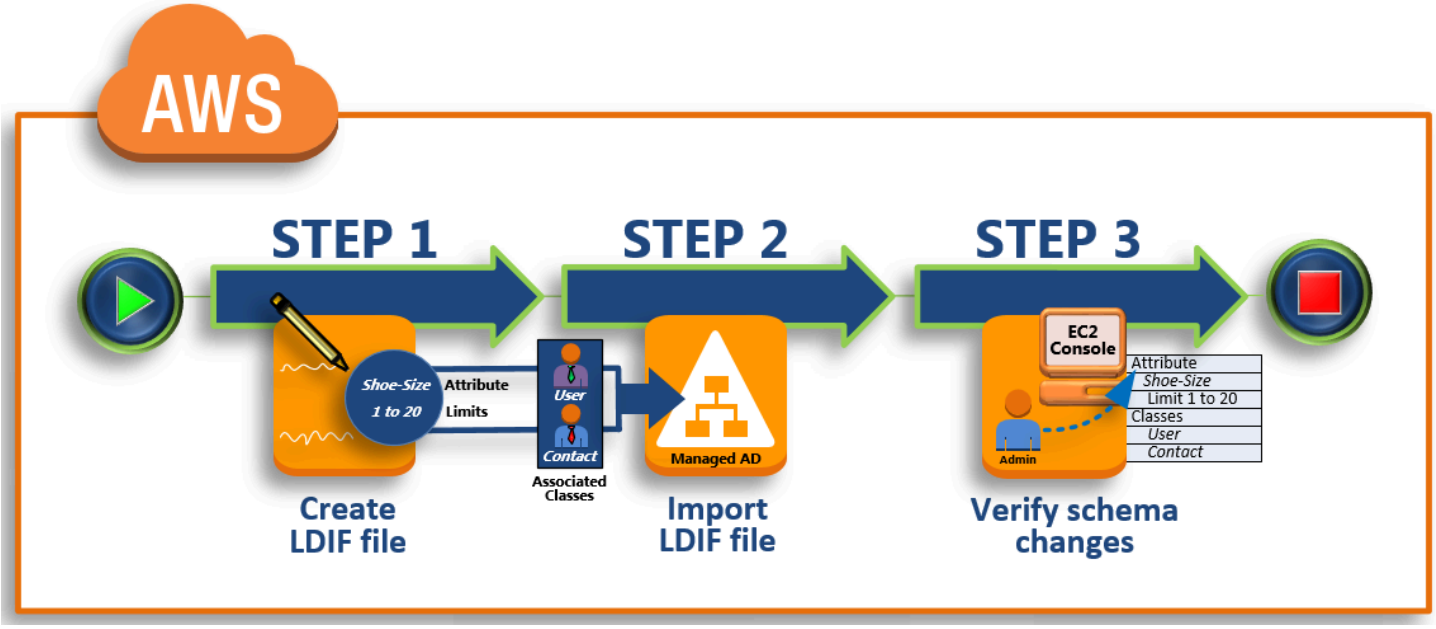
教學課程：擴充 AWS 受管理的 Microsoft AD 架構

在本教程中，您將學習如何擴展模式為您的 AWS Directory Service 的 Microsoft Active Directory 目錄，也稱為 AWS 託管 Microsoft AD，通過添加唯一的屬性和類，滿足您的特定需求。 AWS 受管理的 Microsoft AD 結構描述延伸模組只能使用有效的 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「延伸 AWS Managed Microsoft AD 結構描述的時機」。

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，您可以使用主 AWS Directory Service 控台將 LDIF 檔案匯入至您的 Microsoft 使用中目錄環境。

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 受管理的 Microsoft AD 目錄上執行`ldifde.exe`應用程式， AWS Directory Service 匯入含有結構描述變更的 LDIF 檔案。因此，您會發現它對了解 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 能在 Active Directory 物件的樹狀目錄中找到 Active Directory 物件，且必須包含您目錄的網域元件。例如，此教學中的目錄網域元件是 `DC=example,DC=com`。

  DN 也必須包含 Active Directory 物件的常見名稱 (CN)。第一個 CN 項目是屬性或類別名稱。接下來，您必須使用 `CN=Schema,CN=Configuration`。這個 CN 確保您能夠擴展 Active Directory 結構描述。如前所述，您無法新增或修改 Active Directory 物件的內容。DN 遵循的一般格式。

  ```
  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，如果發生錯誤而您不想從備份還原時，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

若要深入了解如何建構 LDIF 檔案，並查看可用於測試 AWS 受管理 Microsoft AD 結構描述延伸模組的範例 LDIF 檔案，請參閱安全性部落格上如何擴充 AWS 受管理的 Microsoft AD 目錄結構描述文章。AWS

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 來擴充結構描述。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**
>
> 當您對 AWS 受管理的 Microsoft AD 目錄結構描述進行更新時，作業無法復原。換言之，一旦您建立新的類別或屬性，Active Directory 不允許您移除它。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 受管理的 Microsoft AD 會擷取快照以保留目錄的目前狀態。

Note

結構描述延伸模組是 AWS 管理 Microsoft AD 的全域功能。如果您使用 多區域複製，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。不要在生產環境中套用任何未在開發或測試環境中經過應用程式測試的結構描述更新。

LDIF 檔案的套用方式

上傳您的 LDIF 檔案之後，Microsoft AWS 受管理 AD 會採取步驟來保護您的目錄不會發生錯誤，因為它會依照下列順序套用變更。

1. 驗證 LDIF 檔案。由於 LDIF 指令碼可以操控網域中的任何物件，因此 AWS 受管理的 Microsoft AD 會在您上傳之後立即執行檢查，以協助確保匯入作業不會失敗。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 受管理的 Microsoft AD 會隔離其中一個 DC，並將 LDIF 檔案中的更新套用至隔離的 DC。接著，選取您其中一個 DC 成為主結構描述，將該 DC 從目錄複寫中移除，然後使用 `Ldifde.exe` 套用您的 LDIF 檔案。
4. 複寫發生到所有 DC。 AWS 受管理的 Microsoft AD 會將隔離的 DC 新增回複寫，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。

此程序會使用 Active Directory 結構描述嵌入式管理單元和/或 PowerShell 驗證結構描述更新已套用。您必須從已加入 AWS 受管理 Microsoft AD 的網域的電腦執行這些工具。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網站上的指示安裝作用中目錄結構描述嵌入式管理單元。
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。

若要驗證使用 PowerShell

1. 開啟視 PowerShell 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

當您已建立新屬性並想要將新值新增至 AWS 受管理 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. 打開命Windows PowerShell令行實用程序，並使用以下命令設置新屬性。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

維護您的 AWS 管理 Microsoft AD 目錄

本節說明如何維護 AWS 受管理 Microsoft AD 環境的一般系統管理工作。

主題

- 新增替代 UPN 尾碼
- 刪除您 AWS 託管的 Microsoft AD
- 重新命名目錄的站台名稱
- 建立目錄快照或還原目錄
- 升級您的 AWS 管理 Microsoft AD 活動目錄
- 檢視目錄資訊

新增替代 UPN 尾碼

您可以新增替代使用者主體名稱 (UPN) 尾碼到 AWS Managed Microsoft AD 目錄，以簡化 Active Directory (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，請參閱什麼被創建與 AWS 管理 Microsoft AD 活動目錄相關文章。

新增替代 UPN 尾碼

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 找到加入您 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。

刪除您 AWS 託管的 Microsoft AD

刪除受 AWS 管理的 Microsoft AD 時，會刪除所有目錄資料和快照集，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。確保您位於部署的 AWS 區域 Active Directory位置。如需詳細資訊，請參閱選擇區域。
2. 請確定您要刪除的目錄沒有啟用任何 AWS 應用程式。啟用的 AWS 應用程式會阻止您刪除 AWS 受管理的 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 [應用AWS 程式與服務] 區段中，您會看到目錄已啟用哪些 AWS 應用程式。

      - 停用 AWS Management Console 存取權。
      - 若要停用 Amazon WorkSpaces，您必須從 WorkSpaces 主控台中的目錄取消註冊服務。如需詳細資訊，請參閱 Amazon WorkSpaces 管理指南中的從目錄取消註冊。
      - 要禁用 Amazon WorkDocs，您必須在 Amazon WorkDocs 控制台中刪除 Amazon WorkDocs 網站。如需詳細資訊，請參閱 Amazon WorkDocs 管理指南中的刪除網站。
      - 要禁用 Amazon WorkMail，您必須在 Amazon WorkMail 控制台中刪除 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。
      - 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 適用Active Directory於 Windows 檔案伺服器的使用者指南中的使 FSx for Windows File Server。
      - 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 管理手冊》中的〈Active Directory驗證〉。
      - 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 管理員指南》中的刪除 Amazon Connect 執行個體一節。

- 要禁用 Amazon QuickSight，您必須從 Amazon 退訂 QuickSight。如需詳細資訊，請參閱 Amazon QuickSight 使用者指南中的關閉 Amazon QuickSight 帳戶。

> **Note**
>
> 如果您正在使用 AWS IAM Identity Center 且之前已將其連線至您計劃刪除的 AWS 受管理 Microsoft AD 目錄，則必須先變更身分識別來源，然後才能刪除身分識別來源。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。

重新命名目錄的站台名稱

您可以為 AWS Managed Microsoft AD 目錄的預設站台名稱重新命名，使其配合現有的 Microsoft Active Directory (AD) 站台名稱。如此一來，AWS Managed Microsoft AD 可更快速在您的內部部署目錄找到並驗證現有的 AD 使用者。結果便是讓使用者在登入 AWS 資源 (例如您已加入 AWS Managed Microsoft AD 目錄的 Amazon EC2 和 Amazon RDS for SQL Server 執行個體) 時，擁有更佳的體驗。

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，請參閱什麼被創建與 AWS 管理 Microsoft AD 活動目錄相關文章。

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 站台名稱

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 找到加入您 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)。

建立目錄快照或還原目錄

AWS Directory Service提供自動化的每日快照，並能夠為您的AWS受管理 Microsoft AD 活動目錄拍攝資料的手動快照。這些快照集可用來執行 point-in-time 還原作業中的目錄。每個AWS受管理的 Microsoft AD 活動目錄只能使用五個手動快照集。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 的一項全域功能。如果您使用 多區域複製，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。

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。

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 Support 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。

對於 AWS Managed Microsoft AD 目錄，還原目錄可能需要兩到三個小時。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。

升級您的 AWS 管理 Microsoft AD 活動目錄

您可以升級您的標準版 AWS 管理 Microsoft AD 活動目錄到企業版通過聯繫 AWS Support。如需詳細資訊，請參閱AWS Support 使用指南中的建立支援案例和案例管理。

升級 AWS 管理 Microsoft AD 活動目錄時，需要注意一些限制。這些類別為：

- 升級將產生額外費用。如需詳細資訊，請參閱 AWS Directory Service 定價。
- 一旦您的活動目錄升級，它就無法恢復到以前的版本。
- 之前的快照集無法在升級後使用它來還原作用中目錄。
- 升級會在同意的排定日期與時間進行 AWS Support。升級會在太平洋標準時間週一至週五上午 9 點至下午 5 點之間進行。
- 升級過程需要四到五個小時。
- 在升級程序期間，您 AWS 受管理的 Microsoft AD 作用中目錄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，並可能導致維護期間停機。
- 如果您的應用程式使用的是網域控制站的主機名稱或 IP 位址，而非 Active Directory 的網域名稱，則需要更新這些應用程式。
- 如果您使用 LDAPS (透過 SSL 的輕量型目錄存取通訊協定)，網域控制站將需要新的憑證。

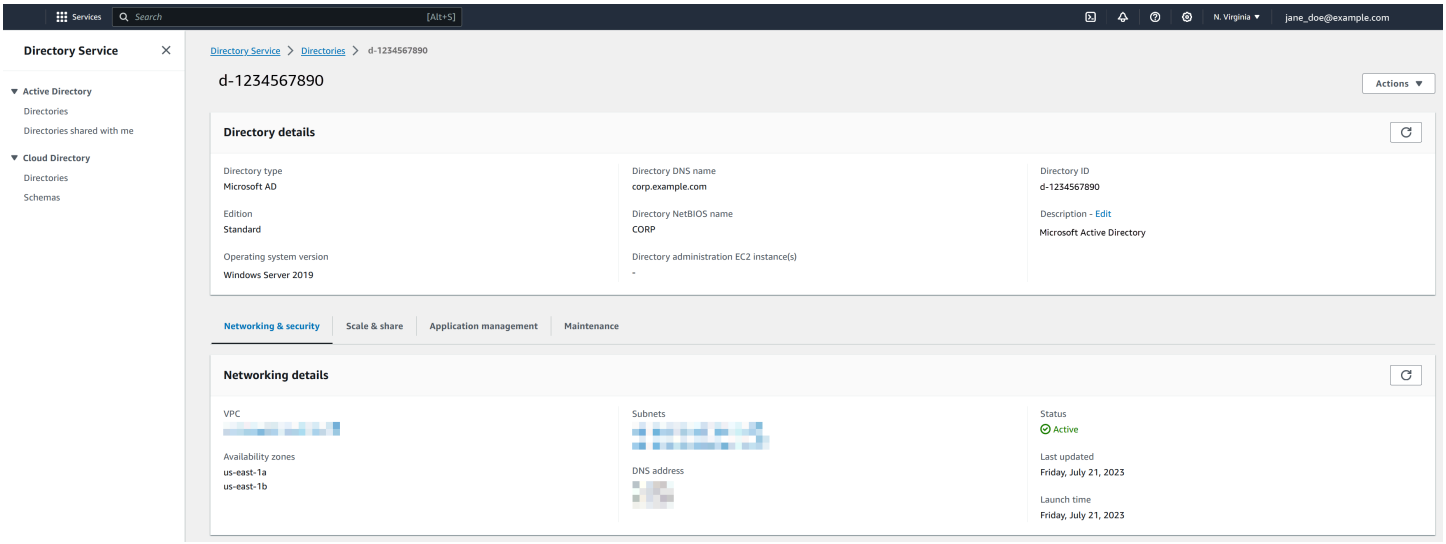
檢視目錄資訊

您可檢視關於目錄的詳細資訊。

檢視詳細目錄資訊

1. 在AWS Directory Service 主控台導覽窗格的下 Active Directory，選取 [目錄]。
2. 按一下目錄的目錄 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」。



授予 AWS 資源存取權給使用者與群組

AWS Directory Service 可讓您的目錄使用者和群組存取 AWS 服務和資源，例如 Amazon EC2 主控台的存取權。類似於授予 IAM 使用者管理目錄的存取權身分類型政策 (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。

如需有關如何授與使用者存取權的資訊 AWS Management Console，請參閱啟用 AD 憑證存取 AWS Management Console。

主題

- 建立新的角色
- 編輯現有角色的信任關係
- 將使用者或群組指派給現有角色
- 檢視指派給角色的使用者和群組
- 從角色移除使用者或群組
- 對 AWS Directory Service 使用 AWS 受管政策

建立新的角色

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 主控台建立該角色。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. 選取您要套用至目錄使用者的原則 (例如 AmazonEC2 FullAccess) 旁邊的核取方塊，然後選擇 [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

以下檢查清單提供您建立新角色以讓特定目錄使用者獲得 Amazon EC2 主控台存取權時，所必須完成的任務範例。

1. 使用上述程序，以 IAM 主控台建立一個角色。當系統提示您提供政策時，請選擇亞馬遜 EC2 FullAccess。
2. 使用編輯現有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。 AWS Management Console 在您啟用下一個步驟的存取權之後，必須執行此步驟，才能立即顯示角色。
3. 依照啟用 AD 憑證存取 AWS Management Console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。

編輯現有角色的信任關係

您可以將現有的 IAM 角色指派給使 AWS Directory Service 用者和群組。但是，要做到這一點，角色必須與信任關係 AWS Directory Service。當您使用中 AWS Directory Service 的程序建立角色時建立新的角色，會自動設定此信任關係。您只需要為非 AWS Directory Service建立的 IAM 角色建立此信任關係。

若要建立現有角色的信任關係 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。

```
{
  "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角色

您可以將現有的 IAM 角色指派給 AWS Directory Service 使用者或群組。為此，請確保您已完成以下操作。

必要條件

- 創建一個 AWS 託管 Microsoft AD。
- 建立使用者或建立群組。
- 建立與信任關係的角色 AWS Directory Service。您可以編輯現有角色的信任關係。

> **Note**
>
> 系統並不支援目錄中的巢狀群組使用者進行存取。父群組的成員可存取主控台，但子群組的成員則否。

將使用者或群組指派給現有 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：
   - 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。
   - 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 [委派主控台存取權] 區段下，為您要指派使用者的現有 IAM 角色選擇 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

若要檢視指派給角色的使用者和群組，請執行下列步驟。

必要條件

- 將您的使用者或群組指派給現有角色。

檢視指派給角色的使用者和群組

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：
   - 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。
   - 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. 在委託主控台存取區段下，選擇您要檢視的 IAM 角色。
5. 在選取的角色頁面的管理此角色的使用者和群組區段下，您可以檢視指派給該角色的使用者和群組。

從角色移除使用者或群組

若要從角色移除使用者或群組，請執行下列步驟。

從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：

- 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。
- 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，選擇您要檢視的角色。
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。

對 AWS Directory Service 使用 AWS 受管政策

AWS Directory Service 提供下列 AWS 受管政策，讓您可將 AWS 服務和資源的存取權 (例如 Amazon EC2 主控台的存取權) 授予您的使用者和群組。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
- 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

如需有關如何自行建立政策的詳細資訊，請參閱《IAM 使用者指南》中的管理 AWS 資源的政策範例。

啟用對應用 AWS 程式和服務的存取

使用者可以授權 AWS 受管 Microsoft AD 給 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，以便與 AWS 受管理的 Microsoft AD 搭配使用。

AWS 應用程式/服務	詳細資訊...
Amazon Chime	如需詳細資訊，請參閱《Amazon Chime 管理指南》。
Amazon Connect	如需詳細資訊，請參閱《Amazon Connect 管理指南》。
Amazon FSx for Windows File Server	如需詳細資訊，請參閱將 Amazon FSx 搭配 AWS Directory Service 搭配 Microsoft 使用中目錄服務。
Amazon QuickSight	如需詳細資訊，請參閱 Amazon QuickSight 使用者指南。
Amazon Relational Database Service	如需詳細資訊，請參閱 Amazon RDS 使用者指南。
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 管理員指南。

AWS 應用程式/服務	詳細資訊...
Amazon WorkSpaces	您可以直接從建立 Simple AD、 AWS 受管理的 Microsoft AD 或 AD 連接器 WorkSpaces。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。
AWS IAM Identity Center	如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南。
AWS License Manager	如需詳細資訊，請參閱 License Manager 使用者指南。
AWS Management Console	如需詳細資訊，請參閱 啟用 AD 憑證存取 AWS Management Console。
AWS Private Certificate Authority	如需詳細資訊，請參閱的AWS Private CA 連接器Active Directory。
AWS Transfer Family	如需詳細資訊，請參閱 AWS Transfer Family 使用者指南。

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，請參閱授權使用的 AWS 應用程式和服務 AWS Directory Service。

主題

建立存取 URL

存取 URL 可用於 AWS 應用程式和服務 (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。

> **Note**
>
> 使用多區域目錄時，只能從主要區域設定存取 URL。

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。如需更多詳細資訊，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。依預設，此 URL 將帶您進入 Amazon WorkDocs 的登入頁面。

單一登入

AWS Directory Service提供允許您的使用者 WorkDocs 從加入目錄的電腦存取 Amazon 的功能，而無需單獨輸入其登入資料。

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體名稱屬性，您可以使用具有修改 AD Connector 服務帳戶權限的帳戶，從加入網域的電腦執行下列 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 Amazon 啟用或停用單一登入 WorkDocs

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 Amazon 的單一登入 WorkDocs。

   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. 如果您稍後想要停用 Amazon 的單一登入 WorkDocs，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。
- 啟用主動腳本（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

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原則：

```
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 政策在網域中的電腦上管理 Chrome 網路瀏覽器，就必須將存取網址新增至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。

啟用 AD 憑證存取 AWS Management Console

AWS Directory Service 可讓您授予 AWS Management Console存取權給目錄成員。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，讓他們可以存取各種 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「檢視目錄資訊」。如需如何建立存取 URL 的詳細資訊，請參閱「建立存取 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 資源存取權給使用者與群組」。

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

相關的 AWS 安全性部落格文章

- 如何使用 AWS Managed Microsoft AD 和內部部署憑證來存取 AWS Management Console

> **Note**
>
> 存取 AWS Management Console 是 AWS Managed Microsoft AD 的區域功能。如果您使用 多區域複製，則必須在每個區域中單獨執行以下程序。如需更多詳細資訊，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：
   - 如果多區域複寫下顯示多個區域，請選取要啟用對 AWS Management Console 的存取的區域，然後選擇應用程式管理索引標籤。如需更多詳細資訊，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。

   在使用者可以使用存取 URL 登入主控台之前，您必須先將使用者新增至角色。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，請選取要停用對 AWS Management Console 的存取的區域，然後選擇應用程式管理索引標籤。如需更多詳細資訊，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。如需更多詳細資訊，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 AWS 資源存取對話方塊中，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)。

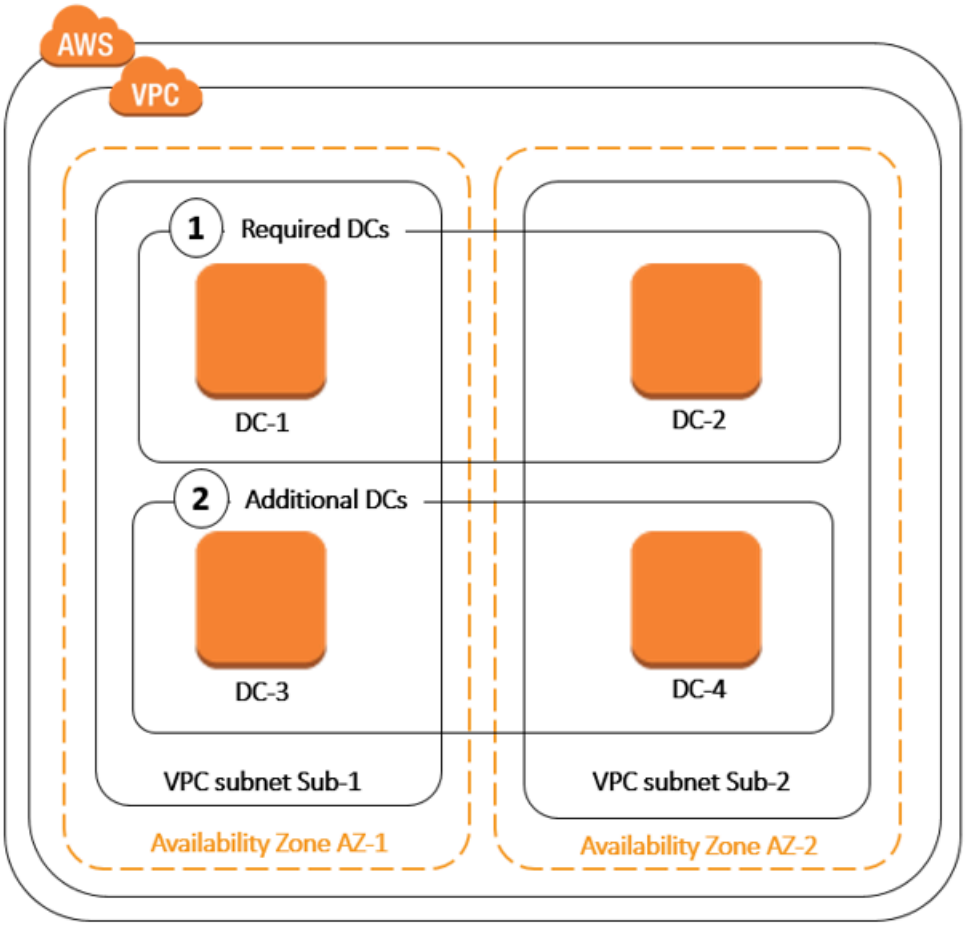
部署其他網域控制器

部署其他網域控制器可提高備援，進而有更佳的復原能力及更高的可用性。由於支援更多 Active Directory 請求，因此也會提高您目錄的效能。例如，您現在可以使用 AWS 受管 Microsoft AD 來支援

部署在亞馬遜 EC2 和亞馬 Amazon RDS for SQL Server 執行個體的大型叢集上的多個 .NET 應用程式。

當您第一次建立您的目錄時，AWS 受管理的 Microsoft AD 會跨多個可用區域部署兩個網域控制站，這是高可用性目的所需。稍後，只要指定您想要的網域控制站總數，就可以透過 AWS Directory Service 主控台輕鬆部署其他網域控制站。AWS 受管 Microsoft AD 會將額外的網域控制站散佈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。主控 AWS Directory Service 台會將這些預設網域控制站稱為 [必要]。AWS 受管理的 Microsoft AD 會在目錄建立程序期間，刻意在不同的可用區域中尋找這些網域控制站。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)。和以前一樣，AWS 受管理的 Microsoft AD 會再次自動將新的網域控制站放置在不同的可用區域，以確保您的網域的高可用性。



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。它也可讓您更輕鬆地在 AWS 雲端中遷移及執行關鍵任務 Active Directory 整合式工作負載，而不需要部署及維護您

自己的 Active Directory 基礎設施。您也可以使用 UpdateNumberOfDomainControllersAPI 部署或移除 AWS 受管理 Microsoft AD 的其他網域控制站。

> **Note**
>
> 其他網域控制站是 AWS 受管理的 Microsoft AD 的區域功能。如果您使用 多區域複製，則必須在每個區域中單獨執行以下程序。如需詳細資訊，請參閱 全域與區域功能。

新增或移除其他域控制站

在新增或刪除其他域控制站之前，以下有關域控制站要求的詳細資訊供您參考：

- 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 受管理的 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 啟用安全的 LDAP 或 LDAP。

使用下列程序，在您的 AWS Managed Microsoft AD 目錄中部署或移除其他域控制站。

新增或移除其他網域控制器

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. AWS 受管 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，而且指派的可用區域和 Amazon VPC 子網路都會出現。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。

相關 AWS 安全部落格文章

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

將使用者從 Active Directory 遷移到 AWS Managed Microsoft AD

您可以使用使用中目錄移轉工具組 (ADMT) 搭配密碼匯出服務 (PES)，將使用者從您自我管理的作用中目錄移轉至受AWS管理的 Microsoft AD 目錄。這可讓您更輕鬆地為使用者移轉 Active Directory 物件和加密密碼。

有關詳細說明，請參閱 AWS 安全部落格上的 How to migrate your on-premises domain to AWS Managed Microsoft AD using ADMT 一文。

AWS 管理 Microsoft AD 的最佳做法

以下是您應該考慮的一些建議和指導方針，以避免發生問題並充分利用 AWS 受管理的 Microsoft 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 提供多種與其他 AWS 服務搭配使用的方式。您可以依所需功能及成本預算，選擇目錄服務：

- AWS Directory Service 的 Microsoft 活動目錄是一個功能豐富的託管在雲上 AWS 託管。 AWS 如果您有 5,000 個以上的使用者，而且需要在 AWS 託管目錄與內部部署目錄之間設定信任關係，則受管理 Microsoft AD 是您的最佳選擇。
- AD 連接器只是將您現有的內部部署連接Active Directory到 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。
- S@@ imple AD 是具有基本Active Directory相容性的低規模、低成本的目錄。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。

如需更詳細的 AWS Directory Service 選項比較，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「AWS 管理 Microsoft AD 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 實例加入您的 AWS 受管 Microsoft AD 活動目錄」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」。

瞭解目錄的 AWS 安全性群組組態和使用方式

AWS 建立安全性群組，並將其附加至目錄的網域控制站彈性網路介面。此安全群組封鎖到域控制站的不必要流量，並允許進行 Active Directory 通訊所必要的流量。 AWS 將安全群組設定為僅開啟進行 Active Directory 通訊所需的連接埠。在預設組態中，安全性群組會接受來自任何 IP 位址的這些連接埠的流量。 AWS 將安全性群組附加至您的網域控制站的介面，這些介面可從對等或調整大小的 VPC 中存取。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，您可以予以修改，使其接受來自更嚴謹之 IP 地址清單的流量。例如，您可以將接受的地址從 0.0.0.0/0 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。不當的變更可能會導致與預定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站的其他連接埠，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。但是， AWS 建議不要這種做法。 AWS 可能有理由修改安全性群組，恕不另行通知，以解決受

管理目錄的功能或安全性需求。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。目錄安全群組接受必要 Active Directory 連接埠上來自任何 IP 地址的流量。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。

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。該帳戶識別碼是管理 Microsoft AD 的 AWS 管理員。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

建議您為 AWS Directory Service 目錄建立 DHCP 選項集，並將 DHCP 選項設定指派給目錄所在的 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 DHCP 選項集」。

啟用條件式轉寄站設定

下列條件式轉寄設定將此條件式轉寄器儲存在 Active Directory 中，複寫方式如下：應啟用。啟用這些設定可防止因基礎結構故障或過載失敗而更換節點時，條件式轉寄站設定消失。

部署其他網域控制器

根據預設， AWS 會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 為可用於建構使用者名稱的大多數字元格式提供支援。但是，在用戶名上強制執行字符限制，這些用戶名將用於登錄 AWS 應用程序 WorkSpaces，例如 Amazon WorkDocs WorkMail，Amazon 或 Amazon 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。

使用您的目錄

以下是使用目錄時需謹記的一些建議。

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 來啟動目錄時， AWS 會建立包含所有目錄物件的組織單位 (OU)。此 OU 有您在建立目錄時所輸入的 NetBIOS 名稱，位於根網域中。網域根目錄擁有及管理 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。這樣做可能會使您的目錄無法訪問您自己和 AWS. 如需詳細資訊，請參閱 什麼被創建與 AWS 管理 Microsoft AD 活動目錄。

自動加入域

啟動屬於網域的 Windows 執行個體時，通常最簡單的方法是將 AWS Directory Service 網域加入為執行個體建立程序的一部分，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 執行個體無縫加入您的 AWS 受管 Microsoft AD Active Directory」中找到詳細資訊。

正確設定信任

在您的 AWS 受管理 Microsoft AD 目錄與其他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「建立信任關係」。

管理您的目錄

考慮以下針對管理目錄的建議。

追蹤域控制站效能

為了協助最佳化擴展決策並改善目錄恢復能力和效能，建議您使用 CloudWatch 指標。如需詳細資訊，請參閱 透過效能指標監控域控制站。

如需有關如何使用 CloudWatch 主控台設定網域控制站指標的指示，請參閱 AWS 安全性部落格中的如何根據使用率指標自動化 AWS 受管 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 擴展您的結構描述。

關於負載平衡器

請勿在 AWS 受管理的 Microsoft AD 端點前面使用負載平衡器。Microsoft 設計的 Active Directory (AD) 搭配一種網域控制站 (DC) 探索演算法使用，可找出具最佳回應速度的運作 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，請參閱負載平衡器和 Microsoft 上的作用中目錄， TechNet 其中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，請先建立備份或建立該執行個體的快照。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 建立目錄快照或還原目錄。

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。

另請記住，如果您有接收訊息的 SNS 主題 AWS Directory Service，則在從 Amazon SNS 主控台刪除該主題之前，應將目錄與其他 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 SNS 設定目錄狀態通知。

應用程式目錄服務設定

AWS 受管理的 Microsoft AD 可讓您自訂安全性組態，以符合您的合規性和安全性需求。 AWS 受管理的 Microsoft AD 會將組態部署並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。您可以按照 API 中編輯目錄安全設定或透過 UpdateSettings API 中的步驟，在主控台中執行此操作。

如需詳細資訊，請參閱 設定目錄安全設定。

刪除目錄前先移除 Amazon 企業應用程式

刪除與一或多個 Amazon 企業應用程式 (例如、、Amazon 應用程式管理員 WorkSpaces、Amazon WorkSpaces WorkDocs、Amazon 關聯式資料庫服務或 Amazon RDS) 相關聯的目錄之前，您必須先移除每個應用程式。 WorkMail AWS Management Console如需移除應用程式的詳細資訊，請參閱刪除您 AWS 託管的 Microsoft AD相關文章。

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

用戶端電腦會使用伺服器訊息區 (SMB) 來存取群組原則、登入指令碼和其他檔案的 AWS 受管理 Microsoft AD 網域控制站上的 SYSVOL 和 NETLOGON 共用。 AWS 管理 Microsoft AD 僅支援中小企業 2.0 版 (SMBv2) 及更新版本。

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。您的目錄可以正常運作，但 SMBv1 用戶端將無

法連線到 AWS 受管理的 Microsoft AD 網域控制站的 SYSVOL 和 NETLOGON 共用，而且也將無法處理群組原則。

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。若要深入了解如何停用 SMBv1 並將其更新為系統上較新的 SMB 版本，請參閱 Microsoft TechNet 和 Support 部門上的這些張貼文章。

追蹤 SMBv1 遠端連線

您可以從遠端連線至 AWS 受管理的 Microsoft AD 網域控制站，檢閱 Microsoft SMB伺服器/稽核視窗事件記錄檔，此記錄檔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Windows PowerShell指令程式集-。SmbServerConfiguration

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 管理 Microsoft AD 的動態 DNS (DDNS) 服務來尋找網域控制站 (DC)。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。這種情況也可能會導致 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 部署其他網域控制器。

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 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	20
手動快照 *	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 ***	5
每個企業 Microsoft AD 的共享域 ***	125
每個目錄的已登錄憑證授權機構 (CA) 憑證數目上限	5
單一 AWS Managed Microsoft AD (企業版) 目錄中的 AWS 區域的數目上限 ****	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。如需更多詳細資訊，請參閱 主要區域與其他區域。

> **Note**
>
> 您無法將公有 IP 地址附加至 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，請參閱編寫程式設計自己的應用程式相關文章。

有關儲存和物件配額，請參閱 AWS Directory Service 定價頁面上的比較表。

AWS 管理 Microsoft AD 的應用程式相容性

AWS Directory Service 的 Microsoft 活動目錄（AWS 管理 Microsoft AD）與多個 AWS 服務和第三方應用程序兼容。

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。
- Amazon EC2 – 如需詳細資訊，請參閱 將 Amazon EC2 實例加入您的 AWS 受管 Microsoft AD 活動目錄。
- Amazon QuickSight -有關更多信息，請參閱在 Amazon QuickSight 企業版中管理用戶帳戶。
- Amazon RDS for MySQL – 如需詳細資訊，請參閱針對 MySQL 使用 Kerberos 身分驗證。
- Amazon RDS for Oracle – 如需詳細資訊，請參閱搭配 Amazon RDS for Oracle 使用 Kerberos 身分驗證。
- Amazon RDS for PostgreSQL – 如需詳細資訊，請參閱搭配 Amazon RDS for PostgreSQL 使用 Kerberos 身分驗證。
- Amazon RDS for SQL Server – 如需詳細資訊，請參閱搭配 Amazon RDS Microsoft SQL Server 資料庫執行個體使用 Windows 身分驗證。
- Amazon WorkDocs -如需詳細指示，請參閱使用 AWS 受管 Microsoft AD 連接到現場部署目錄。
- Amazon WorkMail -有關詳細說明，請參閱將 Amazon WorkMail 與現有目錄集成（標準設置）。

- AWS Client VPN -如需詳細說明，請參閱用戶端驗證和授權。
- AWS IAM Identity Center -如需詳細指示，請參閱將身分識別中心連線到內部部署 Active Directory。
- AWS License Manager -如需詳細資訊，請參閱中的基於使用者的 AWS License Manager訂閱。
- AWS Management Console -如需詳細資訊，請參閱啟用 AD 憑證存取 AWS Management Console。
- FSx for Windows File Server – 如需詳細資訊，請參閱什麼是 FSx for Windows File Server。
- WorkSpaces -如需詳細指示，請參閱 WorkSpace 使用 AWS 受管理的 Microsoft AD 啟動。

由於使用 Active Directory 的自訂和商業 off-the-shelf 應用程式的規模，並 AWS 不能執行正式或廣泛的驗證協力廠商應用程式的相容性與 AWS Directory Service 的 Microsoft Active Directory（AWS 託管 Microsoft AD）。雖然與客戶合 AWS 作，試圖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與 AWS Managed Microsoft AD 相容或將繼續相容。

下列協力廠商應用程式與 AWS 受管理的 Microsoft AD 相容：

- Active Directory 類型啟用 (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(以前稱為 Azure Active Directory (AzureAD))
- Microsoft Entra Connect(以前稱為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 永遠在可用性群組上)
- Microsoft System Center Configuration Manager(SCCM)-建置 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。因為 AWS 必須保留此權限層級的專屬控制權，才能以受管理服務的形式傳遞 Active Directory，因此您無法以網域系統管理員的身分來安裝這類應用程式。不過，您通常可以將特定、較低權限和 AWS 受支援的權限委派給執行安裝的人員，藉此安裝此類應用程式。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。如需有關 AWS 允許您委派之權限的詳細資訊，請參閱什麼被創建與 AWS 管理 Microsoft AD 活動目錄。
- 存取特權Active Directory容器 — 在您的目錄中， AWS 受管理的 Microsoft AD 會提供組織單位 (OU)，讓您擁有完整的系統管理控制權。針對在 Active Directory 中層級比您的 OU 高的容器，您沒有建立或寫入的權限，而且讀取權限可能有限。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。如需管理 OU 的詳細資訊，請參閱 如何管理 AWS Managed Microsoft AD相關文章。
- 安裝工作流程期間的結構描述變更 — 某些Active Directory應用程式需要變更預設 Active Directory 結構描述，而且可能會嘗試將這些變更安裝為應用程式安裝工作流程的一部分。由於結構描述延伸模組的權限性質， AWS 只要透過 AWS Directory Service 主控台、CLI 或 SDK 匯入輕量型目錄交換格式 (LDIF) 檔案，即可實現此目錄。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至目錄。如需 LDIF 匯入程序運作方式的詳細資訊，請參閱教學課程：擴充 AWS 受管理的 Microsoft AD 架構 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

下面列出了我們沒有找到與 AWS 託管 Microsoft AD 一起使 off-the-shelf 用的配置的常見請求的商業應用程序。 AWS 隨時自行決定更新此列表，以便幫助您避免無生產力的努力。 AWS 提供這些信息，而無需擔保或聲明有關當前或 future 的兼容性。

- 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

AWS Microsoft AD 測試實驗室託管教程

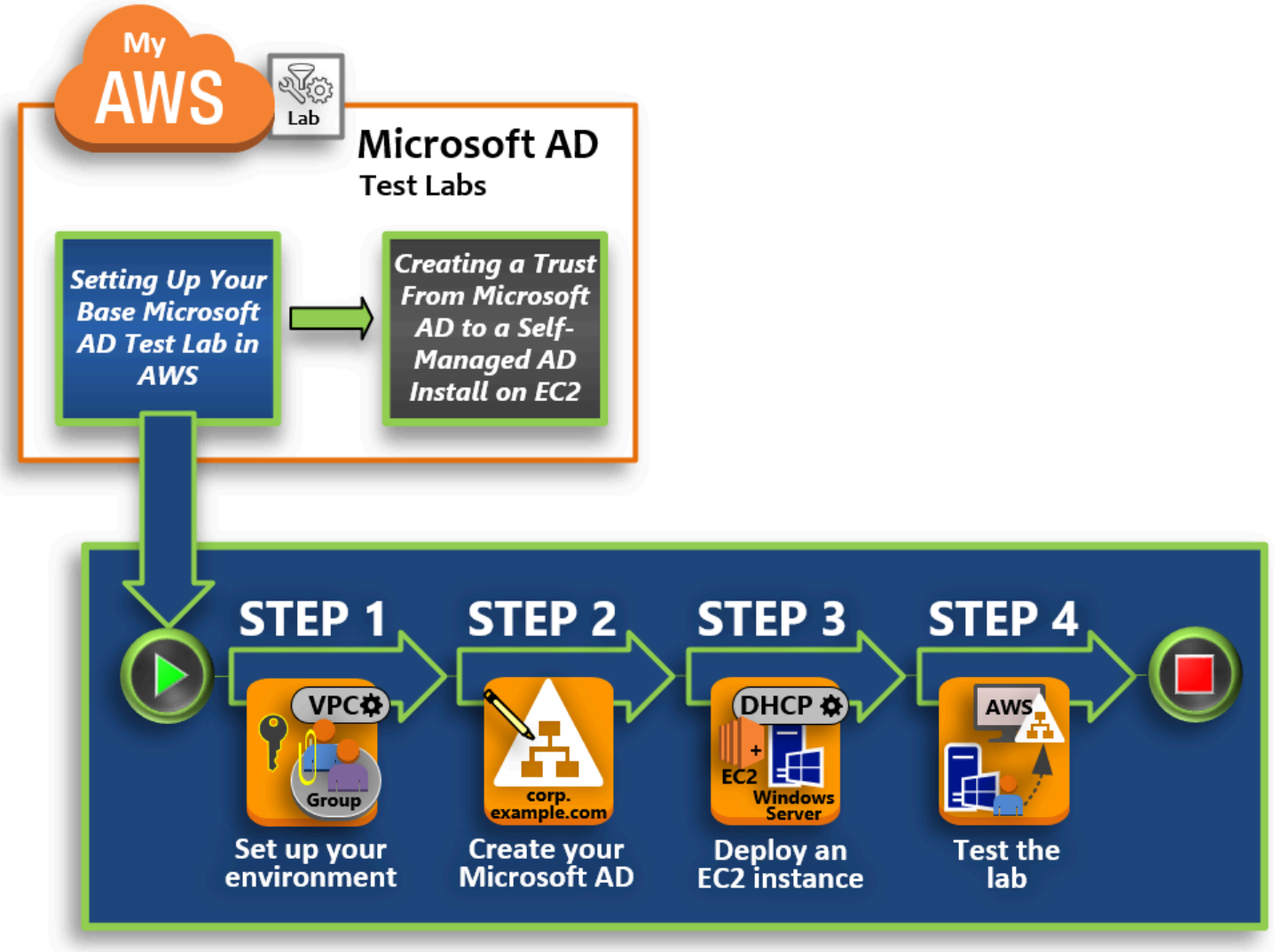
本節提供一系列引導式教學課程，協助您建立測試實驗室環境，讓您可以在 AWS 其中嘗試 AWS 受管理 Microsoft AD。

主題

教學課程：設定您的基礎 AWS 管理 Microsoft AD 測試實驗室 AWS

本教學課程將教導您如何設定 AWS 環境，以準備使用執行 Windows 伺服器 2019 的新 Amazon EC2 執行個體的新 AWS 受管 Microsoft AD 安裝。然後，它會教導您使用典型的活動目錄管理工具，從 EC2 Windows 實例管理您的 Microsoft AD 環境。 AWS 當您完成教學課程時，您將會設定網路必要條件，並設定新的 AWS 受管理 Microsoft AD 樹系。

如下圖所示，您從本教學課程建立的實驗室是實際學習 AWS 受管理 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。



第 1 步：設置您的 AWS 環境 AWS 管理 Microsoft AD 活動目錄

完成先決條件任務後，您可以在 EC2 執行個體中建立並設定 Amazon VPC。

第 2 步：創建 AWS 管理 Microsoft AD 活動目錄

在這個步驟中，您是第一次設定 AWS 受管理 AWS 的 Microsoft AD。

步驟 3：部署 Amazon EC2 執行個體以管理您的 AWS 受管 Microsoft AD 活動目錄

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。

必要條件

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」。但是，如果您打算使用 AWS CLI 命令或 AWS Tools for Windows PowerShell 模塊來創建測試實驗室環境，則必須首先配置以下內容：

- 具有存取和秘密存取金鑰的 IAM 使用者 — 如果要使用 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 （ 可選) — 下載並安裝在視窗 AWS CLI 上。一旦安裝，打開命令提示符或Windows PowerShell窗口，然後鍵入`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 存取金鑰識別碼 [無]：`AKIAIOSFODNN7EXAMPLE`
  - AWS 秘密存取金鑰 [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}
```

第 1 步：設置您的 AWS 環境 AWS 管理 Microsoft AD 活動目錄

在您的 AWS 測試實驗室中建立 AWS 受管 Microsoft AD 之前，您必須先設定 Amazon EC2 key pair，以便所有登入資料都經過加密。

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 金鑰配對的詳細資訊，請參閱建立金鑰配對。

建立一組金鑰對

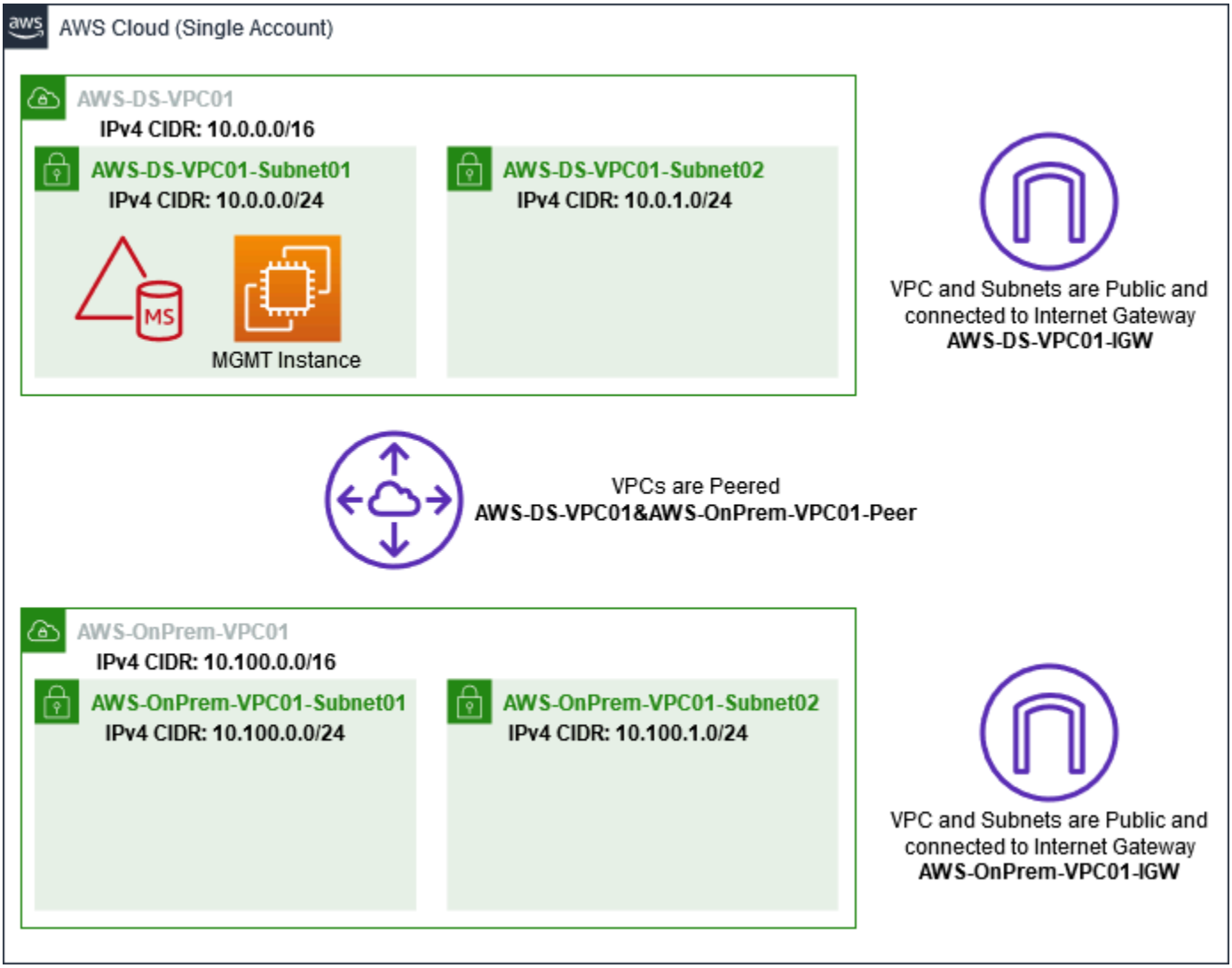
1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。

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 VPC

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 範例都使用下方的 VPC 資訊，並且內建於 US-西 -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同一帳戶中建立兩個 VPC。 AWS 託管 Microsoft AD 支持使用單獨的帳戶與共享您的目錄功能。第一個 VPC 將用於 AWS 管理 Microsoft AD。第二個 VPC 將用於稍後可在 教學：建立從 AWS Managed Microsoft AD 到 Amazon EC2 上自我管理 Active Directory 安裝的信任 中使用的資源。

受管理的使用中目錄 VPC 資訊	內部部署 VPC 資訊
產品名稱標籤: AWS-DS-VPC1	產OnPrem品名稱標籤: AWS

受管理的使用中目錄 VPC 資訊	內部部署 VPC 資訊
IPv4 CIDR 區塊：10.0.0.0/16 IPv6 CIDR block (IPv6 CIDR 區塊): 無 IPv6 CIDR 區塊 租用：預設	IPv4 CIDR 區塊：10.100.0.0/16 IPv6 CIDR block (IPv6 CIDR 區塊): 無 IPv6 CIDR 區塊 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 AWS 管理 Microsoft AD 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
產 AWS品名稱標籤: 虛擬私人電腦:電腦版 AWS 可用區域：us-west-2a IPv4 CIDR 區塊：10.0.0.0/24	產OnPrem品名稱標籤: AWS 虛擬私人電腦:電腦-XXXXXXXX-VPC01 AWS OnPrem 可用區域：us-west-2a IPv4 CIDR 區塊：10.100.0.0/24
產品名稱標籤: AWS-DS-VPC 虛擬私人電腦:電腦版 AWS 可用區域：us-west-2b IPv4 CIDR 區塊：10.0.1.0/24	產OnPrem品名稱標籤： AWS 虛擬私人電腦:電腦-XXXXXXXX-VPC01 AWS OnPrem 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 Internet Gateway 資訊
產品名稱標籤： AWS-DS-VPC01-IGW	產品名稱標籤： AWS-VPC01 OnPrem-IGW
虛擬私人電腦:電腦版 AWS	虛擬私人電腦:電腦-XXXXXXXX-VPC01 AWS OnPrem

如需詳細說明，請參閱 Internet gateways (網際網路閘道)。

步驟四：在 AWS-DS-VPC01 和-VPC01 之間設定虛擬私人電腦對等連線 AWS OnPrem

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 VPC，但本教學課程將使用 VPC 對等互連。 AWS 受管理的 Microsoft AD 支援許多解決方案來連接您的 VPC，其中一些包括 VPC 對等互連、Transit Gateway 和 VPN。

對等連線名稱標籤： AWS-DS-VPC01 AWS OnPrem

VPC (請求者): AWS

帳戶：我的帳戶

區域：此區域

VPC (接受器): 電 AWS腦 OnPrem

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：新增兩個路由到每個 VPC 的主路由表

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。

您可以透過篩選 VPC 名稱標籤 (AWS-DS-VPC01 或--VPC01)，輕鬆找到每個 VPC 的正確路由表。AWS OnPrem

AWS-DS-VPC01 路由 1 資訊	AWS-DS-VPC01 路由 2 資訊	AWS OnPrem-一號路線資訊	AWS OnPrem-二號路線資訊
目的地：0.0.0.0/0 目標：IGW AWS	目的地：10.10 0.0.0/16 目標：電腦-VPC AWSAWS OnPrem	目的地：0.0.0.0/0 目標：IGW-虛擬電腦 AWS	目的地：10.0.0.0/16 目標：電腦-VPC AWSAWS OnPrem

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)。

為 Amazon EC2 執行個體建立安全群組

根據預設， AWS 受管理的 Microsoft AD 會建立安全性群組，以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：
安全組名稱： AWS DS 測試實驗室安全組
說明： AWS DS 測試實驗室安全組
虛擬私人電腦:電腦版 AWS

AWS-DS-VPC01 的安全性群組輸入規則

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

Type	通訊協定	連接埠範圍	來源	流量類型
所有流量	全部	全部	10.0.0.0/16	所有本機 VPC 流量

AWS-DS-VPC01 的安全性群組輸出規則

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 安全性群組資訊：
安全組名稱： AWS OnPrem 測試實驗室安全組。
描述： AWS OnPrem 測試實驗室安全組。
虛擬私人電腦:電腦-XXXXXXXX-VPC01 AWS OnPrem

下列項目的安全性群組輸入規則 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

Type	通訊協定	連接埠範圍	來源	流量類型
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

下列項目的安全性群組輸出規則 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)。

第 2 步：創建 AWS 管理 Microsoft AD 活動目錄

您可以使用三種不同的方法來建立目錄。您可以使用 AWS Management Console 程序 (本自學課程建議使用)，也可以使用 AWS CLI 或 AWS Tools for Windows PowerShell 程序來建立目錄。

方法 1：要創建 AWS 管理 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：要創建 AWS 管理 Microsoft AD（Windows PowerShell）（可選）

1. 打開 Windows 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：要創建 AWS 管理 Microsoft AD（AWS CLI）（可選）

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 受管 Microsoft AD 活動目錄

在這個實驗室中，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。在生產環境中，您可以使用只能透過 VPN 或 AWS Direct Connect 連結存取的私有 VPC 中的執行個體。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。

可選：為您的目錄建立一個在 AWS-DS-VPC01 中設定的 DHCP 選項

在此選用程序中，您可以設定 DHCP 選項範圍，讓 VPC 中的 EC2 執行個體自動使用 AWS 受管 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. 前往 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**
>
> 若要尋找這些位址，請移至 [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，將 Windows 執行個體加入您的 AWS 管理 Microsoft AD 網域

使用此程序設定將 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 執行個體無縫加入您的 AWS 受管 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：

   - 選取亞馬遜 SSM 管理策略旁邊的核ManagedInstanceCore取方塊。此政策提供使用 Systems Manager 服務所需的最低權限。
   - 選取亞馬遜 SSM 受管理策略旁邊的核DirectoryServiceAccess取方塊。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. 在角色名稱中，輸入角色名稱，該名稱說明該角色用於將執行個體加入網域，例如 EC2 DomainJoin。
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，您可以在 EC2 執行個體中設定 Windows 伺服器系統，稍後可用於管理使用中目錄中的使用者、群組和政策。

建立 EC2 執行個體並自動加入目錄

1. 在 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***)。
- 對於 IAM 角色，請選擇您為執行個體角色指定的名稱建立角色，將 Windows 執行個體加入您的 AWS 管理 Microsoft AD 網域，例如 EC2 DomainJoin。
- 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。您可以使用伺服器管理員 UI (建議在本教學課程中使用) 或Windows 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. 如果您尚未取得密碼，請在 Connect To Your Instance (連接至您的執行個體) 對話方塊中，選擇 Get Password (取得密碼) 取回您的密碼，然後選擇 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**)。
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
    - 使用中的目錄模組 Windows 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 實例上安裝活動目錄工具（Windows PowerShell）（可選）

1. 啟動 Windows 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 伺服器是否已正確設定、可以連線至 corp.example.com 網域，以及用來管理您 AWS 的受管理 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] 底下，請注意您在本教學課程的步驟 2 中建立 AWS 受管理的 Microsoft AD 時自動建立的網域控制站名稱。

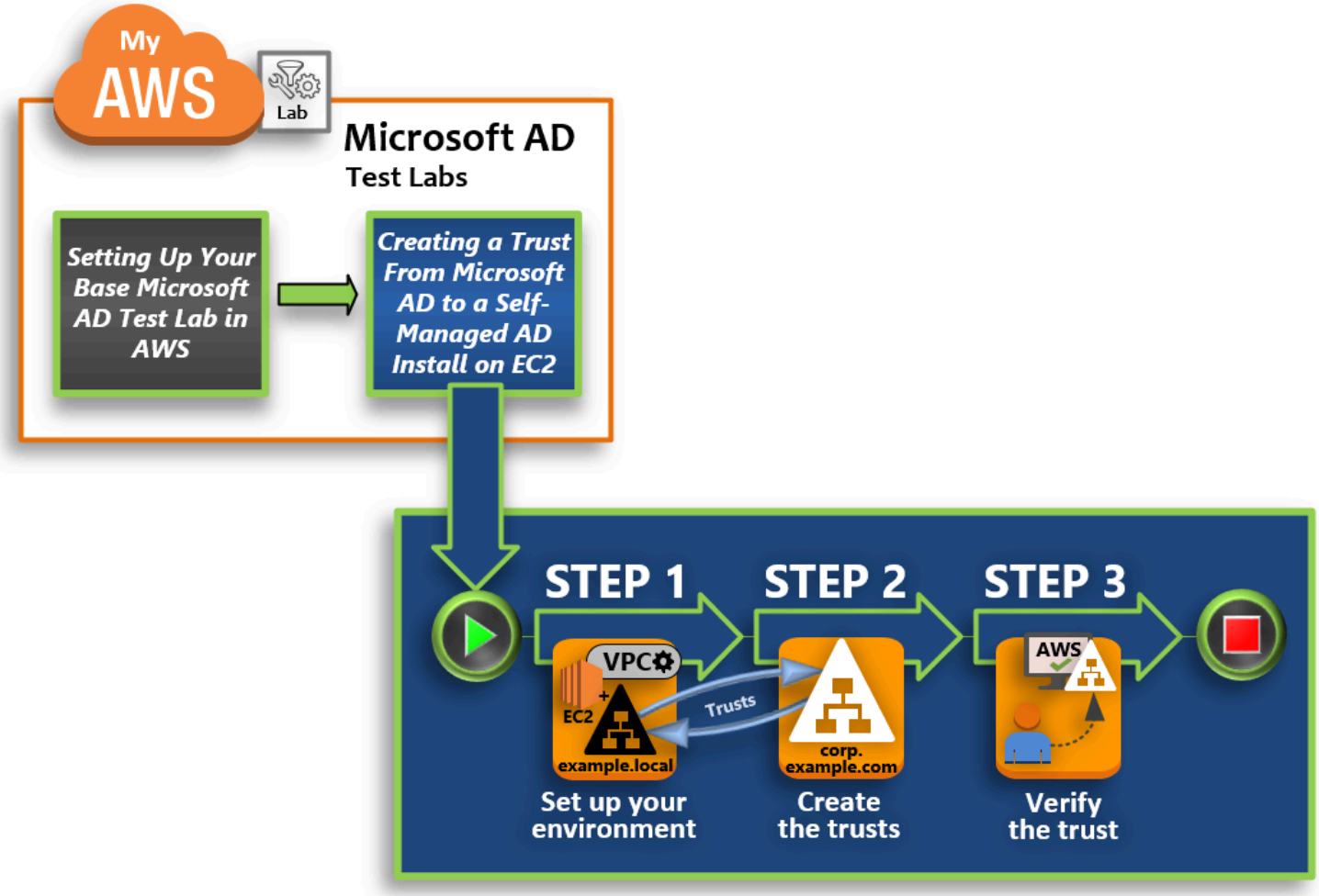
恭喜您！您的 AWS 受管理 Microsoft AD 基礎測試實驗室環境現在已經設定完成。您可以開始新增系列中的下一個測試實驗室。

下一個教學：「教學：建立從 AWS Managed Microsoft AD 到 Amazon EC2 上自我管理 Active Directory 安裝的信任」

教學：建立從 AWS Managed Microsoft AD 到 Amazon EC2 上自我管理 Active Directory 安裝的信任

在本教學中，您將了解如何在您於基礎教學中建立的 AWS Directory Service for Microsoft Active Directory 樹系之間建立信任。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，您從此教學建立的實驗室是設定完整 AWS Managed Microsoft AD 測試實驗室所必備的第二個建置區塊基礎。您可以使用測試實驗室來測試純雲端或混合雲端式 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

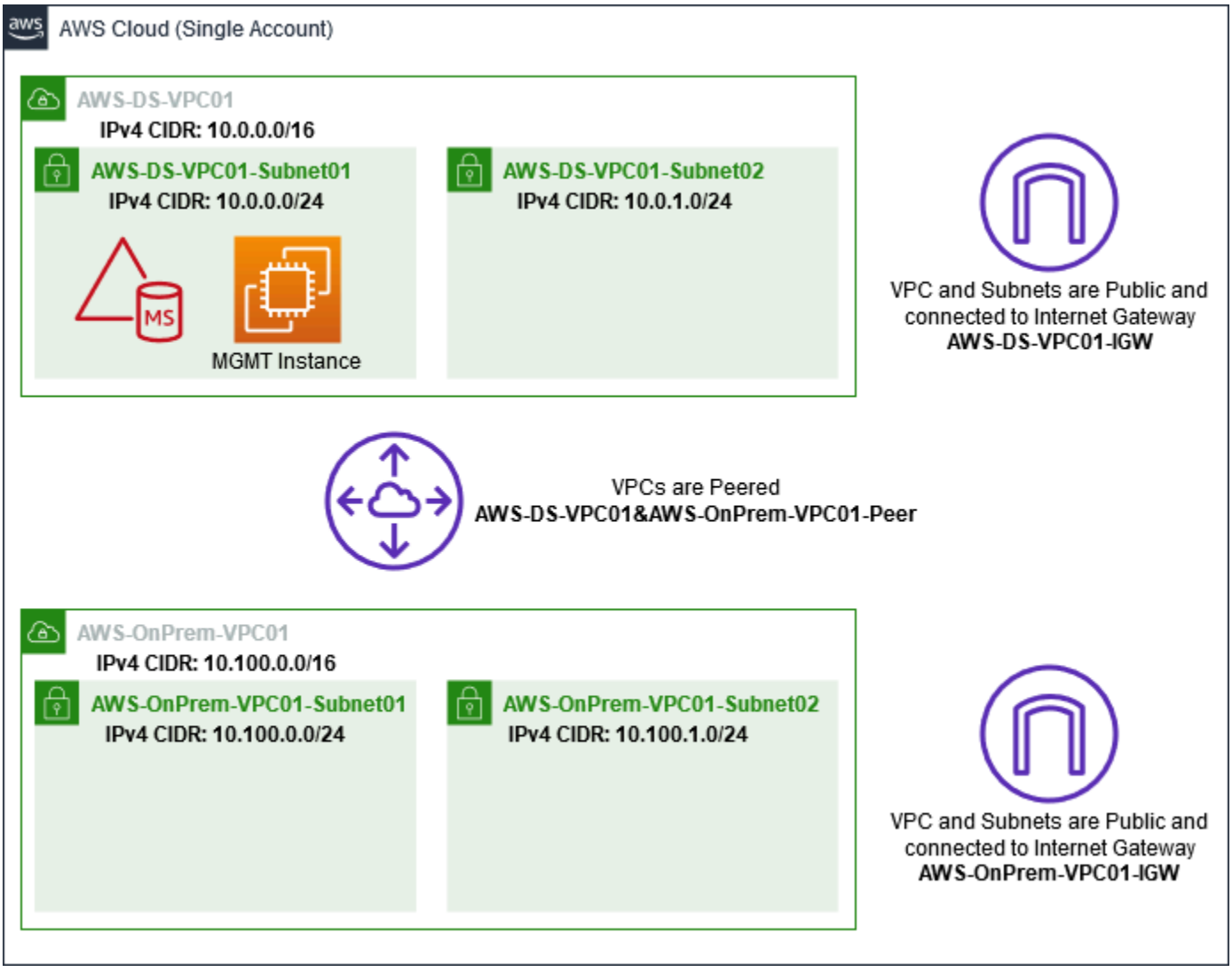
在此步驟中，您會在 Amazon EC2 中所託管之新建立的 Active Directory 樹系與 AWS 中的 AWS Managed Microsoft AD 樹系之間，建立雙向林信任關係。

步驟 3：驗證信任

最後，身為管理員，您會使用 AWS Directory Service 主控台來驗證新的信任可運作。

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，並準備好要與 AWS 建立信任的 VPC。



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：
   - 對於「網路」，請選取「vpc-***xxxxxxxxxxx*** AWS-OnPrem VPC01」(您先前在「基準」自學課程中設置)。
   - ***############-AWS OnPrem AWS OnPrem***
   - 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 AWS 中建立域控制站並複寫為您的內部部署網路，您必須先手動將 EC2 執行個體加入您的內部部署域。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。
    - 在指定網域控制站功能下，確認已選取網域名稱系統 (DNS) 伺服器和通用類別目錄 (GC)。
    - 輸入目錄服務還原模式 (DSRM) 密碼並確認。然後選擇 Next (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 [其他選項] 頁面上，確定 [範例] 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，記下您之前在基礎教學中建立之 corp.example.com 的 AWS 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 Directories (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 按一下這裡新增...，輸入您 AWS Managed Microsoft AD 目錄的第一個 DNS 地址 (您在上一個程序中記下的值)，然後按 Enter 鍵。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 域建立而來，另一個信任是從 AWS 中的 AWS Managed Microsoft AD 建立而來。

建立從 EC2 域到 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 多區域複製，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。

建立從 AWS Managed Microsoft AD 到 EC2 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上一個程序中設定的相同信任類型 (建立從 EC2 域到 AWS Managed Microsoft AD 的信任)。

   - 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 Add (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。

疑難排解 AWS 管理 Microsoft AD

以下可協助您針對建立或使用目錄時可能遇到的一些常見問題進行故障診斷。

AWS 管理 Microsoft AD 的問題

某些疑難排解工作只能由完成 AWS Support。以下是一些任務：

- 重新啟動您 AWS Directory Service提供的網域控制站。
- 升級您的 AWS 管理 Microsoft AD 活動目錄.

若要建立支援案例，請參閱建立支援案例和案例管理。

Netlogon 安全通道通訊的問題

作為 CVE–2020–1472 的緩解措施，Microsoft 發佈了修補程序，該修補程序修改了域控制站處理 Netlogon 安全通道通訊的方式。由於引進了這些安全的 Netlogon 變更，某些 Netlogon 連線 (伺服器、工作站和信任驗證) 可能不會接受您的 AWS 管理 Microsoft AD。

若要驗證您的問題是否與 Netlogon 或安全通道通訊有關，請在 Amazon CloudWatch 日誌中搜尋事件識別碼 5827 (針對裝置身份驗證相關問題) 或 5828 (針對 AD 信任驗證相關問題)。如需有關 AWS 受管理 Microsoft AD CloudWatch 中的資訊，請參閱啟用日誌轉發。

如需 CVE–2020–1472 緩解措施的詳細資訊，請參閱 Microsoft 網站上的如何管理 Netlogon 中與 CVE-2020-1472 相關聯的 Netlogon 安全通道連線中的變更一文。

密碼復原

如果使用者忘記密碼，或在登入您的 Simple AD 或 AWS 受管理 Microsoft AD 目錄時遇到問題，您可以使用 AWS Management Console、Windows PowerShell或. AWS CLI

如需詳細資訊，請參閱 重設使用者密碼。

其他資源

下列資源可協助您在使用時進行疑難排解 AWS。

- AWS 知識中心：尋找常見問題集和其他資源的連結，以協助您疑難排解問題。
- AWS S@@ upport 中心 — 取得技術支援。
- AWS 頂級 Support 中心 — 取得頂級技術支援。

主題

- 使用 Microsoft 事件檢視器監控 DNS 伺服器
- Linux 域加入錯誤
- Active Directory 低可用儲存空間
- 結構描述延伸錯誤

- 信任建立狀態原因

使用 Microsoft 事件檢視器監控 DNS 伺服器

您可以稽核您的 AWS Managed Microsoft AD DNS 事件，讓您更輕鬆地識別 DNS 問題並進行故障診斷。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，請參閱什麼被創建與 AWS 管理 Microsoft AD 活動目錄相關文章。

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. 找到加入您 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. 選取其他電腦，輸入您的 AWS Managed Microsoft AD DNS 伺服器名稱或 IP 地址的其中一個，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)。

Linux 域加入錯誤

以下內容可協助您疑難排解將 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 實例必須在 DNS 中進行反向解析，然後一個領域才能與 Microsoft 活動目錄一起工作。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，嘗試使用網域認證進入執行個體的 SSH 可能會失敗，並顯示下列錯誤：

$ 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受管理的 Microsoft AD 和內部部署 Active Directory 之間建立了單向傳出信任，則在嘗試使用 Winbind 的受信任 Active Directory 認證對網域加入的 Linux 執行個體進行驗證時，可能會遇到驗證問題。

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

7 月 31 日 00:05: 請求失敗:WBC_ER_AUTH 錯誤, PAM_ 溫綁定 (身份驗證): 請求 wbcLogonUser 失敗:WBC_ER_ 驗證錯誤, PAM 錯誤:系統錯誤:找不到錯誤訊息:物件名稱。

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
```

Active Directory 低可用儲存空間

當您的 AWS Managed Microsoft AD 因 Active Directory 的可用儲存空間過低而受到損害時，您需要立即採取動作來使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 儲存空間的定價資訊，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。任何非必要的檔案都應存放在您 AWS Managed Microsoft AD 域控制站以外的檔案伺服器。

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。如果您不想要自行管理檔案伺服器，AWS 提供了受管檔案伺服器選項 Amazon FSx。

如要移除任何非必要的檔案，您可以透過通用命名慣例 (UNC) 路徑來存取 SYSVOL 共享。例如，如果您網域的完整網域名稱 (FQDN) 是 example.com，則 SYSVOL 的 UNC 路徑就會是 “\\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。如果在 30 分鐘後目錄仍未回到作用中狀態，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 會在 AD 資源回收筒中保留項目 180 天，之後這些項目才會成為 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 支援的物件數目的詳細資訊，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 管理 AWS Managed Microsoft AD 中的使用者和群組。

```
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標準版本，請向 AWS Support 開啟案例，請求將您的目錄升級至企業版本。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 Delegated Deleted Object Lifetime Administrators 群組具備修改 `msDS-DeletedObjectLifetime` 屬性的能力，這項屬性會設定遭刪除物件在成為 Recycled-Objects 前於 AD 資源回收筒中保留的時間長度 (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。如需更多詳細資訊，請參閱 建立目錄快照或還原目錄。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。如果您想要使生命週期更長或更短，請將 “30” 取代成任何您偏好的數字。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

以下內容可協助您在延伸 AWS Managed Microsoft AD 目錄結構描述時，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. The extended server error is: 0000202B: RefErr: DSID-0310082F, data 0, 1 access points \tref 1: ‘example.com’ Number of Objects Modified: 0

疑難排解

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

疑難排解

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

疑難排解

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

疑難排解

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

疑難排解

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

疑難排解

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. The extended server error is: 0000208D: NameErr: DSID-03100238, problem 2,001 (NO_OBJECT), data 0, best match of: 'CN=Schema,CN=Configuration,DC=example,DC=com' Number of Objects Modified: 0

疑難排解

辨別名稱 (DN) 所參考的物件不存在。

信任建立狀態原因

當信任建立失敗時，狀態訊息會包含額外的資訊。以下是可協助您了解這些訊息意義的一些資訊。

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。為解決此問題，請嘗試以下操作：

- 受 AWS 管理的 Microsoft AD Active Directory 和Active Directory您想要建立信任關係的自我管理，必須具有相同的第一個網站名稱。「第一個站台」名稱設定為`Default-First-Site-Name`。如果這些名稱因網域而異，就會發生拒絕存取錯誤。
- 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

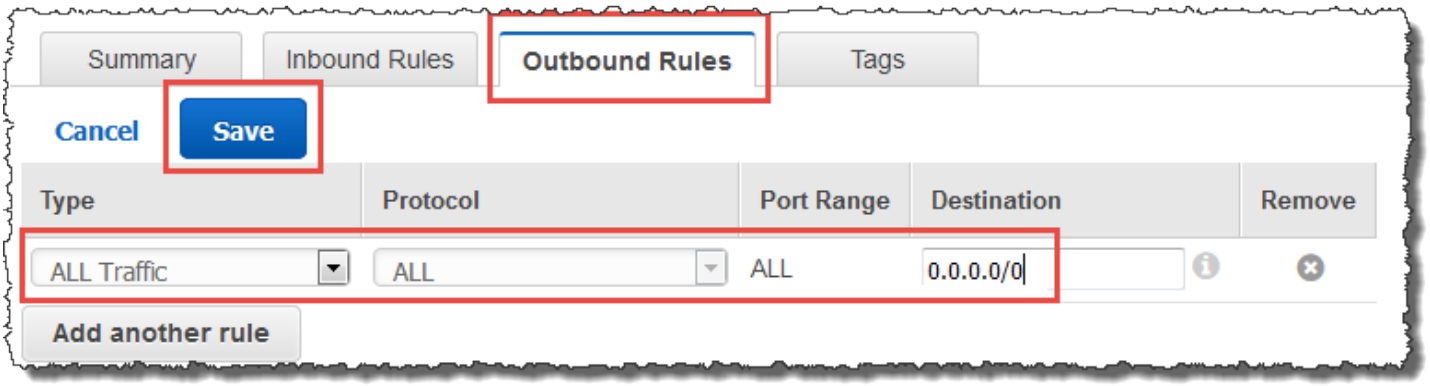
- 確認上述命名管道是否存在於NullSessionPipes登錄路徑 HKLM\ SYSTEM\ 服務\LanmanServer\ 參數中的登錄機碼上的值。CurrentControlSet這些值必須插入到單獨的列中。

> **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`。

- 確認預設網域控制站原則中的下列伺服器訊息區 (SMB) 簽署設定。您可以在 [電腦設定] > [Windows 設定] > [安全性設定] > [本機原則/安全性選項] 下找到這些設定。它們應該符合下列設定：
  - Microsoft網路用戶端：數位簽署通訊 (一律)：預設值：啟用
  - Microsoft網路用戶端：數位簽署通訊 (如果伺服器同意)：預設值：已啟用
  - Microsoft網路伺服器：數位簽署通訊 (永遠)：已啟用
  - Microsoft網路伺服器：數位簽署通訊 (如果用戶端同意)：預設值：已啟用

指定的網域名稱不存在或無法聯絡

為解決此問題，請確定您域的安全群組設定與您 VPC 的存取控制清單 (ACL) 皆正確，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 必要條件。

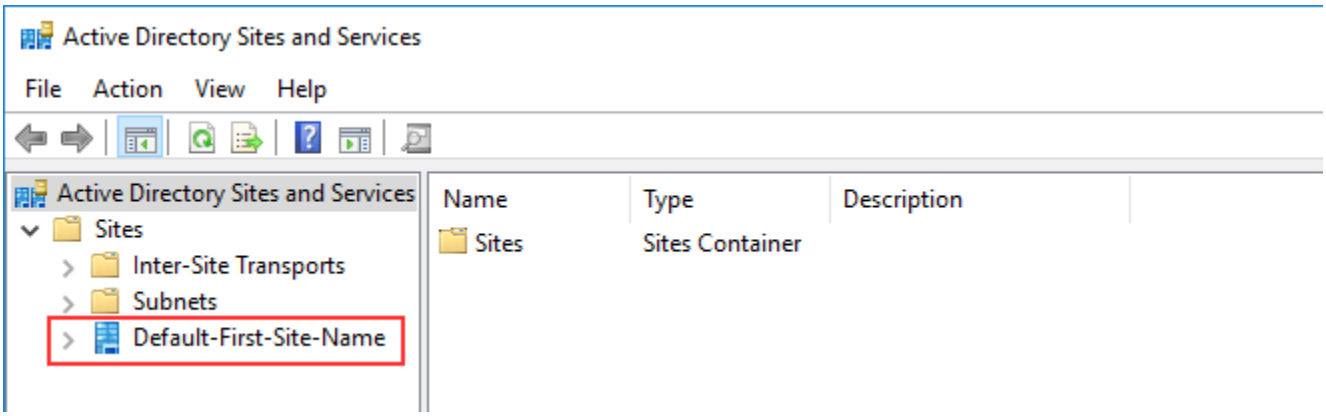
網際網路號碼分配局 (IANA) 為私有網際網路保留了以下三個 IP 地址空間區塊：

- 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://tools.ietf.org/html/rfc1918。

確認 AWS 受管理 Microsoft AD 的預設 AD 站台名稱與內部部署基礎結構中的預設 AD 網站名稱相符。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。

如需其運作方式的詳細資訊，請參閱網站上跨樹系信任的Microsoft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 受管理的 Microsoft AD 不支援具有單一標籤網域的信任。如需詳細資訊，請參閱單一標籤網域的Microsoft支援。
- 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，請參閱遵守網站上主機和Microsoft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 自動化疑難排

Sup@@ port 自動化工作流程（SAW）利用 AWS Systems Manager 自動化為 AWS Directory Service 您提供預定義的手冊。AWSSupport-TroubleshootDirectoryTrust runbook 工具可協助您診斷 AWS 受管理 Microsoft AD 與內部部署MicrosoftActive Directory之間的常見信任建立問題。

DirectoryServicePortTest 工具

當疑難排解 AWS 受管理的 Microsoft AD 與內部部署 Active Directory 之間的信任建立問題時，DirectoryServicePortTest測試工具會很有幫助。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。有關如何使用這些工具的示例，請參閱網站上的 Netdom 和 NLTEST。Microsoft

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 是目錄閘道，可供您將目錄請求重新導向至您的內部部署 Microsoft Active Directory，而無需快取任何雲端資訊。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 不支援作用中目錄轉移信任。AD 連接器和您的內部部署作用中目錄網域具有 1 對 1 的關聯性。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。如果這是一項要求，請考慮使用 AWS Managed Microsoft AD 來 共享您的目錄。AD Connector 也不能感知多 VPC，這表示類似WorkSpaces的AWS應用程式必須佈建到與 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登入AWS應用程式 WorkDocs，例如 WorkSpaces Amazon 或 Amazon WorkMail。
- 您可以透過以 IAM 角色為基礎的 AWS Management Console 存取權，管理 AWS 資源，如 Amazon EC2 執行個體或 Amazon S3 儲存貯體。
- 無論使用者或 IT 管理員存取您內部部署基礎設施或 AWS 雲端的資源，您都可以一致地強制執行現有的安全政策 (如密碼過期、密碼歷史記錄和帳戶鎖定)。
- 您可以使用 AD Connector 與您現有的 RADIUS 型 MFA 基礎設施整合，來啟用多重驗證，以在使用者存取 AWS 應用程式時，多一層安全保護。

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
- 如何管理 AD Connector
- AD Connector 的最佳實務

- AD Connector 配額
- AD Connector 應用程式相容性政策
- AD Connector 疑難排解

AD Connector 入門

使用 AD Connector，您可以連接 AWS Directory Service 到您現有的企業活動目錄。連線到現有目錄時，所有目錄資料都會保留在網域控制站上。 AWS Directory Service 不會複製任何目錄資料。

主題

- AD Connector 事前準備
- 建立 AD Connector
- 什麼獲取與您的 AD Connector 創建

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。構成目錄的 EC2 執行個體在您的 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」

若要取得有關的更多資訊 AWS Direct Connect，請參閱AWS Direct Connect 使用者指南。

現有 Active Directory

您需要連接到具有Active Directory域的現有網絡。

> **Note**
>
> AD Connector 不支援單一標籤域。

此Active Directory網域的功能層級必須是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
- 將電腦加入網域-僅在使用無縫網域加入和 WorkSpaces
- 建立電腦物件-僅在使用無縫網域加入和 WorkSpaces
- 服務帳戶密碼應符合 AWS 密碼需求。 AWS 密碼應該是：

- 長度介於 8 到 128 個字元之間，包括在內。
- 至少包含以下四種類別中的三個字符：
  - 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。驗證是由 AWS 內部服務處理，該服務使用 Kerberos 票證以使用者身分執行 LDAP 作業。

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 上的 SRV 資源記錄。 TechNet

子網路的連接埠

若要讓 AD Connector 將目錄請求重新導向至您現有的網Active Directory域控制站，您現有網路的防火牆必須對 Amazon VPC 中兩個子網路的 CIDR 開放下列連接埠。

- 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 器和 Amazon WorkSpaces，您的網域控制站必須設定為 0。這是網域控制站的預設設定。如果已啟用停用 LvLvSupport 屬性，則 AD Connector 將無法查詢目錄中的使用者。如此可防止 AD Connector 使用 Amazon WorkSpaces。

> **Note**
>
> 如果您現有網域的 DNS 伺服器或網Active Directory域控制站伺服器位於 VPC 內，則與這些伺服器相關聯的安全性群組必須對 VPC 中兩個子網路的 CIDR 開放上述連接埠。

如需其他連接埠需求，請參閱Microsoft文件中的 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。如需有關此設定的一般資訊，請移至預先驗證的Microsoft TechNet。

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 前提

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 連接器已在 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 使用指南中的 IAM 身分中心先決條件。

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伺服器的預設 RADIUS AWS Directory Service 伺服器連接埠 (1812) 輸入流量。
- 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 為 AD Connector 啟用多重因素認證。

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`、委派連線 AWS Directory Service 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。

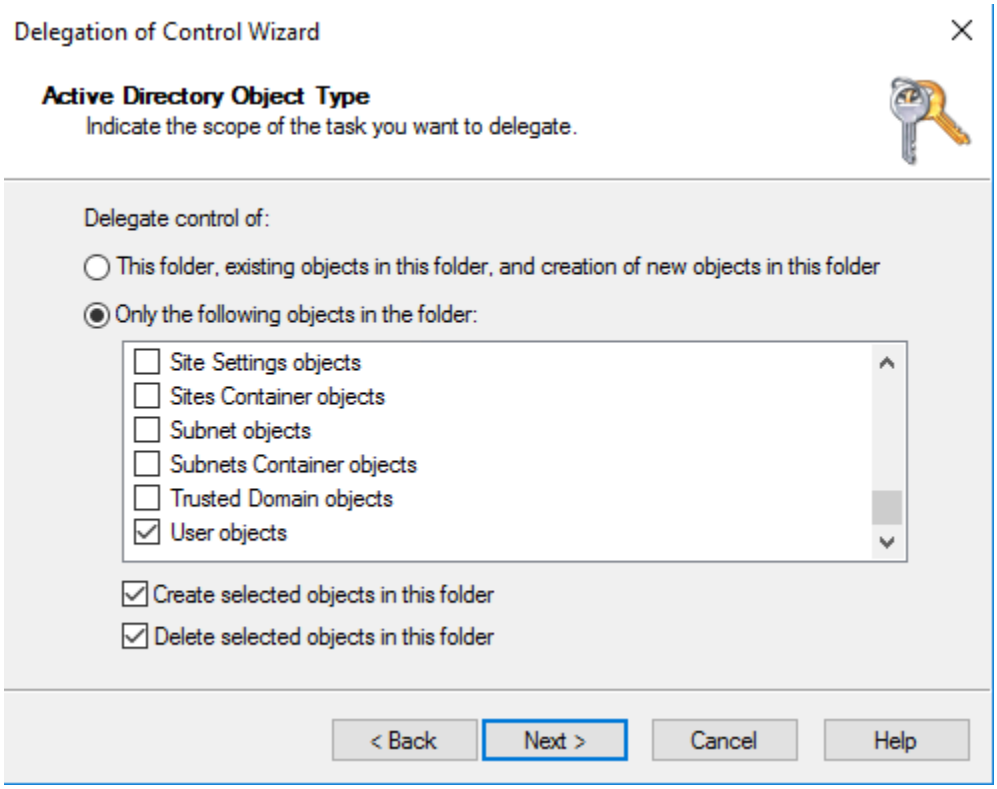
委派權限給您的服務帳戶

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)。

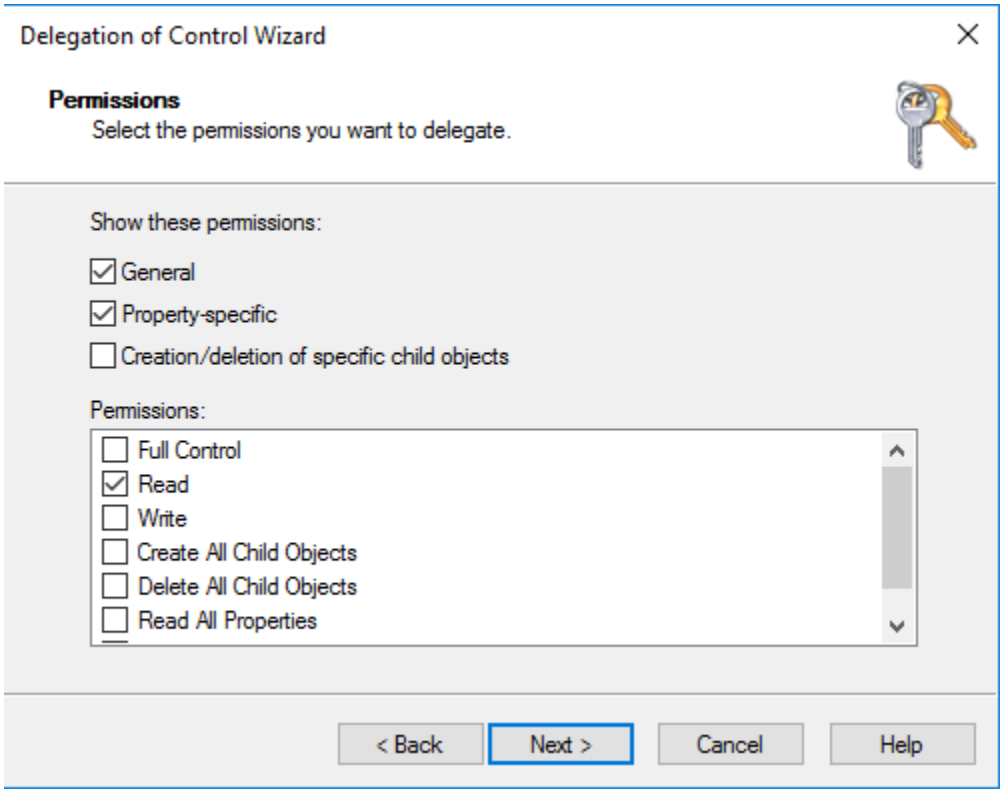
欄位	值/選項
Group name (群組名稱)	`Connectors`
Group scope (群組範圍)	全域
Group type (群組類型)	安全性

4. 在 Active Directory User and Computers (Active Directory 使用者和電腦) 導覽樹狀目錄中，選取您的根網域。在選單中，選取 Action (動作)，再選取 Delegate Control (委派控制)。如果您的 AD 連接器連線到 AWS 受管理的 Microsoft AD，您將無法存取網域根層級的委派控制項。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**
>
> 如果您將使用無縫網域加入 WorkSpaces，或者，您也必須啟用寫入權限，以便 Active Directory 可以建立電腦物件。



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。此使用者將稱為您的 AD Connector 服務帳戶，因為它現在是Connectors群組的成員，因此現在擁有足夠的權限可連線 AWS Directory Service 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**
>
> 只有當網域和樹系功能層級設定為 Windows 伺服器 2012 R2 及以下版本時，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

   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 位址之間有網路連線 AWS，這些伺服器就可以位於的外部。

   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)。

什麼獲取與您的 AD Connector 創建

建立 AD Connector 時， AWS Directory Service 會自動建立 elastic network interface (ENI)，並將其與每個 AD Connector 執行個體建立關聯。這些 ENI 中的每一個對於 VPC 和 AWS Directory Service AD 連接器之間的連接都是必不可少的，因此不應刪除。您可以 AWS Directory Service 通過以下描述來識別所有保留用於的網絡接口：「為目錄目錄 ID AWS 創建的網絡接口」。如需詳細資訊，請參閱《適用於 Windows 執行個體的 Amazon EC2 使用者指南》中的彈性網路介面一節。

> **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。

當您登入任何與 AD Connector 器 (AWS IAM Identity Center 內含) 整合的應用程 AWS 式或服務時，應用程式或服務會將您的驗證要求轉送至 AD Connector 器，然後將要求轉送至您自我管理 Active Directory 中的網域控制站以進行驗證。如果您已成功驗證自我管理的 Active Directory，AD Connector 著會將驗證權杖傳回給應用程式或服務 (類似於 Kerberos 權杖)。此時，您現在可以訪問該 AWS 應用程序或服務。

如何管理 AD Connector

本節列出所有操作和維護 AD Connector 環境的程序。

主題

- 保護您的 AD Connector 目錄
- 監控您的 AD Connector 目錄
- 將 EC2 執行個體加入您的 Active Directory 目錄
- 維護您的 AD Connector 目錄
- 啟用對應用 AWS 程式和服務的存取

- 為 AD Connector 更新 DNS 地址

保護您的 AD Connector 目錄

本節說明保護 AD Connector 環境的安全考量。

主題

- 在 AWS Directory Service 中更新 AD Connector 服務帳戶憑證
- 為 AD Connector 啟用多重因素認證
- 使用 AD Connector 啟用用戶端 LDAPS
- 在 AD Connector 中啟用 mTLS 身分驗證以與智慧卡配合使用
- 設定 AD 的 AWS Private CA 連接器

在 AWS Directory Service 中更新 AD Connector 服務帳戶憑證

您在 AWS Directory Service 中提供的 AD Connector 憑證代表存取您現有內部部署目錄所用的服務帳戶。您可以執行下列步驟來在 AWS Directory Service 中修改服務帳戶登入資料。

> **Note**
>
> 如果啟用目錄的 AWS IAM Identity Center，AWS Directory Service 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 AWS Directory Service 中更新 AD Connector 服務帳戶憑證

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。

為 AD Connector 啟用多重因素認證

當您的 Active Directory 在內部部署或在 EC2 執行個體上執行時，可以啟用 AD Connector 多重要素驗證。如需搭配 AWS Directory Service 使用多重驗證的詳細資訊，請參閱 AD Connector 事前準備。

> **Note**
>
> 多重要素驗證不可用於 Simple AD。不過，您可以在 AWS Managed Microsoft AD 目錄啟用 MFA。如需詳細資訊，請參閱為 AWS Managed Microsoft AD 啟用多重要素驗證。

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 Amazon 企業應用程式和服務 (例如 WorkSpaces、Amazon 或亞馬 Amazon QuickSight Chime) 的存取權。AWS Management Console它不提供 MFA 給 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，您必須使用執行 MFA 的解決方案， out-of-band 例如用戶的 SMS 文本驗證。在 out-of-band MFA 解決方案中，您必須確定針對您的解決方案適當地設定 RADIUS 逾時值。使用 out-of-band

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 AWS Directory Service 伺服器透過預設 RADIUS 伺服器連接埠 (UDP:1812) 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 支援的用戶端 LDAPS 會將 Microsoft Active Directory (AD) 和 AWS 應用程式之間的通訊加密。此類應用程式包括 WorkSpaces、AWS IAM Identity Center、Amazon QuickSight 和 Amazon Chime 等。此加密有助於保護您組織的身分資料並符合您的安全要求。

主題

- 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。

主題

- 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 流量僅在 TCP 連接埠 636 上執行，不會回復到 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。將 AWS 安全群組和網路防火牆設為允許 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 或 AWS CLI。

主題

步驟 1：將憑證登錄於 AWS Directory Service

使用以下任一方法將憑證登錄於 AWS Directory Service。

方法 1：若要將您的憑證登錄於 AWS Directory Service (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 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：若要將您的憑證登錄於 AWS Directory Service (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。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：若要在 AWS Directory Service (AWS Management Console) 中檢查憑證登錄狀態

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：若要在 AWS Directory Service (AWS CLI) 中檢查憑證登錄狀態

- 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

使用以下其中一個方法在 AWS Directory Service 中啟用用戶端 LDAPS。

> **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：若要在 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：若要在 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

使用以下其中一個方法，在 AWS Directory Service 中檢查 LDAPS 狀態。

方法 1：若要在 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：若要在 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 或 AWS CLI。

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：若要在 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：若要在 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：若要在 AWS Directory Service (AWS Management Console) 中取消登錄憑證

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：若要取消登錄 AWS Directory Service (AWS CLI) 中的憑證

- 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：若要在 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：若要在 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 身分驗證以與智慧卡配合使用

您可以使用憑證型相互傳輸層安全性 (MTL) 身份驗證搭配智慧卡， WorkSpaces 透過自我管理的 Active Directory (AD) 和 AD Connector 向 Amazon 驗證使用者。啟用後，使用者會在 WorkSpaces 登入畫面選取其智慧卡，然後輸入 PIN 進行驗證，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 中的智慧卡驗證僅適用於下列項目 AWS 區域，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)

主題

- 必要條件
- 啟用智慧卡身分驗證
- 管理智慧卡身分驗證設定

必要條件

若要為 Amazon 用 WorkSpaces 戶端使用智慧卡啟用憑證型相互傳輸層安全性 (MTL) 身份驗證，您需要一個與自我管理整合的操作智慧卡基礎設施。Active Directory如需有關如何使用 Amazon 設定智慧卡身份驗證的詳細資訊 WorkSpaces Active Directory，請參閱 Amazon WorkSpaces 管理指南。

在啟用智慧卡驗證之前 WorkSpaces，請檢閱下列考量事項：

- CA 憑證要求
- 使用者憑證要求
- 憑證撤銷檢查流程
- 其他考量

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「憑證傳輸服務」已設定為「自動」並在執行中。

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 (UPN) 的主體別名 userPrincipalName (SAN)。

- 使用者的智慧卡憑證在智慧卡登入 (1.3.6.1.4.1.311.20.2.2) 用戶端驗證 (1.3.6.1.5.5.7.3.2) 時，使用者的智慧卡憑證具有增強的金鑰使用方式。
- 使用者智慧卡憑證的線上憑證狀態通訊協定 (OCSP) 資訊應為「授權單位資訊存取」中的「存取方法」=「線上憑證狀態通訊協定」(1.3.6.1.5.5.7.48.1)。

如需 AD Connector 和智慧卡身份驗證需求的詳細資訊，請參閱 Amazon WorkSpaces 管理指南中的要求。如需疑難排解 Amazon WorkSpaces 問題 (例如登入 WorkSpaces、重設密碼或連線) 的說明 WorkSpaces，請參閱 Amazon WorkSpaces 使用者指南中的疑難排解用 WorkSpaces 戶端問題。

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 的規定。此外，OCSP 伺服器必須支援使用 GET 方法來處理總共小於或等於 255 位元組之要求的要求。

> **Note**
>
> AD Connector 要求 OCSP 回應程式 URL 為 HTTP URL。

其他考量

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型智慧卡可能可以運作，但尚未經過 WorkSpaces串流通訊協定的測試。
- 智慧卡驗證會將使用者名稱和密碼驗證取代為 WorkSpaces。

  如果您在 AD Connector 目錄中設定了啟用智慧卡驗證的其他 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 WorkSpaces 上啟用智慧卡驗證，首先您需要將憑證授權單位 (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。

主題

- 步驟 1：為 AD Connector 服務帳戶啟用 Kerberos 限制委派
- 步驟 2：在 AD Connector 中登錄 CA 憑證
- 步驟 3：為支援的 AWS 應用程式和服務啟用智慧卡身分驗證

步驟 1：為 AD Connector 服務帳戶啟用 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。這項功能可讓管理員透過限制範圍來指定及強制執行應用程式信任邊界，其中應用程式服務可代表使用者執行動作。如需更多詳細資訊，請參閱 Kerberos 限制委派。

> **Note**
>
> K@@ erberos 限制委派 (KCD) 需要 AD Connector 服務帳戶的使用者名稱部分，才能符合相同使用者AccountName 的 SAM。SAM 限制AccountName 為 20 個字元。SAM AccountName 是用來作為舊版 Windows 用戶端和伺服器的登入名稱的 Microsoft 活動目錄屬性。

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. 針對使用中目錄中的其他網域控制站重複此程序。或者，您可以使用自動化該過程 PowerShell。

步驟 2：在 AD Connector 中登錄 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。

步驟 3：為支援的 AWS 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。

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。您可以使用該 AWS Management Console 方法或方 AWS CLI 法。

主題

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：若要在 AWS Directory Service (AWS Management Console) 中檢視憑證詳細資料

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：若要在 AWS Directory Service (AWS CLI) 中檢視憑證詳細資料

- 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：若要在 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：若要在 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：若要在 AWS Directory Service (AWS Management Console) 中停用智慧卡驗證

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：若要在 AWS Directory Service (AWS CLI) 中停用智慧卡驗證

- 執行下列命令。

```
aws ds disable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

設定 AD 的 AWS Private CA 連接器

您可以將自我管理的 Active Directory (AD) 與 AWS Private Certificate Authority (CA) 與 AD 連接器整合，以便為 AD 網域加入的使用者、群組和電腦發行和管理憑證。 AWS Private CA AD 連接器可讓您針對自我管理的企業 CA 使用完全受控的 AWS Private CA 嵌入式替代方案，而不需要部署、修補或更新本機代理程式或 Proxy 伺服器。

您可以透過 Directory Service 主控台、AD AWS Private CA 連接器主控台或呼叫 `CreateTemplate`API 來設定與目錄的 AWS Private CA 整合。若要透過使用中目錄的 AWS Private CA 連接器主控台設定私人 CA 整合，請參閱作用中目錄的AWS Private CA 連接器。請參閱以下有關如何從 AWS Directory Service 主控台設定此整合的步驟。

先決條件

使用 AD Connector 時，您需要向服務帳戶委派額外的許可。在服務帳戶上設定存取控制清單 (ACL)，以便您能夠執行下列操作。

- 新增和移除自身的服務主體名稱 (SPN)。
- 在以下容器中建立並更新憑證授權機構：

```
#containers
CN=Public Key Services,CN=Services,CN=Configuration
CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration
CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration
```

- 創建和更新 NT AuthCertificates 證書授權單位對象，如下面的例子。如果 NT AuthCertificates 憑證授權單位物件存在，您必須委派它的權限。如果該物件不存在，您必須委派在公有金鑰服務容器上建立子物件的能力。

```
#objects
CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration
```

> **Note**
>
> 如果您使用的是 AWS 受管理的 Microsoft AD，當您使用目錄授權 AD 服務的 AWS Private CA 連接器時，會自動委派其他權限。

您可以使用下列 PowerShell 指令碼委派其他權限，並建立 NT AuthCertifiates 憑證授權單位物件。將 "myconnectoraccount" 替換為服務帳戶名稱。

```
$AccountName = 'myconnectoraccount'

# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module -Name 'ActiveDirectory'
$RootDSE = Get-ADRootDSE

# Getting AD Connector service account Information
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
$AccountAclPath = $AccountProperties.DistinguishedName

# Getting ACL settings for AD Connector service account.
$AccountAcl = Get-ACL -Path "AD:\$AccountAclPath"

# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AccountAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGuid, 'None'
$AccountAcl.AddAccessRule($AccountAccessRule)
Set-ACL -AclObject $AccountAcl -Path "AD:\$AccountAclPath"

# Add ACLs allowing AD Connector service account the ability to create certification
 authorities
[System.GUID]$CertificationAuthorityGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'certificationAuthority' }
 -Properties 'schemaIDGUID').schemaIDGUID
```

```
$CAAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty,CreateChild,DeleteChild', 'Allow',
 $CertificationAuthorityGuid, 'None'
$PKSDN = "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$PKSACL = Get-ACL -Path "AD:\$PKSDN"
$PKSACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $PKSACL -Path "AD:\$PKSDN"

$AIADN = "CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$AIAACL = Get-ACL -Path "AD:\$AIADN"
$AIAACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $AIAACL -Path "AD:\$AIADN"

$CertificationAuthoritiesDN = "CN=Certification Authorities,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
$CertificationAuthoritiesACL = Get-ACL -Path "AD:\$CertificationAuthoritiesDN"
$CertificationAuthoritiesACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $CertificationAuthoritiesACL -Path "AD:\$CertificationAuthoritiesDN"

$NTAuthCertificatesDN = "CN=NTAuthCertificates,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
If (-Not (Test-Path -Path "AD:\$NTAuthCertificatesDN")) {
New-ADObject -Name 'NTAuthCertificates' -Type 'certificationAuthority' -OtherAttributes
 @{certificateRevocationList=[byte[]]'00';authorityRevocationList=[byte[]]'00';cACertificate=[b
 -Path "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
}

$NTAuthCertificatesACL = Get-ACL -Path "AD:\$NTAuthCertificatesDN"
$NullGuid = [System.GUID]'00000000-0000-0000-0000-000000000000'
$NTAuthAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty', 'Allow', $NullGuid, 'None'
$NTAuthCertificatesACL.AddAccessRule($NTAuthAccessRule)
Set-ACL -AclObject $NTAuthCertificatesACL -Path "AD:\$NTAuthCertificatesDN"
```

設定 AD 的 AWS Private CA 連接器

1. 登入 AWS Management Console 並開啟 AWS Directory Service 主控台，位於https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在 [網路與安全性] 索引標籤下的 [ADAWS Private CA 連接器] 下，選擇 [設定 AD 的 AWS Private CA 連接器]。此時會顯示「建立私人 CA 憑證 Active Directory」頁面。依照主控台上的步驟，為 Active Directory連接器建立私人 CA，以便在私人 CA 中註冊。如需詳細資訊，請參閱建立連接器。
4. 建立連接器後，請按照以下步驟檢視詳細資訊，包括連接器的狀態和關聯的私有 CA 的狀態。

若要檢視 AD 的 AWS Private CA 連接器

1. 登入 AWS Management Console 並開啟 AWS Directory Service 主控台，位於https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories (目錄) 頁面中，選擇目錄 ID。
3. 在網路與安全性中的適用於 AD 的AWS Private CA 連接器下，您可以檢視私有 CA 連接器和關聯的私有 CA。依預設，您會看到下列欄位：

    a. AWS Private CA 連接器 ID — 連接 AWS Private CA 器的唯一識別碼。按一下它會導致該 AWS Private CA 連接器的詳細資料頁面。

    b. AWS Private CA 主旨 — 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 — 以 AWS Private CA 連接器和的狀態檢查為基礎 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 — 建立 AWS Private CA 連接器的日期。

如需詳細資訊，請參閱檢視連接器詳細資訊。

監控您的 AD Connector 目錄

您可以使用下列方法來監控您的 AD Connector 目錄：

主題

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 Support 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 疑難排解 AWS 管理 Microsoft AD、AD Connector 疑難排解、Simple AD 疑難排解。對於一般維護相關問題，請在 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 Support 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 建立目錄快照或還原目錄。

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

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 Support 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 SNS 設定目錄狀態通知

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。使用以下步驟，您可以將 AWS Directory Service 作為發佈者新增至 Amazon SNS 主題。當 AWS Directory Service 偵測到目錄狀態變更時，會將訊息發佈到該主題，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**
>
> 如果您使用僅具有DirectoryServiceFullAccess受管政策的 IAM 使用者或角色登入，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. 選擇建立。

如果您想要指定其他 SNS 訂閱者 (例如其他電子郵件地址、Amazon SQS 佇列) AWS Lambda，或者，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。如果要刪除整個主題，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，請將您的目錄與其他 Amazon SNS 主題建立關聯。

將 EC2 執行個體加入您的 Active Directory 目錄

AD Connector 是目錄閘道，可供您將目錄請求重新導向至您的內部部署 Microsoft Active Directory，而無需快取任何雲端資訊。以下是有關如何將 Amazon EC2 加入 Active Directory 域的詳細資訊：

- 執行個體啟動時，您可以順暢地將 EC2 執行個體加入您的 Active Directory 網域。如需詳細資訊，請參閱將 Windows 執行個體無縫加入 AWS 受管理的 AD 網域。
- 如果您需要手動將 EC2 執行個體加入 Active Directory 網域，則必須在適當 AWS 區域 的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的 Active Directory (內部部署) 後，該執行個體將直接與 Active Directory 通訊並繞過 AD Connector。

主題

- 使用 AD 連接器將 Windows EC2 執行個體無縫連接到您的作用中目錄
- 使用 AD Connector 將 Linux EC2 執行個體無縫加入您的作用中目錄

使用 AD 連接器將 Windows EC2 執行個體無縫連接到您的作用中目錄

此程序可將 Windows EC2 執行個體無縫連接到您的 AWS 受管 Microsoft AD 目錄。

無縫加入 Windows EC2 執行個體

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 在導航欄中，選擇與現有目錄 AWS 區域 相同的目錄。
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。

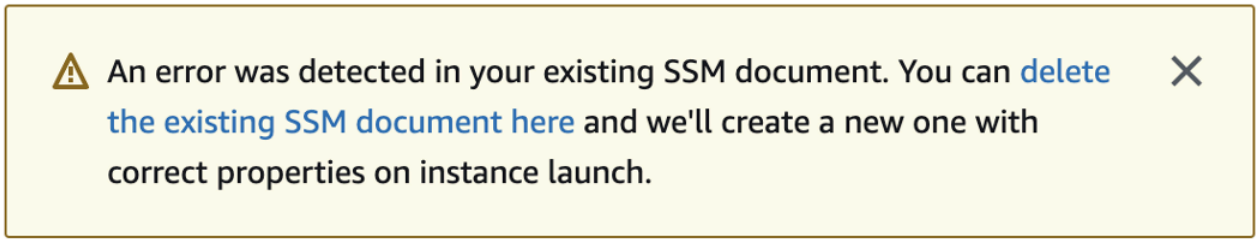
   > **Important**
   >
   > 這是您儲存私有金鑰檔案的唯一機會。

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 地址的詳細資訊，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的 Amazon EC2 執行個體 IP 地址一節。

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 啟動精靈識別具有未預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
>
> - 如果您之前已編輯過 SSM 文件，且預期會有屬性，請選擇 [關閉] 並繼續啟動 EC2 執行個體而不進行任何變更。
> - 選取此處刪除現有 SSM 文件連結以刪除 SSM 文件。這將允許創建具有正確屬性的 SSM 文檔。SSM 文件會在您啟動 EC2 執行個體時自動建立。

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已DirectoryServiceAccess附加 AWS 受管政策 AmazonSSM ManagedInstanceCore 和 AmazonSSM 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 [新增權限] 下方的原則清單中，選取 [亞馬遜 SSM] ManagedInstanceCore 和 [亞馬遜 SSM] 原則。DirectoryServiceAccess在搜尋方塊中，輸入 **SSM** 以篩選政策。選擇下一步。

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess 提供將執行個Active Directory體加入至管理的權限。 AWS Directory Service亞馬遜 SSM ManagedInstanceCore 提供了使用該服務所需的最低權限。 AWS Systems Manager 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。

使用 AD Connector 將 Linux EC2 執行個體無縫加入您的作用中目錄

此程序可將 Linux EC2 執行個體無縫連接到您的 AWS 受管 Microsoft AD 目錄。

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 之前的發行版不支援無縫域加入功能。

必要條件

您需要完成本節中的流程，然後才能設定 Linux EC2 執行個體的無縫域加入。

選取無縫域加入服務帳戶

您可以透過 AD Connector 將 Linux 電腦無縫加入到內部部署 Active Directory 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。您可以使用 AD Connector 服務帳戶。您也可以使用具有足夠權限的任何其他帳戶將電腦加入域。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。

若要將電腦加入網域所需的最低權限委派帳戶，您可以執行下列 PowerShell 命令。您必須從已加入域並安裝了 安裝適用於 AWS 受管理 Microsoft AD 的活動目錄管理工具 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。此命 PowerShell 令會設定權限，以允許服務帳戶在網域的預設電腦容器中建立電腦物件。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。

```
$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。

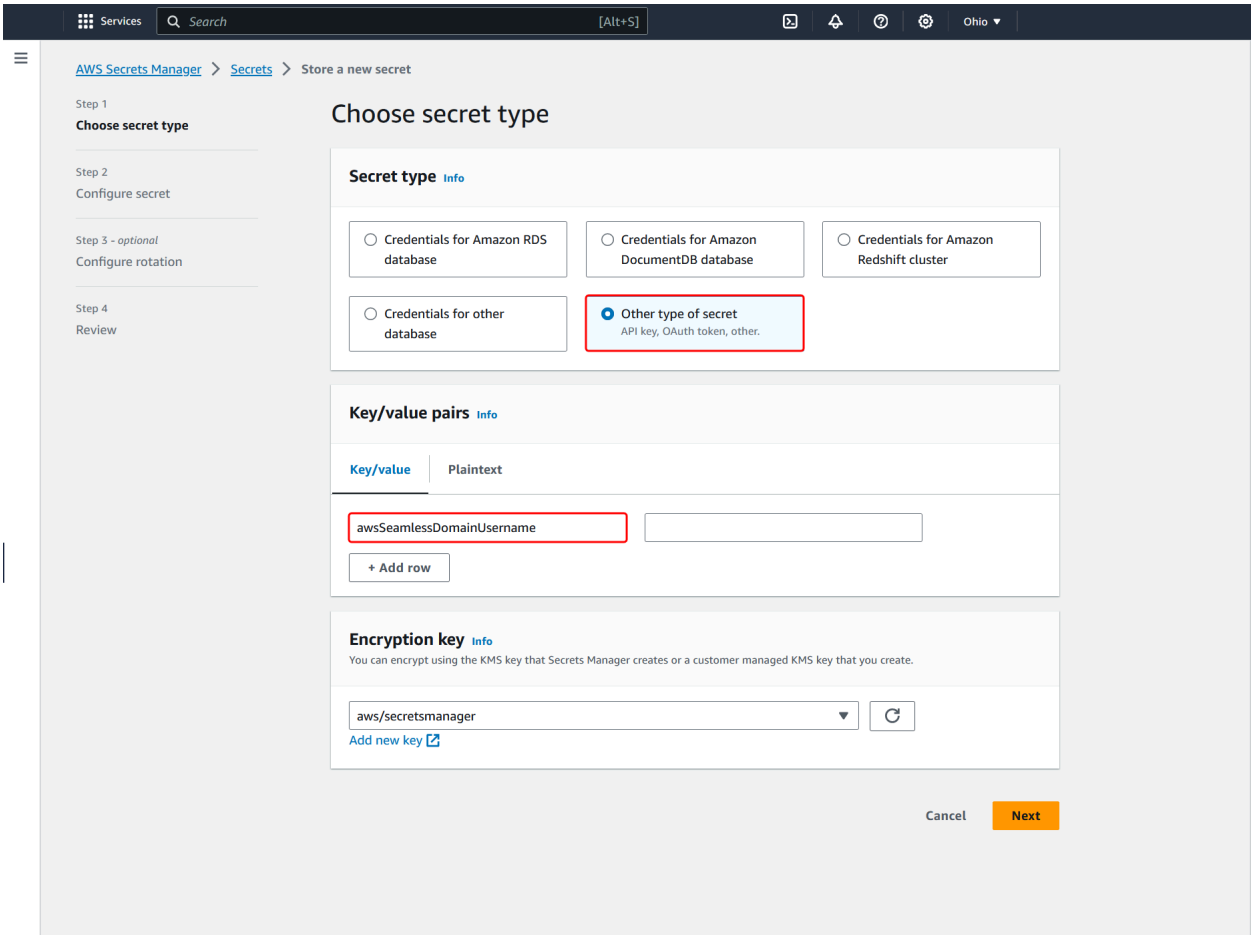
建立儲存域服務帳戶的機密

您可以用 AWS Secrets Manager 來儲存網域服務帳戶。

建立機密並儲存域服務帳戶資訊

1. 請登入 AWS Management Console 並開啟 AWS Secrets Manager 主控台，網址為 https://console.aws.amazon.com/secretsmanager/。
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「其他類型的機密」。
   b. 在「鍵/值配對」下，執行下列操作：
      i. 在第一個方塊中，輸入 **awsSeamlessDomainUsername**。在同一列的下一個方塊中，輸入服務帳戶的使用者名稱。例如，如果您之前使用了該 PowerShell 命令，則服務帳戶名稱將是**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] 底下，保留預設值`aws/secretsmanager`。 AWS Secrets Manager 當您選擇此選項時，一律會加密密碼。您也可以選擇您建立的金鑰。

> **Note**
>
> 根據您使用的秘密 AWS Secrets Manager，有相關費用。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/secretsmanager`的 AWS 受管理金鑰來免費加密您的密鑰。如果您建立自己的 KMS 金鑰來加密密碼，請按照目前的 AWS 費 AWS KMS 率向您收費。如需詳細資訊，請參閱 AWS Key Management Service 定價。

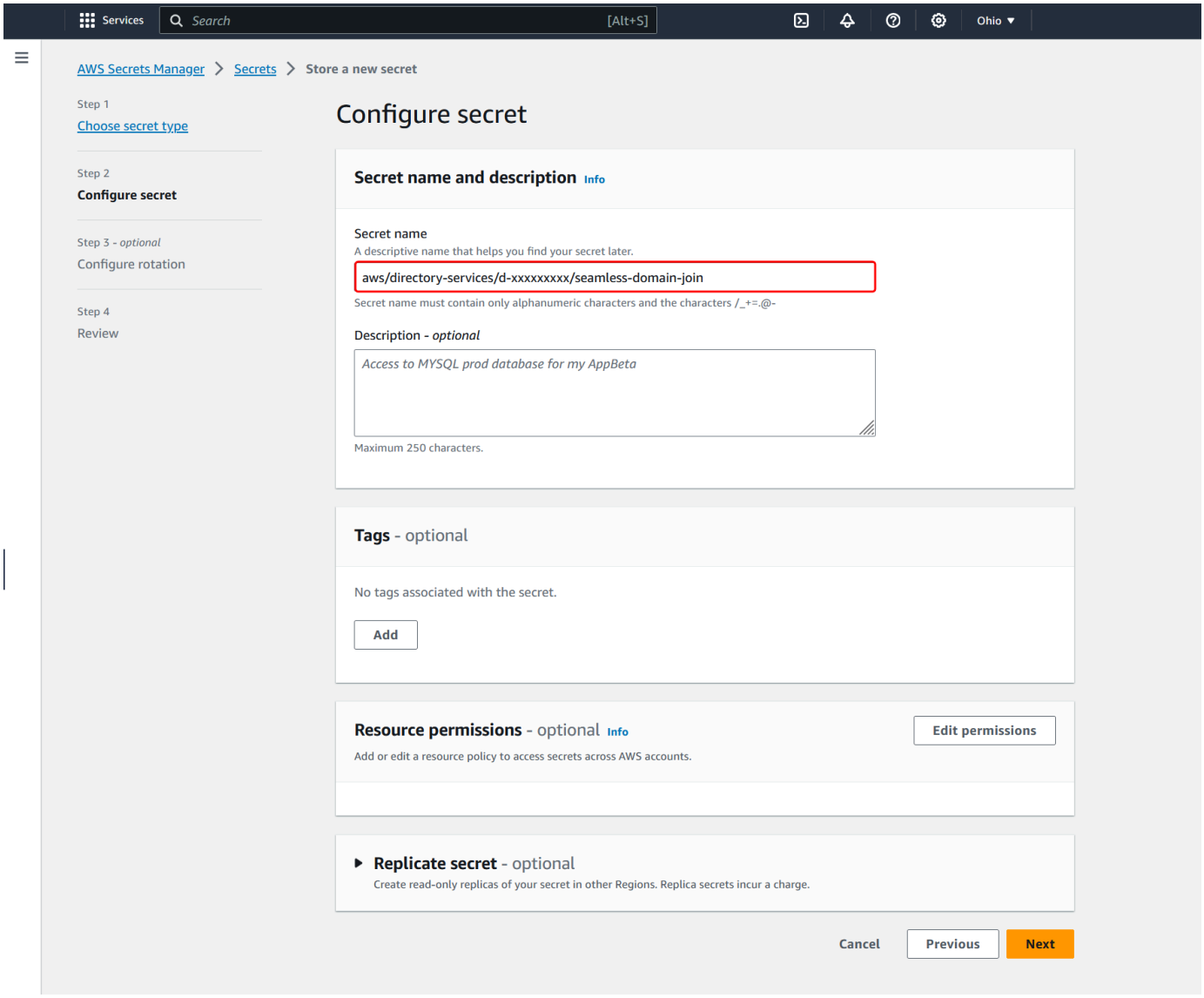
v. 選擇下一步。

4. 在密碼名稱下，使用下列格式輸入包含您目錄 ID 的密碼名稱，並以您的目錄識別碼取代 *d-xxxxxxxxx*：

```
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-xxxxxxxxx* 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。
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。

建立必要的 IAM 政策和角色

使用下列先決條件步驟來建立自訂政策，允許您的 Secrets Manager 無縫網域加入密碼 (您之前建立) 的唯讀存取權限，以及建立新的 LinuxEC2 DomainJoin 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 政策權限的使用者身分登入。 AWS Management Console 前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在功能窗格的 [存取管理] 中，選擇 [原則]。
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**
>
> 請確定您將 [區域] 和 [資源 ARN] 取代為您先前建立的密碼的實際 [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。

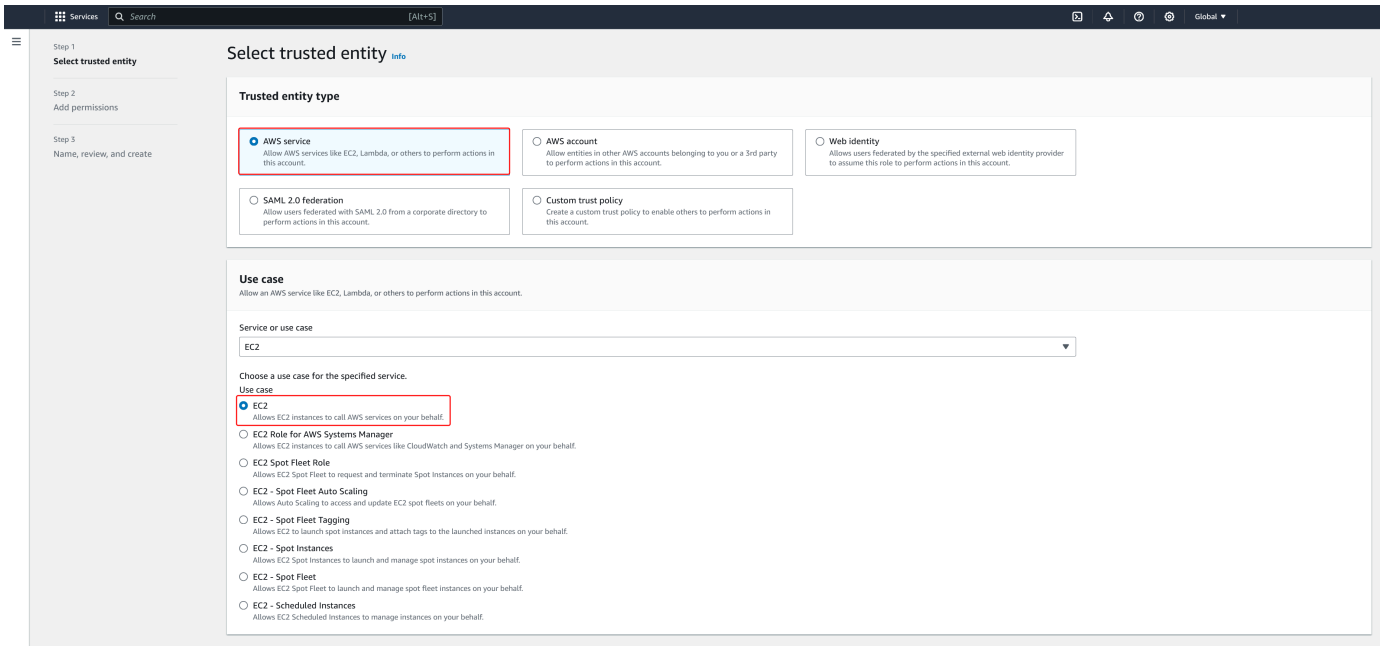
> **Note**
>
> 我們建議您為每個機密建立一個政策。這樣做可以確保執行個體只能存取適當的機密，並在執行個體受到入侵時將影響降至最低。

建立角色 DomainJoin

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。

若要建立 Linux 角DomainJoin 色

1. 以具有建立 IAM 政策權限的使用者身分登入。 AWS Management Console 前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在功能窗格的 [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] 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. 新增上面列出的三個策略之後，請選取 [建立角色]。

> **Note**
>
> AmazonSSM DirectoryServiceAccess 提供將執行個Active Directory體加入至管理的權限。 AWS Directory Service亞馬遜 SSM ManagedInstanceCore 提供了使用該服務所需的最低權限。 AWS Systems Manager 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. 輸入新角色的名稱，例如**LinuxEC2DomainJoin**，在「角色名稱」欄位中輸入您偏好的名稱。
8. (選用) 針對 Role description (角色描述)，輸入描述。
9. (選擇性) 在「步驟 3：新增標籤」下方選擇「新增標籤」以新增標籤。標籤鍵值配對可用來組織、追蹤或控制此角色的存取。
10. 選擇建立角色。

將您的 Linux EC2 執行個體順暢地加入您的 AWS 受管 Microsoft AD 目錄

現在您已經設定了所有先決條件任務，您可以使用下列程序順暢地加入 EC2 Linux 執行個體。

無縫加入您的 Linux 執行個體

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 從導覽列的 [區域] 選取器中，選擇與現有目錄 AWS 區域 相同的選項。
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，輸入您想要用於 Linux 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 機器映像) 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 代理程式) 2.3.1644.0 或更高版本。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 會在將 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格式為 EC2AMAZ-*XXXXXX* 格式。如需有關的詳細資訊`aws:domainJoin`，請參閱AWS Systems Manager 使用指南中的指AWS Systems Manager 令文件外掛程式參考。

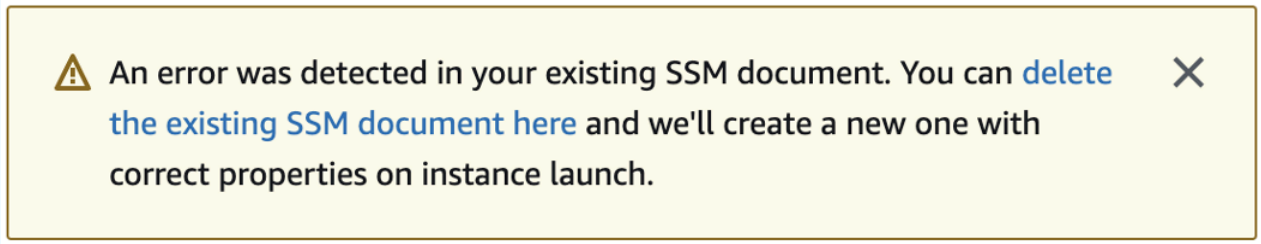
7. 在執行個體類型區段中，從執行個體類型下拉式清單中選擇您要使用的執行個體類型。
8. 在金鑰對 (登入) 區段中，您可以選擇建立新金鑰對或從現有金鑰對中進行選擇。若要建立新的金鑰對，請選擇建立新金鑰對。輸入金鑰對的名稱，然後選取金鑰對類型和私有金鑰檔案格式的選項。若要將私有金鑰儲存為可與 OpenSSH 搭配使用的格式，請選擇 .pem。若要將私有金鑰儲存為可與 PuTTY 搭配使用的格式，請選擇 .ppk。選擇建立金鑰對。您的瀏覽器會自動下載私有金鑰檔案。將私有金鑰檔案存放在安全的地方。

   > **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 地址的詳細資訊，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的 Amazon EC2 執行個體 IP 地址一節。
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 啟動精靈識別具有未預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
>
> - 如果您之前已編輯過 SSM 文件，且預期會有屬性，請選擇 [關閉] 並繼續啟動 EC2 執行個體而不進行任何變更。
> - 選取此處刪除現有 SSM 文件連結以刪除 SSM 文件。這將允許創建具有正確屬性的 SSM 文檔。SSM 文件會在您啟動 EC2 執行個體時自動建立。

15. 對於 IAM 執行個體設定檔，請在先決條件部分步驟 2：建立 LinuxEC2 DomainJoin 角色中選擇先前建立的 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。

維護您的 AD Connector 目錄

本節說明如何進行 AD Connector 環境的常見管理工作。

主題

- 刪除 AD Connector
- 檢視目錄資訊

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。請確定您所 AWS 區域 在的 AD Connector 部署位置。如需詳細資訊，請參閱選擇區域。
2. 確定您要刪除的 AD Connector 沒有啟用任何 AWS 應用程式。啟用的 AWS 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 [應用AWS 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 存取權。
      - 若要停用 Amazon WorkSpaces，您必須從 WorkSpaces 主控台中的目錄取消註冊服務。如需詳細資訊，請參閱 Amazon WorkSpaces 管理指南中的從目錄取消註冊。
      - 要禁用 Amazon WorkDocs，您必須在 Amazon WorkDocs 控制台中刪除 Amazon WorkDocs 網站。如需詳細資訊，請參閱 Amazon WorkDocs 管理指南中的刪除網站。
      - 要禁用 Amazon WorkMail，您必須在 Amazon WorkMail 控制台中刪除 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。
      - 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 適用Active Directory於 Windows 檔案伺服器的使用者指南中的使 FSx for Windows File Server。
      - 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 管理手冊》中的〈Active Directory驗證〉。
      - 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 管理員指南》中的刪除 Amazon Connect 執行個體一節。
      - 要禁用 Amazon QuickSight，您必須從 Amazon 退訂 QuickSight。如需詳細資訊，請參閱 Amazon QuickSight 使用者指南中的關閉 Amazon QuickSight 帳戶。

> **Note**
>
> 如果您正在使用 AWS IAM Identity Center 且之前已將其連線至您計劃刪除的 AWS 受管理 Microsoft AD 目錄，則必須先變更身分識別來源，然後才能刪除它。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。

檢視目錄資訊

您可檢視關於目錄的詳細資訊。

檢視詳細目錄資訊

1. 在AWS Directory Service 主控台導覽窗格的下 Active Directory，選取 [目錄]。
2. 按一下目錄的目錄 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」。

啟用對應用 AWS 程式和服務的存取

使用者可以授權 AD Connector，讓 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，以便與 AD Connector 搭配使用。

AWS 應用程式/服務	詳細資訊...
Amazon Chime	如需詳細資訊，請參閱《Amazon Chime 管理指南》。
Amazon Connect	如需詳細資訊，請參閱《Amazon Connect 管理指南》。
Amazon WorkDocs	如需詳細資訊，請參閱 Amazon WorkDocs 管理指南。

AWS 應用程式/服務	詳細資訊...
Amazon WorkMail	如需詳細資訊，請參閱 Amazon WorkMail 管理員指南。
Amazon WorkSpaces	您可以直接從建立 Simple AD、 AWS 受管理的 Microsoft AD 或 AD 連接器 WorkSpaces。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《使用者指南》AWS Client VPN。
AWS IAM Identity Center	如需詳細資訊，請參閱《使用者指南》AWS IAM Identity Center。
AWS Management Console	如需詳細資訊，請參閱 啟用 AD 憑證存取 AWS Management Console。
AWS Transfer Family	如需詳細資訊，請參閱《使用者指南》AWS Transfer Family。

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，請參閱授權使用的 AWS 應用程式和服務 AWS Directory Service。

為 AD Connector 更新 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。
> 如果您將 WorkSpaces 與 AD Connector 搭配使用，您還需更新 WorkSpace 的 DNS 地址。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。

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 提供多種與其他 AWS 服務搭配使用的方式。您可以依所需功能及成本預算，選擇目錄服務：

- AWS Directory Service 的 Microsoft 活動目錄是一個功能豐富的託管在雲上 AWS 託管。 AWS 如果您有 5,000 個以上的使用者，而且需要在 AWS 託管目錄與內部部署目錄之間設定信任關係，則受管理 Microsoft AD 是您的最佳選擇。
- AD 連接器只是將您現有的內部部署連接Active Directory到 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。
- S@@ imple AD 是具有基本Active Directory相容性的低規模、低成本的目錄。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。

如需更詳細的 AWS Directory Service 選項比較，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「AWS 管理 Microsoft AD 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 實例加入您的 AWS 受管 Microsoft AD 活動目錄」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」。

瞭解目錄的 AWS 安全性群組組態和使用方式

AWS 建立安全性群組，並將其附加至目錄的彈性網路介面，這些介面可從對等或調整大小的 V PC 中存取。 AWS 設定安全群組以封鎖目錄的不必要流量，並允許必要的流量。

修改目錄安全群組

如果您要修改目錄安全群組的安全，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。不當的變更可能會導致與預定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，因為這樣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，您可以將目錄的安全群組與您所建立的其他 EC2 執行個體產生關聯。但是，AWS 建議不要這種做法。 AWS 可能有理由修改安全性群組，恕不另行通知，以解決受管理目錄的功能或安全性需求。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。

瞭解應用程式的使 AWS 用者名

AWS Directory Service 為可用於建構使用者名稱的大多數字元格式提供支援。但是，在用戶名上強制執行字符限制，這些用戶名將用於登錄 AWS 應用程序 WorkSpaces，例如 Amazon WorkDocs WorkMail，Amazon 或 Amazon 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 AWS Directory Service 中更新 AD Connector 服務帳戶憑證。

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，您必須確定您的內部部署目錄與 AWS Directory Service s 保持相容。如需您責任的詳細資訊，請參閱我們的「共同的責任模型」。

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 應用程式相容性政策

作為 AWS Directory Service for Microsoft Active Directory (AWS 管理 Microsoft AD) 的替代方案，AD Connector 是僅用於 AWS 建立的應用程式和服務的 Active Directory 代理程式。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 視窗或 Linux 的無縫活動目錄網域加入功能，將您的執行個體加入自我管理的活動目錄 (現場部署)。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 EC2 執行個體加入您的 Active Directory 目錄。
- AWS Management Console – 您可以藉由 AD Connector 利用使用者的 Active Directory 登入資料來驗證 AWS Management Console 使用者，無需設定 SAML 基礎設施。如需詳細資訊，請參閱啟用 AD 憑證存取 AWS Management Console。
- Amazon QuickSight -有關更多信息，請參閱在 Amazon QuickSight 企業版中管理用戶帳戶。
- AWS IAM Identity Center – 如需詳細說明，請參閱將 IAM Identity Center 連線到內部部署 Active Directory 相關文章。
- AWS Transfer Family – 有關詳細說明，請參閱使用 Microsoft Active Directory 的AWS Directory Service 相關文章。
- AWS Client VPN – 如需詳細說明，請參閱用戶端身分驗證和授權相關文章。
- Amazon WorkDocs -如需詳細指示，請參閱使用 AD 連接器連接到現場部署目錄。
- Amazon WorkMail -有關詳細說明，請參閱將 Amazon WorkMail 與現有目錄集成（標準設置）。
- WorkSpaces -如需詳細指示，請參閱啟動 WorkSpace 使用 AD Connector。

> **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常見問題集頁面中的AWS受管理 Microsoft AD 一節。

AD Connector 疑難排解

下列項目可協助您疑難排解建立或使用 AD Connector 時可能會遇到的一些常見問題。

主題

創作問題

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

在 2012 年之前建立的某些 AWS 帳戶可能會存取不支援 AWS Directory Service 目錄的美國東部 (維吉尼亞北部)、美國西部 (加利佛尼亞北部) 或亞太區域 (東京) 區域的可用區域。如果您在建立時收到類似的錯誤訊息Active Directory，請在不同的可用區域中選擇子網路，然後嘗試再次建立目錄。

我嘗試建立 AD 連接器時收到「偵測到連線問題」錯誤

如果您在嘗試建立 AD 連接器時收到「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 密碼複雜性所致。您可以測試 AD 連接器的連線，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。連線測試應該在連接至 AD 連接器 IP 位址相關聯的兩個子網路的執行個體上執行。

如果連線測試成功，且執行個體加入網域，請檢查 AD 連接器的密碼。AD Connector 必須符合 AWS 密碼複雜性需求。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 不符合這些需求，請使用符合這些需求的密碼重新建立 AD Connector。

連線問題

以下是 AD 連接器的常見連線問題

- 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

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：

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: <IP address>
 Kerberos/authentication unavailable (TCP port 88) for IP: <IP address> Please ensure
 that the listed ports are available and retry the operation.
```

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)

根據您的需求，您可能需要額外的 TCP/UDP 連接埠。請參閱下列清單以瞭解其中一些連接埠。如需所使用之連接埠的相關資訊Active Directory，請參閱Microsoft說明文件中的如何為Active Directory網域和信任設定防火牆。

- 135 (RPC 端點對應程式)
- 646 (安全伺服器)
- 3268 (少量政府)
- 3269 (路由伺服器加密伺服器)

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」。

驗證問題

以下是 AD Connector 的一些常見驗證問題：

- 當我嘗試 Amazon WorkSpaces 使用智慧卡登入時，收到「憑證驗證失敗」的錯誤訊息
- 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
- 我在使用應用程式搜尋使 AWS 用者或群組時收到「無法驗證」的錯誤訊息
- 當我嘗試更新 AD Connector 服務帳戶時，我收到有關目錄認證的錯誤
- 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」的錯誤訊息

當您嘗試 WorkSpaces 使用智慧卡登入時，您會收到類似下列內容的錯誤訊息：

```
ERROR: Certificate Validation failed. Please try again by restarting your browser or
 application and make sure you select the correct certificate.
```

如果智慧卡的憑證未正確儲存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，請參閱必要條件。

請使用下列程序疑難排解智慧卡在使用者憑證存放區中儲存憑證的能力：

1. 在存取憑證時遇到問題的裝置上，存取 Microsoft Management Console (MMC)。

   > **Important**
   >
   > 在下一步之前，請先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。如需檢視 MMC 中憑證存放區的詳細資訊，請參閱說明文件中的 HOW TO：使用 MMC 嵌入式管理單元檢視憑證。Microsoft
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**
   >
   > 如果智慧卡未將憑證重新填入使用者存放區，則無法將其用於 WorkSpaces 智慧卡驗證。

AD 連接器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之後，應該檢查內部部署網域控制站，以判斷它們是否遭到主體替代名稱的使用者主體名稱 (UPN) 對應封鎖。如需有關此變更的詳細資訊，請參閱Microsoft說明文件中的如何停用 UPN 對應的主體替代名稱。

請使用下列程序來檢查網域控制站的登錄機碼：

1. 在註冊表編輯器中，導航到以下配置單元鍵

   HKEY _ 本地機器\ 系統\\ 服務\ Kdc\ CurrentControlSet UseSubjectAltName
2. 選取 UseSubjectAltName。確保該值設置為 0。

> **Note**
>
> 如果在內部部署網域控制站上設定登錄機碼，則 AD Connector 器將無法找到使用者，Active Directory並導致上述錯誤訊息。

憑證授權單位 (CA) 憑證應該上傳至 AD Connector 智慧卡憑證。憑證應包含 OCSP 資訊。以下列出 CA 的其他需求：

- 憑證應位於網域控制站的受信任根授權單位、憑證授權單位伺服器和 WorkSpaces.
- 離線和根 CA 憑證不會包含 OSCP 資訊。這些憑證包含其撤銷的相關資訊。
- 如果您使用協力廠商 CA 憑證進行智慧卡驗證，則 CA 和中繼憑證必須發行至 Active Directory NTauth 存放區。它們必須安裝在所有網域控制站、憑證授權單位伺服器和的受信任根授權單位中 WorkSpaces。
  - 您可以使用跟隨命令將證書發佈到 Active Directory NTAuth 存儲區：

```
certutil -dspublish -f Third_Party_CA.cer NTAuthCA
```

如需 WorkSpaces 有關將憑證發佈到 NTAuth 存放區的詳細資訊，請參閱使用一般存取卡存取 Amazon 安裝指南中的將發行的 CA 憑證匯入企業 NTAuth 存放區。

您可以依照下列程序檢查使用者憑證或 CA 鏈結憑證是否已由 OCSP 驗證：

1. 將智慧卡憑證匯出至本機電腦上的位置，例如 C: 磁碟機。
2. 開啟命令列提示，並瀏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. 命令後面應會出現一個彈出窗口。選取右上角的 OCSP 選項，然後選取擷取。狀態應該返回為已驗證。

如需有關 certutil 命令的詳細資訊，請參閱文件中的 cer tutil Microsoft

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。

我在使用應用程式搜尋使 AWS 用者或群組時收到「無法驗證」的錯誤訊息

在使用應用程式 (例如 WorkSpaces 或 Amazon) 時搜尋使 AWS 用者時，即使 AD Connector 狀態為作用中 QuickSight，您也可能會遇到錯誤。過期的憑證會使得 AD Connector 無法在 Active Directory 中無法完成物件的相關查詢。使用中提供的順序步驟更新服務帳戶的密碼Amazon EC2 實例的無縫域加入停止工作。

當我嘗試更新 AD Connector 服務帳戶時，我收到有關目錄認證的錯誤

嘗試更新 AD Connector 服務帳戶時，您會收到類似下列一或多項的錯誤訊息：

```
Message:An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials.
```

```
An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials
following Update your AD Connector Service Account Credentials
```

```
Message:
An Error Has Occurred
Your request has a problem. Please see the following details.
There was an error with the service account/password combination
```

時間同步處理和 Kerberos 可能存在問題。AD Connector 會將 Kerberos 驗證要求傳送至。Active Directory這些請求是時間敏感的，如果請求被延遲，他們將失敗。若要解決此問題，請參閱文件中的建議-使用授權時間來源設定根 PDC 和避免廣泛的時間偏差。Microsoft如需有關計時服務和同步處理的詳細資訊，請參閱下文：

- Windows時間服務的運作方式
- 電腦時脈同步的最大容差
- 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。如需有關此設定的詳細資訊，請移至預先驗證的Microsoft TechNet。

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 實例的無縫域加入停止工作

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 Support。

Amazon EC2 實例的無縫域加入停止工作

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。 過期的認證可能會阻止 AD Connector 在您的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. 更新您的服務帳戶的密碼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 AWS Directory Service 中更新 AD Connector 服務帳戶憑證。

> **Important**
>
> 僅在中更新密碼 AWS Directory Service 並不會將密碼變更推送到現有的內部部署，Active Directory因此請務必依照上一個程序所示的順序進行密碼變更。

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。如需需要停

用才能刪除 AD Connector 的應用程式清單，請參閱刪除 AD Connector。如果您仍然無法刪除 AD Connector，您可以透過以下方式要求協助AWS Support。

簡易 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 中的部分功能，包括能夠管理使用者帳戶和群組成員資格、建立及套用群組政策、安全連線到 Amazon EC2 執行個體，以及提供 Kerberos 單一登入 (SSO)。不過，請注意，Simple AD 不支援諸如多因素驗證 (MFA)、與其他網域的信任關係、Active Directory 系統管理中心、 PowerShell 支援、Active Directory 資源回收筒、群組管理服務帳戶，以及 POSIX 和 Microsoft 應用程式的結構描述延伸等功能。

Simple AD 提供許多優點：

- Simple AD 可讓您更輕鬆地管理在 Linux 和 Windows 上執行的 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 中的用戶帳戶允許訪問 Amazon 或 Amazon WorkSpaces WorkDocs 等AWS應用程序 WorkMail。
- 您可以透過 AWS Management Console 的 IAM 角色型存取來管理 AWS 資源。
- 每日自動化快照可進行 point-in-time 復原。

Simple AD 不支援下列各項：

- Amazon AppStream 2.0
- Amazon Chime
- 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 會在雲端中建立完全受控、以 Samba 為基礎的 AWS 目錄。當您使用 Simple AD 建立目錄時，請代表您 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 的不同子網路中建立的，此冗餘有助於確保即使發生故障，您的目錄仍可存取。

主題

Simple AD 先決條件

要創建一個 Simple AD 活動目錄，你需要一個 Amazon VPC 具有以下內容：

- VPC 必須具有預設硬體租用。
- VPC 不得設定下列 VPC 端點：
  - 路由 53 VPC 人雲端端點，其中包含解析為非公用 IP 位址的 DNS 條件式覆寫 AWS
  - CloudWatch VPC 端點

  - Systems Manager VPC 端點
  - Security Token Service VPC 端點
- 在兩個不同的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， AWS Directory Service 會代表您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 VPC 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。構成目錄的 EC2 執行個體在您的 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。

創建您的 Simple AD 活動目錄

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

若要建立 Simple AD Active Directory

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 簡易 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。

   只有當您在啟動過程中建立目錄時，才能使用此欄位 WorkSpaces。

   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。目錄建立程序會建立含有使用者名稱 `Administrator` 與這組密碼的管理者帳戶。

   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。

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

   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)。

什麼獲取與您的 Simple AD 活動目錄創建

當您使用 Simple AD 建立作用中目錄時，請代表您 AWS Directory Service 執行下列工作：

- 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 不儲存此密碼，也無法擷取密碼。不過，您可以從 AWS Directory Service 主控台或使用 ResetUserPasswordAPI 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`。此帳戶可用 AWS Directory Service 來執行目錄維護作業的自動化作業，例如擷取目錄快照和 FSMO 角色傳輸。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 ENI 中的每一個對於 VPC 和 AWS Directory Service 網域控制站之間的連線都是必不可少的，而且永遠不會刪除。您可以 AWS Directory Service 通過以下描述來識別所有保留用於的網絡接口：「為目錄目錄 ID AWS 創建的網絡接口」。如需詳細資訊，請參閱 Amazon EC2 Windows 執行個體使用者指南中的彈性網路界面。 AWS 管理 Microsoft AD 的預設 DNS 伺服器Active Directory是無類別網域間路由 (CIDR) +2 下的 VPC 擬私人雲端 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。

設定 Simple AD 的 DNS

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。

> **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。

如何管理 Simple AD

本節列出所有操作和維護 Simple AD 環境的程序。

主題

- 管理 Simple AD 中的使用者和群組
- 監控您的 Simple AD 目錄
- 將 Amazon EC2 實例加入到您的 Simple AD 活動目錄
- 維護您的 Simple AD 目錄
- 啟用對應用 AWS 程式和服務的存取
- 啟用 AD 憑證存取 AWS Management Console

管理 Simple AD 中的使用者和群組

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，您必須使用已加入您 AWS Directory Service 目錄的執行個體 (來自內部部署或 EC2)，並以具有建立使用者和群組之權限的使用者身分登入。您還需要在 EC2 執行個體上安裝 Active Directory 工具，才可在 Active Directory 使用者和電腦嵌入的狀態下，新增您的使用者和群組。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 實例加入到您的 Simple AD 活動目錄」。

> **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。如需有關此設定的詳細資訊，請移至 Microsoft TechNet 上的預先驗證。

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 的活動目錄管理工具

若要從 Amazon EC2 Windows 伺服器執行個體管理您的作用中目錄，您需要在執行個體上安裝活動目錄網域服務和使用中目錄輕量型目錄服務工具。請使用下列程序在 EC2 Windows 伺服器執行個體上安裝這些工具。

必要條件

開始此程序之前，請完成下列步驟：

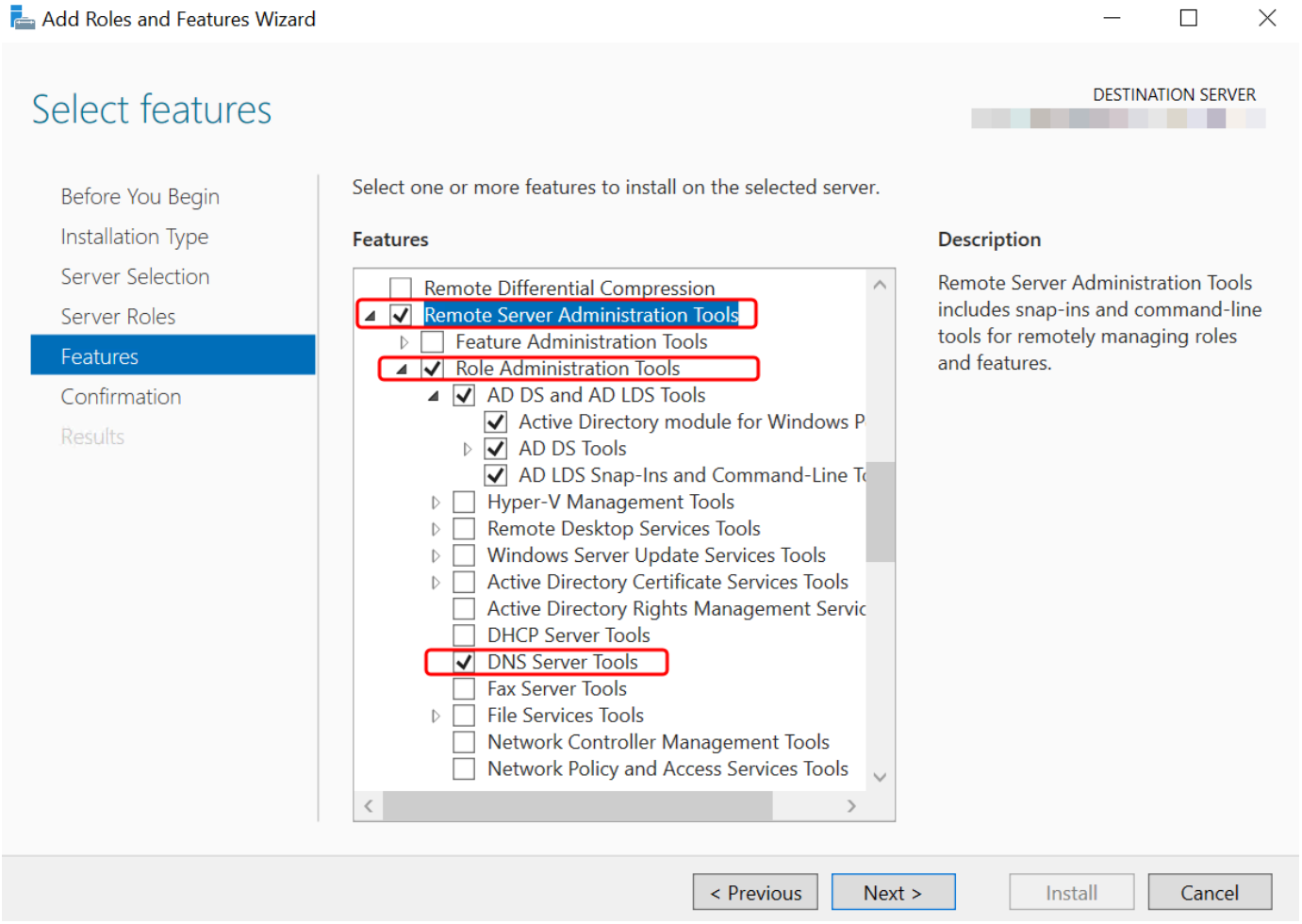
1. 創建一個簡單的 AD 活動目錄。如需詳細資訊，請參閱 創建您的 Simple AD 活動目錄。
2. 啟動並加入 EC2 Windows 伺服器執行個體到您的 Simple AD 活動目錄。EC2 執行個體需要下列政策來建立使用者和群組：**AWSSSMManagedInstanceCore**和**AmazonSSMDirectoryServiceAccess**。如需詳細資訊，請參閱 將 Amazon EC2 Windows 實例無縫加入到您的 Simple AD 活動目錄。
3. 您將需要您的活動目錄域管理員的憑據。這些認證是在創建 Simple AD 時創建的。如果您遵循中的程序創建您的 Simple AD 活動目錄，則您的管理員使用者名稱會包含您的 NetBIOS 名稱、**corp\administrator**。

在 EC2 Windows 伺服器執行個體上安裝作用中目錄管理工具

若要在 EC2 Windows 伺服器執行個體上安裝作用中目錄管理工具

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 安全性」對話方塊中，複製 Windows 伺服器電腦的本機系統管理員認證以進行登入。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，則**corp\administrator**會是使用者名稱創建您的 Simple AD 活動目錄。
7. 登入 Windows Server 執行個體之後，請選擇 [伺服器管理員]，從 [開始] 功能表中開啟 [伺服器管理員]。
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，會選取用於Windows PowerShell、AD DS 工具和 AD LDS 嵌入式管理單元和命令列工具的Active Directory模組。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。

在 EC2 Windows 服務器實例上安裝活動目錄管理工具的替代方法

- 以下是另一種安裝活動目錄管理工具的方法：
  - 您可以選擇使用安裝活動目錄管理工具Windows PowerShell。例如，您可以使用 PowerShell 提示安裝 Active Directory 遠端管理工具`Install-WindowsFeature RSAT-ADDS`。如需詳細資訊，請參閱 Microsoft 網站WindowsFeature上的安裝。

建立使用者

請使用下列步驟以在加入您 Simple AD 目錄的 EC2 執行個體上建立使用者。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。

您可以使用下列任何一種方法來建立使用者：

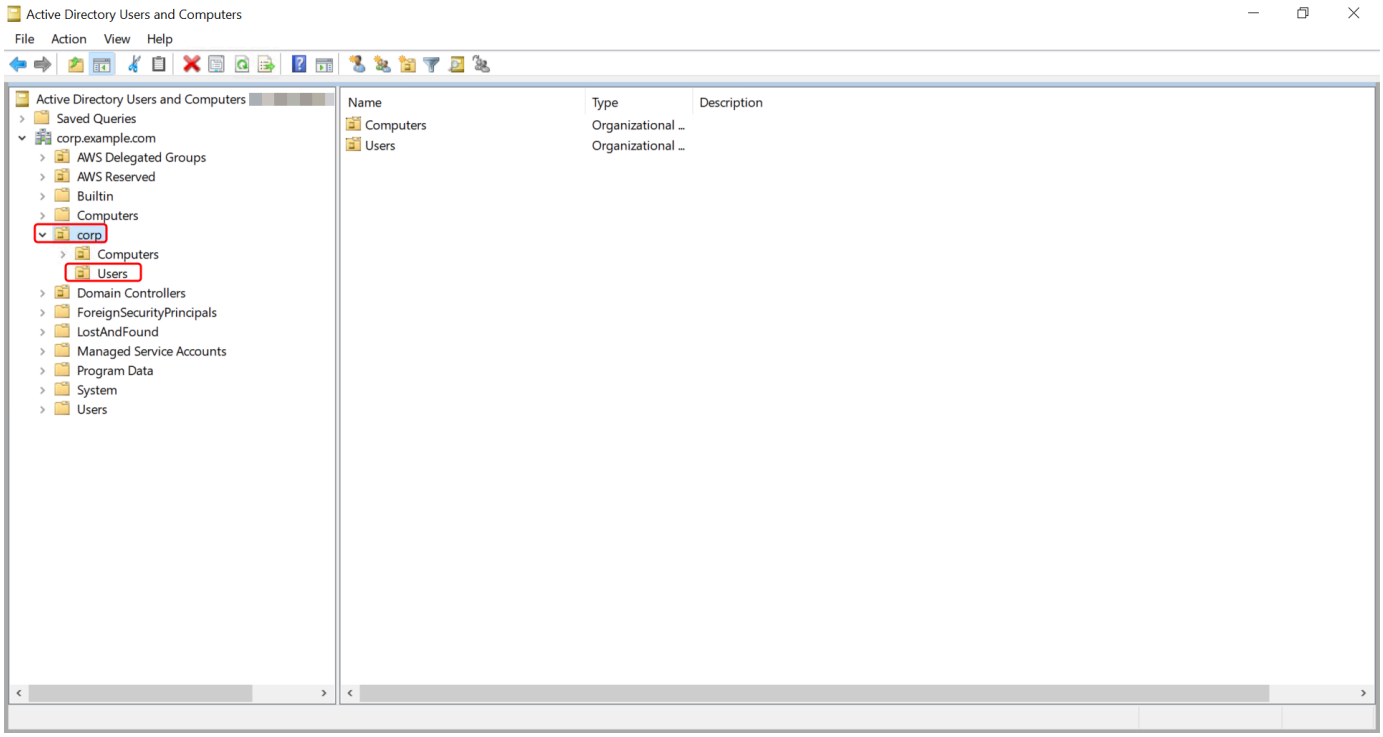
- Active Directory管理工具
- Windows PowerShell

使用Active Directory管理工具建立使用者

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「使用中目錄使用者和電腦」工具。在 Windows 系統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. 在目錄樹狀結構中，選取您要儲存使用者的目錄 NetBIOS 名稱 OU 下的 OU (例如，**corp\Users**)。如需中目錄所使用 OU 結構的詳細資訊 AWS，請參閱什麼被創建與 AWS 管理 Microsoft AD 活動目錄。



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。

在中建立使用者 Windows PowerShell

1. 以系統管理員身分 Connect 至加入您Active Directory網域的Active Directory執行個體。
2. 打開 Windows PowerShell.
3. 輸入以下指令，將使**`jane.doe`**用者名稱取代為您要建立的使用者名稱。系統會提示您Windows PowerShell提供新使用者的密碼。如需Active Directory密碼複雜性需求的詳細資訊，請參閱Microsoft文件。有關 New AdUser 命令的更多信息，請參閱Microsoft文檔。

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

刪除使用者

請使用下列步驟以在加入您 Simple AD 目錄的 EC2 Windows 執行個體上刪除使用者。

您可以使用下列任何一種方法來刪除使用者：

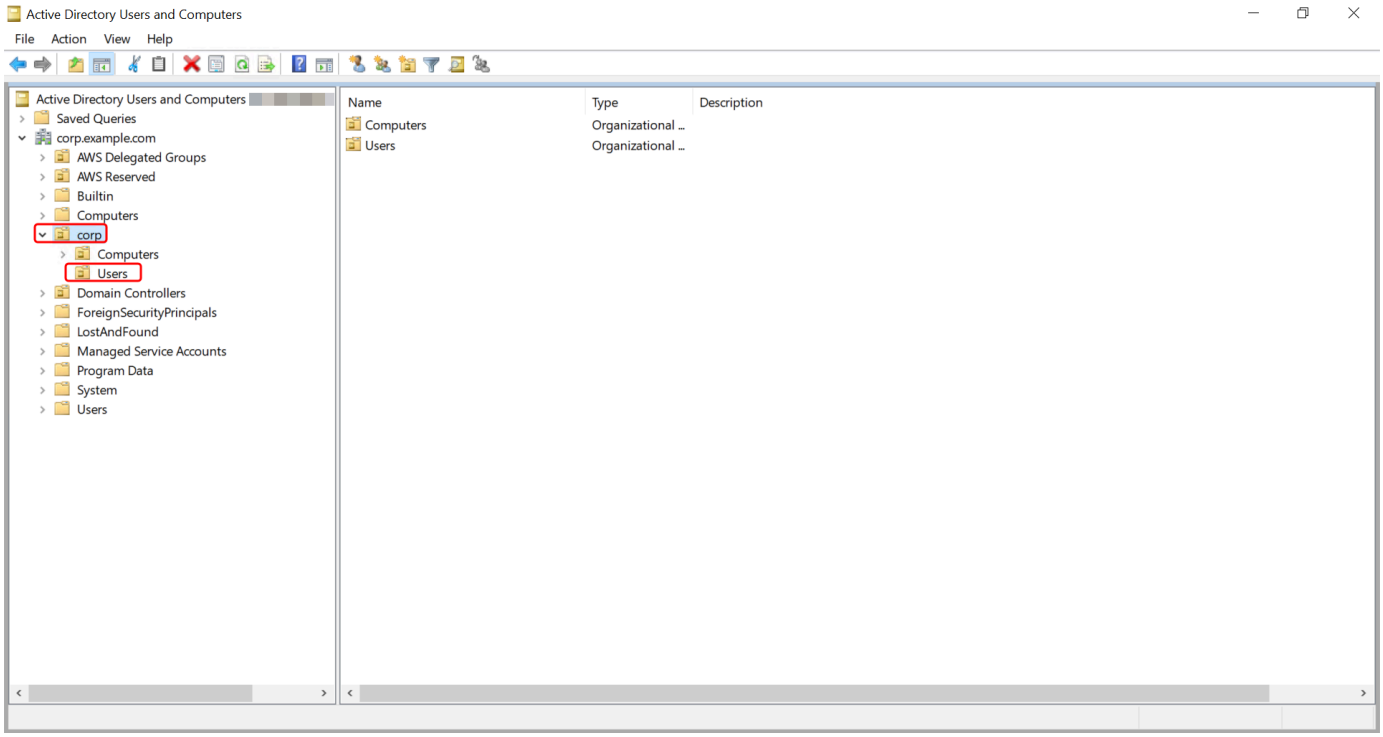
- Active Directory管理工具
- Windows PowerShell

使用Active Directory管理工具刪除使用者

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「使用中目錄使用者和電腦」工具。在 Windows 系統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. 在目錄樹狀結構中，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。

刪除中的使用者 Windows PowerShell

1. 以系統管理員身分 Connect 至加入您Active Directory網域的Active Directory執行個體。
2. 打開 Windows PowerShell.
3. 輸入以下指令，以您要刪除的使**jane.doe**用者名稱取代使用者名稱的使用者名稱。有關刪除 AdUser 命令的更多信息，請參閱文檔。Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

重設使用者密碼

使用者必須遵守中定義的密碼策略Active Directory。有時候，這可以得到最好的用戶，包括Active Directory管理員，他們忘記了他們的密碼。發生這種情況時，您可以使用 AWS Directory Service 如果用戶駐留在 Simple AD 中快速重置用戶的密碼。

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「管理資 AWS Directory Service 源存取權限概觀」。

您可以為您Active Directory的任何使用者重設密碼，但下列情況例外：

- 您可以在組織單位 (OU) 內重設任何使用者的密碼，這些使用者是以您Active Directory建立時所使用的 NetBIOS 名稱為基礎。例如，如果您遵循中的程序創建您的 Simple AD 活動目錄，您的 NetBIOS 名稱將是 CORP，而您可以重設的使用者密碼將是「公司/使用者 OU」的成員。
- 您無法重設 OU 以外的任何使用者的密碼，該使用者的密碼是根據您Active Directory在建立時使用的 NetBIOS 名稱。如需 Simple AD 之 OU 結構的詳細資訊，請參閱什麼獲取與您的 Simple AD 活動目錄創建。
- 您無法為身為兩個網域成員的任何使用者重設密碼。您也無法重設屬於網域系統管理員或企業系統管理員群組成員的任何使用者的密碼，但系統管理員使用者除外。

您可以使用下列任何一種方法來重設使用者密碼：

- AWS Management Console
- AWS CLI
- Windows PowerShell

重設中的使用者密碼 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Active Directory在清單中選取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] 對話方塊的 [使用者名稱] 中，輸入需要變更密碼之使用者的使用者名稱。
4. 在新密碼和確認密碼中輸入密碼，然後選擇重設密碼。

重設使用者密碼 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，並以您的目錄 ID 和所需的認證取代Active Directory目錄 ID **`jane.doe`**、使用者名稱和密碼**`P@ssw0rd`**。如需更多資訊，請參閱〈AWS CLI 指令參考〉reset-user-password中的〈

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

重設使用者密碼 Windows PowerShell

1. 以系統管理員身分 Connect 至加入您Active Directory網域的Active Directory執行個體。
2. 打開 Windows PowerShell.
3. 輸入下列指令**jane.doe**，以您的目錄 ID 和所需的認證取代使用者名稱、Active Directory目錄 ID 和密碼**P@ssw0rd**。如需詳細資訊，請參閱重設-DS UserPassword 指令程式。

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

建立群組

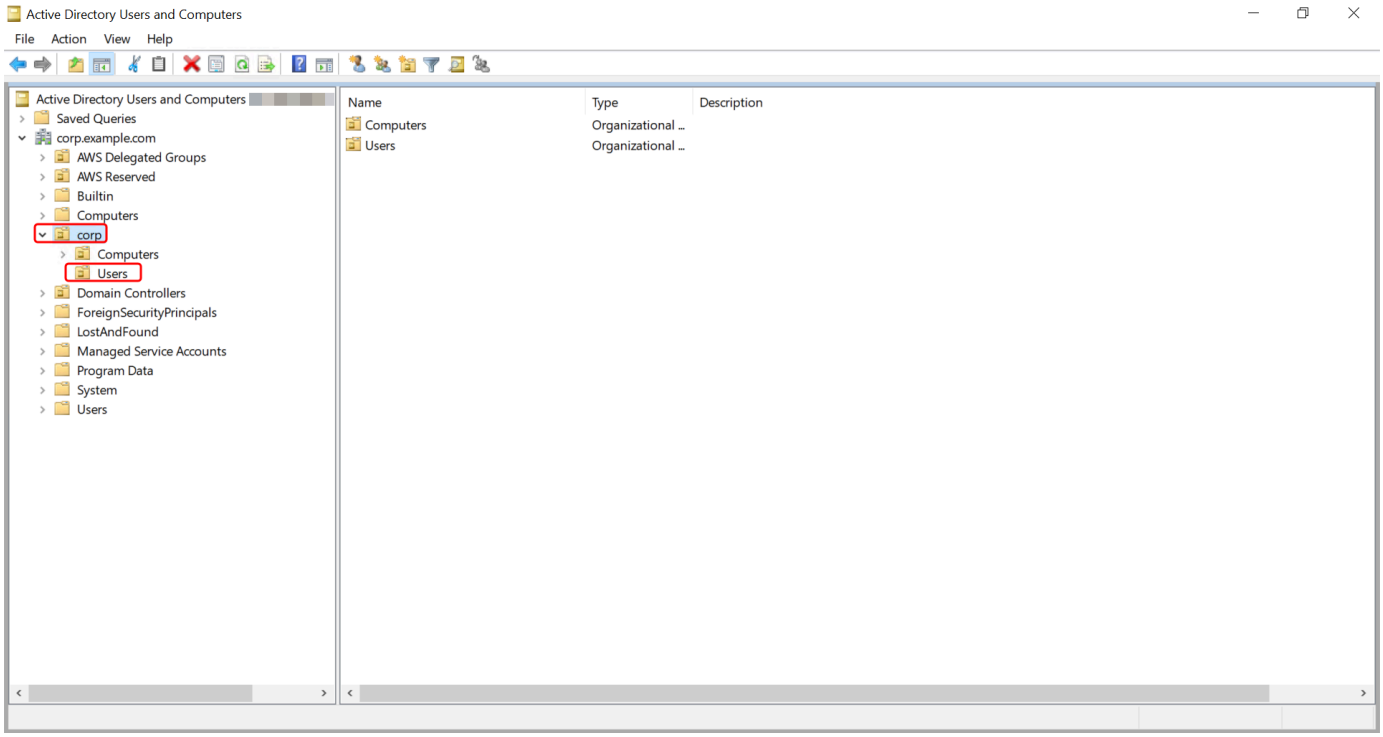
請使用下列步驟以在加入您 Simple AD 目錄的 EC2 執行個體上建立安全群組。在建立安全群組之前，您需要完成安裝 Active Directory 管理工具中所述的程序。

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 AWS 中目錄使用的 OU 結構的詳細資訊，請參閱 什麼被創建與 AWS 管理 Microsoft AD 活動目錄。



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。

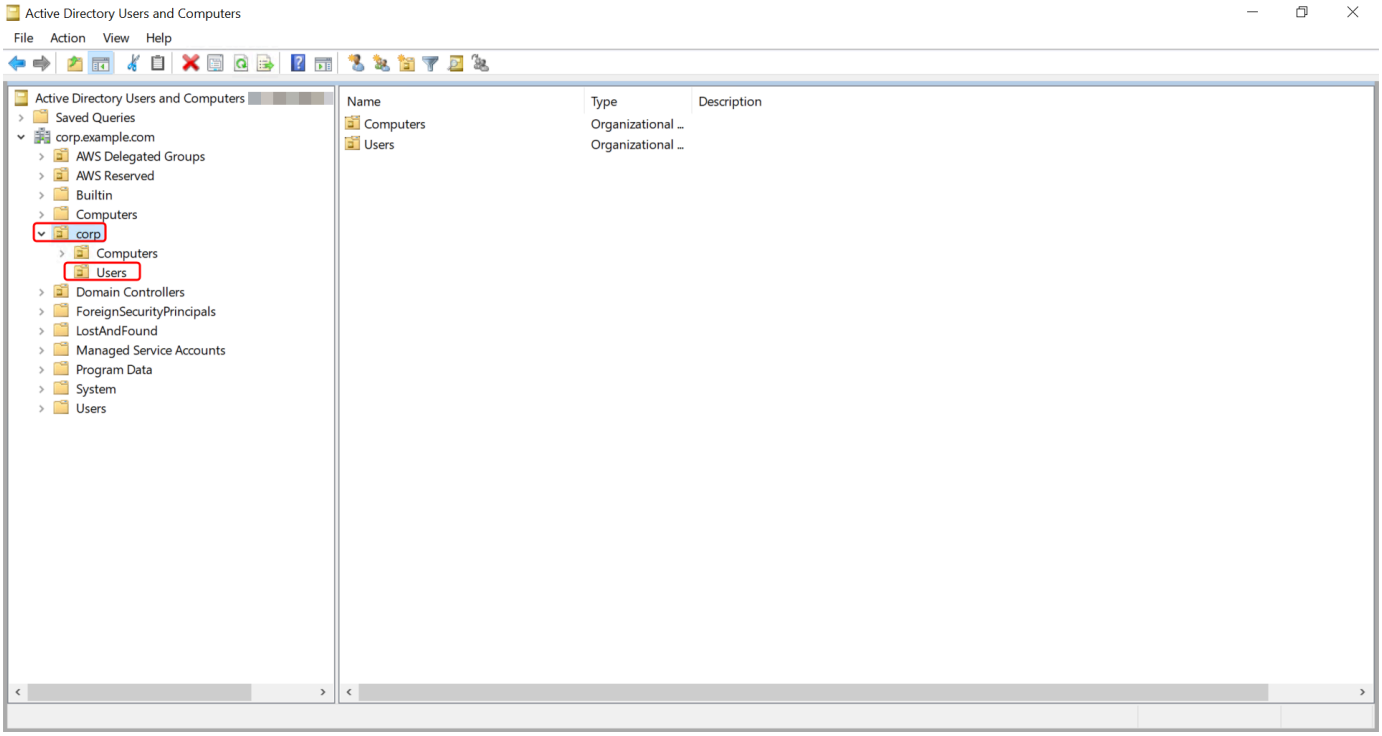
將使用者新增至群組

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. 在 [輸入要選取的物件名稱] 中，輸入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。

監控您的 Simple AD 目錄

您可以使用以下方法來監控您的 Simple AD 目錄：

主題

- 了解您的目錄狀態

- 使用 Amazon SNS 設定目錄狀態通知

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 Support 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 疑難排解 AWS 管理 Microsoft AD、AD Connector 疑難排解、Simple AD 疑難排解。對於一般維護相關問題，請在 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 Support 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 建立目錄快照或還原目錄。

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

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 Support 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。

如需更多詳細資訊，請參閱 Simple AD 目錄狀態原因。

使用 Amazon SNS 設定目錄狀態通知

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。使用以下步驟，您可以將 AWS Directory Service 作為發佈者新增至 Amazon SNS 主題。當 AWS Directory Service 偵測到目錄狀態變更時，它會將訊息發佈到該主題，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**
>
> 如果您使用僅具有DirectoryServiceFullAccess受管政策的 IAM 使用者或角色登入，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. 選擇建立。

如果您想要指定其他 SNS 訂閱者 (例如其他電子郵件地址、Amazon SQS 佇列) AWS Lambda，或者，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。如果要刪除整個主題，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，請將您的目錄與其他 Amazon SNS 主題建立關聯。

將 Amazon EC2 實例加入到您的 Simple AD 活動目錄

啟動執行個體時，您可以順暢地將 Amazon EC2 執行個體加入您的Active Directory網域。如需詳細資訊，請參閱 將 Amazon EC2 Windows 執行個體無縫加入您的 AWS 受管 Microsoft AD Active Directory。您也可以使用自動化功能直接從 AWS Directory Service 主控台啟AWS Systems Manager 動 EC2 執行個體並將其加入Active Directory網域。

如果您需要手動將 EC2 執行個體加入網Active Directory域，則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 實例無縫加入到您的 Simple AD 活動目錄
- 手動將 Amazon EC2 Windows 實例加入到您的 Simple AD 活動目錄
- 將 Amazon EC2 Linux 實例無縫加入到您的 Simple AD 活動目錄
- 手動將 Amazon EC2 Linux 實例加入到您的 Simple AD 活動目錄
- 委派 Simple AD 目錄加入權限
- 建立 DHCP 選項集

將 Amazon EC2 Windows 實例無縫加入到您的 Simple AD 活動目錄

此程序無縫地將 Amazon EC2 Windows 執行個體連接到您的 Simple AD 活動目錄。

無縫加入 EC2 視窗執行個體

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 在導航欄中，選擇與現有目錄 AWS 區域 相同的目錄。
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。

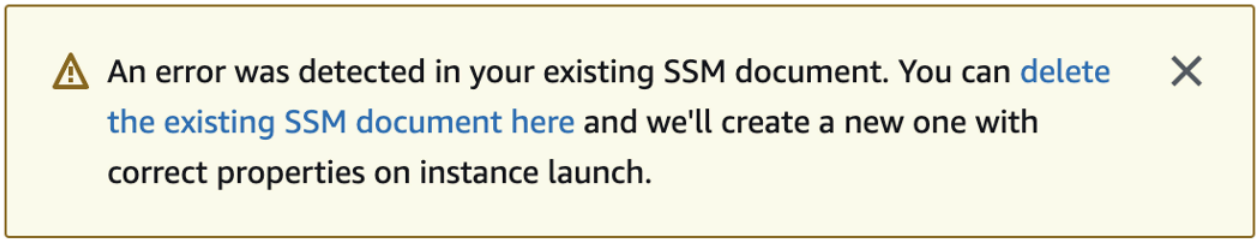
   > **Important**
   >
   > 這是您儲存私有金鑰檔案的唯一機會。

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 地址的詳細資訊，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的 Amazon EC2 執行個體 IP 地址一節。

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 啟動精靈識別具有未預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
>
> - 如果您之前已編輯過 SSM 文件，且預期會有屬性，請選擇 [關閉] 並繼續啟動 EC2 執行個體而不進行任何變更。
> - 選取此處刪除現有 SSM 文件連結以刪除 SSM 文件。這將允許創建具有正確屬性的 SSM 文檔。SSM 文件會在您啟動 EC2 執行個體時自動建立。

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已DirectoryServiceAccess附加 AWS 受管政策 AmazonSSM ManagedInstanceCore 和 AmazonSSM 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 [新增權限] 下方的原則清單中，選取 [亞馬遜 SSM] ManagedInstanceCore 和 [亞馬遜 SSM] 原則。DirectoryServiceAccess在搜尋方塊中，輸入 **SSM** 以篩選政策。選擇下一步。

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess 提供將執行個Active Directory體加入至管理的權限。 AWS Directory Service亞馬遜 SSM ManagedInstanceCore 提供了使用該服務所需的最低權限。 AWS Systems Manager 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。

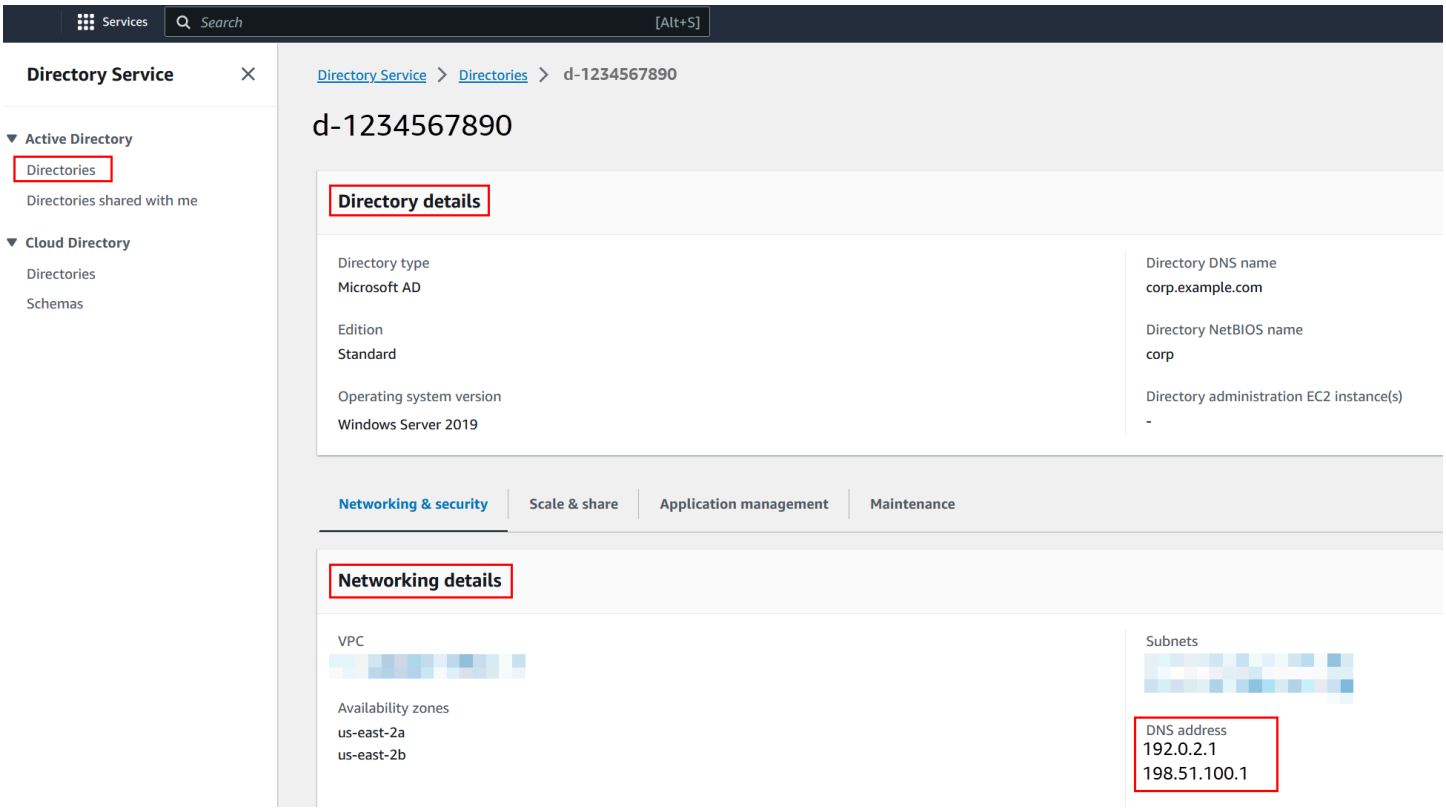
5. 在命名、檢閱和建立頁面上，針對角色名稱輸入角色名稱。您將需要此角色名稱來連接到 EC2 執行個體。
6. (選用) 您可以在描述欄位中提供 IAM 執行個體設定檔的描述。
7. 選擇建立角色。
8. 返回啟動執行個體頁面，然後選擇 IAM 執行個體設定檔旁的重新整理圖示。剛剛建立的 IAM 執行個體設定檔應顯示在 IAM 執行個體設定檔下拉式清單中。選擇這個新的設定檔並將其餘設定保留為預設值。

16. 選擇啟動執行個體。

手動將 Amazon EC2 Windows 實例加入到您的 Simple AD 活動目錄

若要將現有的 Amazon EC2 Windows 執行個體手動加入 Simple AD 活動目錄，必須使用中指定的參數啟動執行個體將 Amazon EC2 Windows 實例無縫加入到您的 Simple AD 活動目錄。

您將需要 Simple AD DNS 伺服器的 IP 位址。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。



若要將 Windows 執行個體加入 Simple AD 作用中目錄

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。

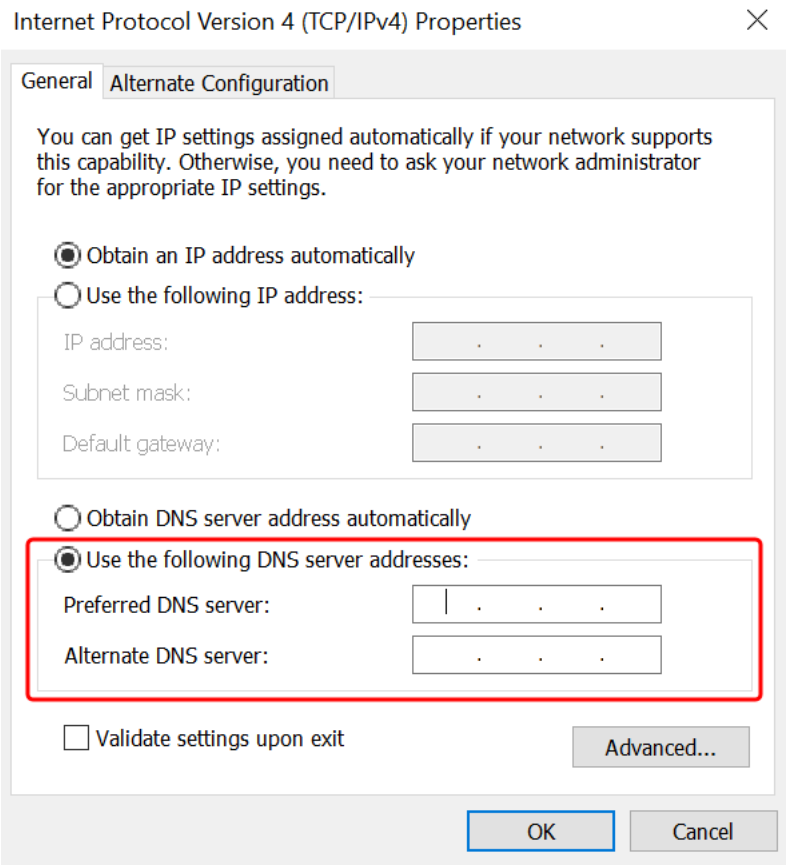
   a. 開啟 Network Connections (網路連線)。

   > **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 伺服器位址]，將 [慣用的 DNS 伺服器] 和 [替代 DNS 伺服器位址] 變更為簡單 AD 提供的 DNS 伺服器的 IP 位址，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 [成員屬於] 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之帳戶的使用者名稱和密碼。如需委派這些權限的詳細資訊，請參閱「委派 Simple AD 目錄加入權限」。

> **Note**
>
> 您可以輸入網域的完整名稱或 NetBIOS 名稱，接著輸入反斜線 (\)，然後輸入使用者名稱。用戶名將是管理員。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，您可以從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。使用中的目錄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 的活動目錄管理工具。

將 Amazon EC2 Linux 實例無縫加入到您的 Simple AD 活動目錄

此程序無縫地將 Amazon EC2 Linux 執行個體連接到您的 Simple AD 活動目錄。

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 之前的發行版不支援無縫域加入功能。

必要條件

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。

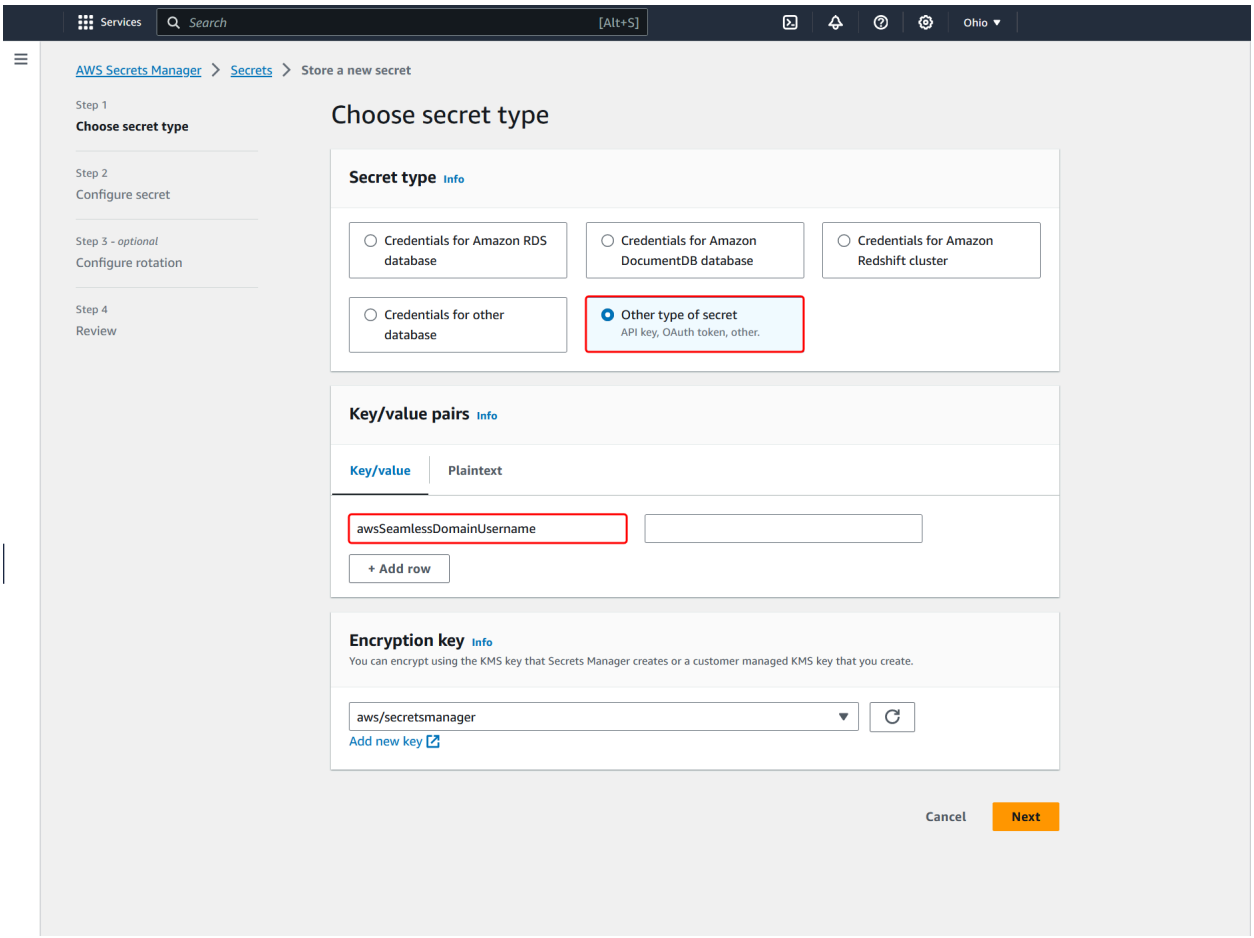
建立儲存域服務帳戶的機密

您可以用 AWS Secrets Manager 來儲存網域服務帳戶。

建立機密並儲存域服務帳戶資訊

1. 請登入 AWS Management Console 並開啟 AWS Secrets Manager 主控台，網址為 https://console.aws.amazon.com/secretsmanager/。
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「其他類型的機密」。
   b. 在「鍵/值配對」下，執行下列操作：
      i. 在第一個方塊中，輸入 **awsSeamlessDomainUsername**。在同一列的下一個方塊中，輸入服務帳戶的使用者名稱。例如，如果您之前使用了該 PowerShell 命令，則服務帳戶名稱將是**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] 底下，保留預設值`aws/secretsmanager`。 AWS Secrets Manager 當您選擇此選項時，一律會加密密碼。您也可以選擇您建立的金鑰。

> **Note**
>
> 有相關的費用 AWS Secrets Manager，具體取決於您使用的秘密。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/secretsmanager`的 AWS 受管理金鑰來免費加密您的密鑰。如果您建立自己的 KMS 金鑰來加密密碼，請按照目前的 AWS 費 AWS KMS 率向您收費。如需詳細資訊，請參閱 AWS Key Management Service 定價。

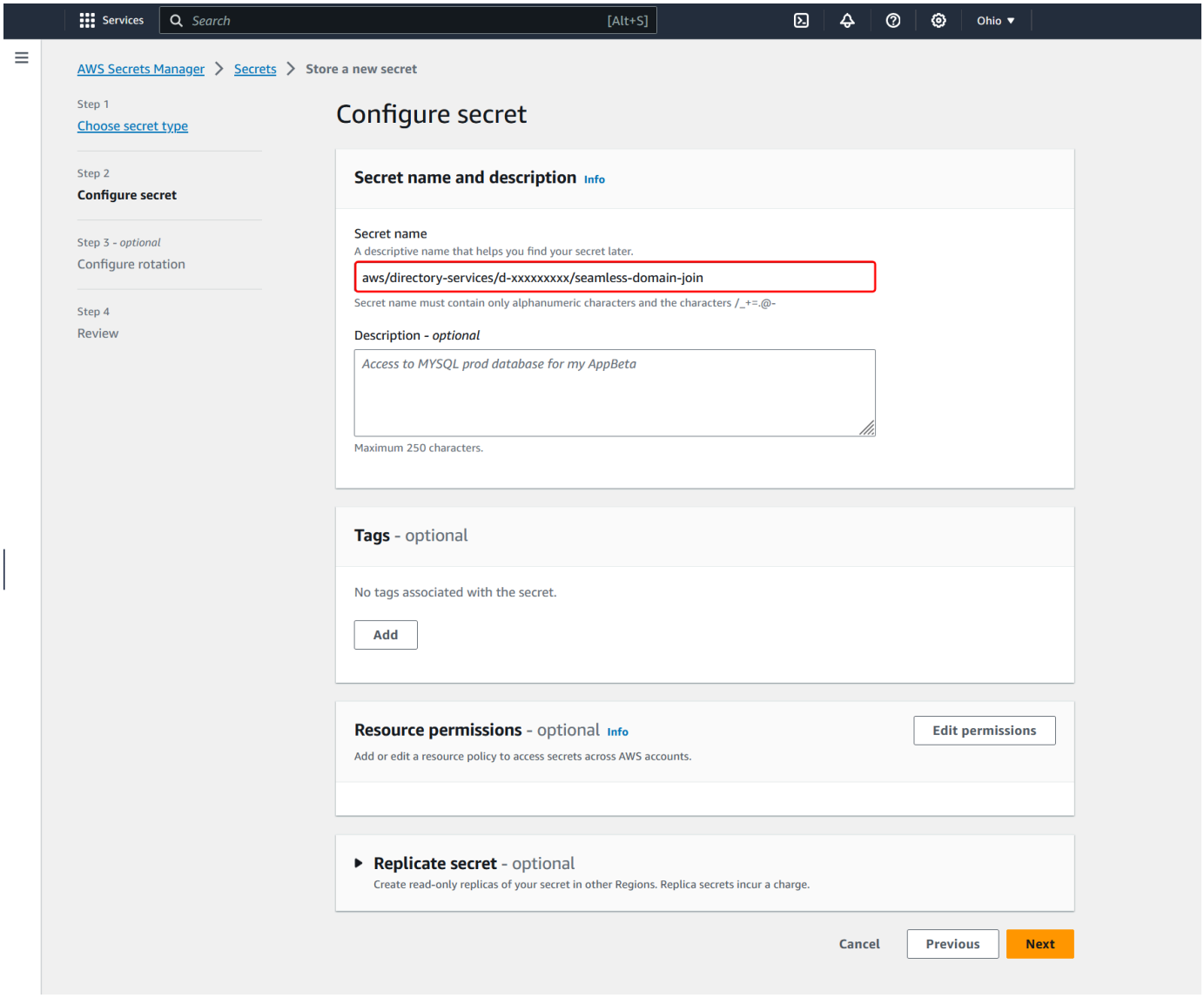
v. 選擇下一步。

4. 在密碼名稱下，使用下列格式輸入包含您目錄 ID 的密碼名稱，並以您的目錄識別碼取代 *d-xxxxxxxxx*：

```
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-xxxxxxxxx* 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。
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。

建立必要的 IAM 政策和角色

使用下列先決條件步驟來建立自訂政策，允許您的 Secrets Manager 無縫網域加入密碼 (您之前建立) 的唯讀存取權限，以及建立新的 LinuxEC2 DomainJoin 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 政策權限的使用者身分登入。 AWS Management Console 前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在功能窗格的 [存取管理] 中，選擇 [原則]。
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**
>
> 請確定您將 [區域] 和 [資源 ARN] 取代為您先前建立的密碼的實際 [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。

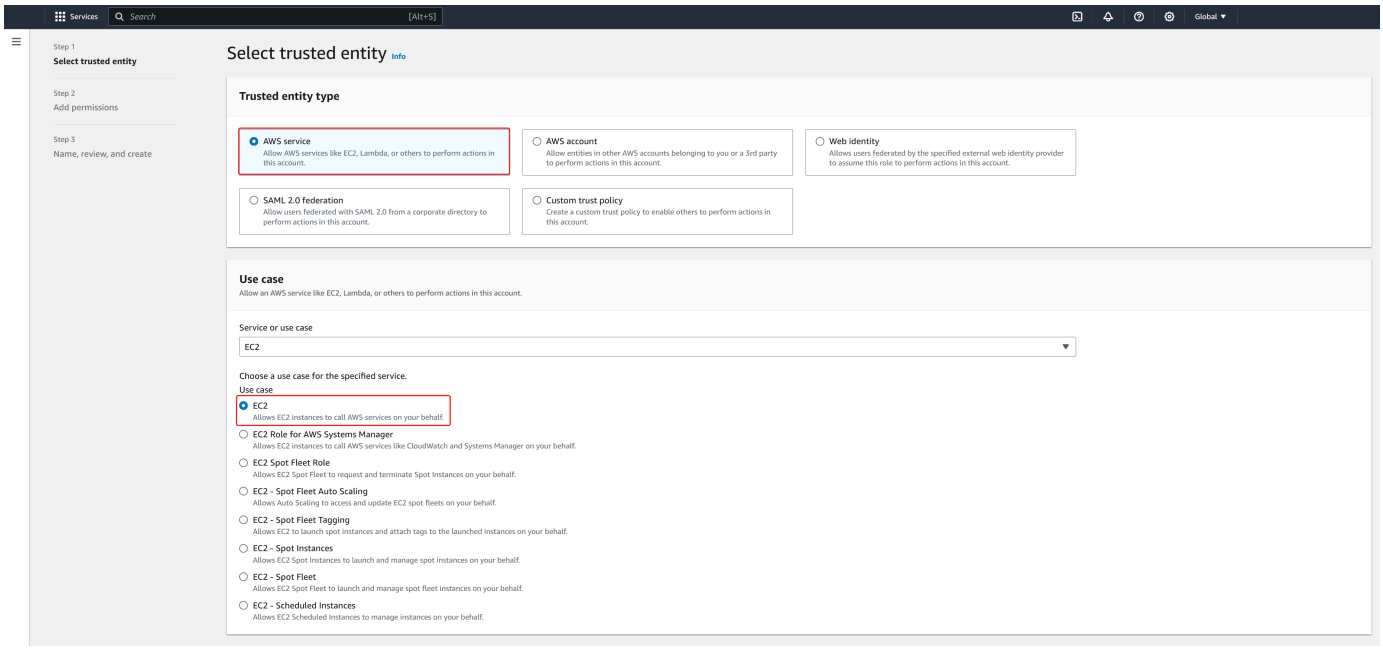
> **Note**
>
> 我們建議您為每個機密建立一個政策。這樣做可以確保執行個體只能存取適當的機密，並在執行個體受到入侵時將影響降至最低。

建立角色 DomainJoin

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。

若要建立 Linux 角DomainJoin 色

1. 以具有建立 IAM 政策權限的使用者身分登入。 AWS Management Console 前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在功能窗格的 [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] 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. 新增上面列出的三個策略之後，請選取 [建立角色]。

> **Note**
>
> AmazonSSM DirectoryServiceAccess 提供將執行個Active Directory體加入至管理的權限。 AWS Directory Service亞馬遜 SSM ManagedInstanceCore 提供了使用該服務所需的最低權限。 AWS Systems Manager 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. 輸入新角色的名稱，例如**LinuxEC2DomainJoin**，在「角色名稱」欄位中輸入您偏好的名稱。
8. (選用) 針對 Role description (角色描述)，輸入描述。
9. (選擇性) 在「步驟 3：新增標籤」下方選擇「新增標籤」以新增標籤。標籤鍵值配對可用來組織、追蹤或控制此角色的存取。
10. 選擇建立角色。

將 Linux 實例無縫加入到您的 Simple AD 活動目錄

現在您已經設定了所有先決條件任務，您可以使用下列程序順暢地加入 EC2 Linux 執行個體。

無縫加入您的 Linux 執行個體

1. 登入 AWS Management Console 並開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。
2. 從導覽列的 [區域] 選取器中，選擇與現有目錄 AWS 區域 相同的選項。
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，輸入您想要用於 Linux 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 機器映像) 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 代理程式) 2.3.1644.0 或更高版本。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 會在將 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格式為 EC2AMAZ-*XXXXXX* 格式。如需有關的詳細資訊`aws:domainJoin`，請參閱AWS Systems Manager 使用指南中的指AWS Systems Manager 令文件外掛程式參考。

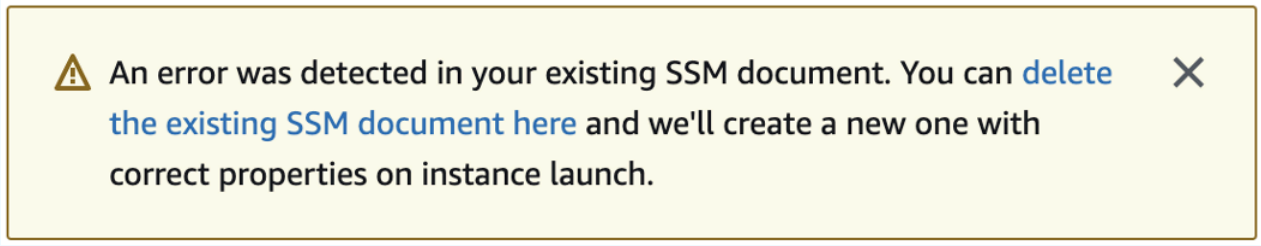
7. 在執行個體類型區段中，從執行個體類型下拉式清單中選擇您要使用的執行個體類型。
8. 在金鑰對 (登入) 區段中，您可以選擇建立新金鑰對或從現有金鑰對中進行選擇。若要建立新的金鑰對，請選擇建立新金鑰對。輸入金鑰對的名稱，然後選取金鑰對類型和私有金鑰檔案格式的選項。若要將私有金鑰儲存為可與 OpenSSH 搭配使用的格式，請選擇 .pem。若要將私有金鑰儲存為可與 PuTTY 搭配使用的格式，請選擇 .ppk。選擇建立金鑰對。您的瀏覽器會自動下載私有金鑰檔案。將私有金鑰檔案存放在安全的地方。

   > **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 地址的詳細資訊，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的Amazon EC2 執行個體 IP 地址一節。
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 啟動精靈識別具有未預期屬性的現有 SSM 文件，就會發生此錯誤。您可以執行下列任一作業：
>
> - 如果您之前已編輯過 SSM 文件，且預期會有屬性，請選擇 [關閉] 並繼續啟動 EC2 執行個體而不進行任何變更。
> - 選取此處刪除現有 SSM 文件連結以刪除 SSM 文件。這將允許創建具有正確屬性的 SSM 文檔。SSM 文件會在您啟動 EC2 執行個體時自動建立。

15. 對於 IAM 執行個體設定檔，請在先決條件部分步驟 2：建立 LinuxEC2 DomainJoin 角色中選擇先前建立的 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 實例加入到您的 Simple AD 活動目錄

除了 Amazon EC2 Windows 執行個體之外，您還可以將某些 Amazon EC2 Linux 執行個體加入您的 Simple AD 活動目錄。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
- 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。

必要條件

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 實例無縫加入到您的 Simple AD 活動目錄 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. 將 Linux 執行個體設定為使用 AWS Directory Service提供之 DNS 伺服器的 DNS 伺服器 IP 位址。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 受管 Microsoft AD 目錄加入權限」。

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. 將 Linux 執行個體設定為使用 AWS Directory Service提供之 DNS 伺服器的 DNS 伺服器 IP 位址。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 受管 Microsoft AD 目錄加入權限」。

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. 將 Linux 執行個體設定為使用 AWS Directory Service提供之 DNS 伺服器的 DNS 伺服器 IP 位址。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

example.com 網域中具有網域加入權限之帳戶的 SAM AccountName。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 受管 Microsoft AD 目錄加入權限」。

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. 將 Linux 執行個體設定為使用 AWS Directory Service提供之 DNS 伺服器的 DNS 伺服器 IP 位址。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

example.com 網域中具有網域加入權限之帳戶的 SAM AccountName。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 受管 Microsoft AD 目錄加入權限」。

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
```

識別碼對應

識別碼對應可以透過兩種方法執行，以維持 UNIX/Linux 使用者識別碼 (UID) 與群組識別碼 (GID) 與視窗與Active Directory安全性識別碼 (SID) 身分之間的統一體驗。

1. 集中式
2. 分散式

> **Note**
>
> 中的集中式使用者身分對應Active Directory需要可攜式作業系統介面或 POSIX。

集中使用者身分對應

Active Directory或其他輕量型目錄存取通訊協定 (LDAP) 服務提供 UID 和 GID 給 Linux 使用者。在中 Active Directory，這些識別碼會儲存在使用者屬性中：

- UID-使用者名稱 (字串)
- UID 號碼-Linux 使用者識別碼編號 (整數)
- GID 號碼-Linux 群組識別碼 (整數)

若要將 Linux 執行個體設定為使用來源的 UID 和 GIDActive Directory，請在 sssd.conf 檔案`ldap_id_mapping = False`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

分佈式用戶身份映射

如果Active Directory沒有 POSIX 擴充功能，或者您選擇不集中管理身分對應，Linux 可以計算 UID 和 GID 值。Linux 會使用使用者的唯一安全性識別碼 (SID) 來維持一致性。

若要設定分散式使用者識別碼對應，請`ldap_id_mapping = True`在 sssd.conf 檔案中進行設定。

Connect 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，回應會類似下列內容：

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 目錄加入權限

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。

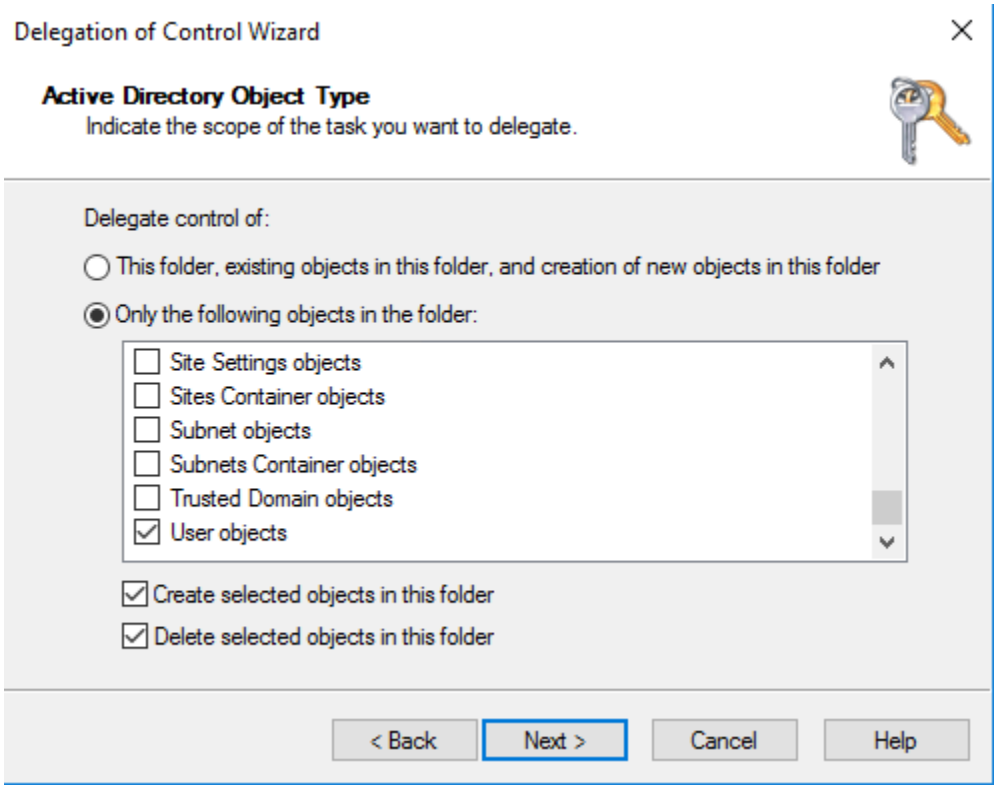
不過，最佳實務是您應該使用只有所需最低權限的帳戶。下列程序示範如何建立稱為 `Joiners` 的新群組，並將權限委派給需要將電腦加入目錄的這個群組。

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。

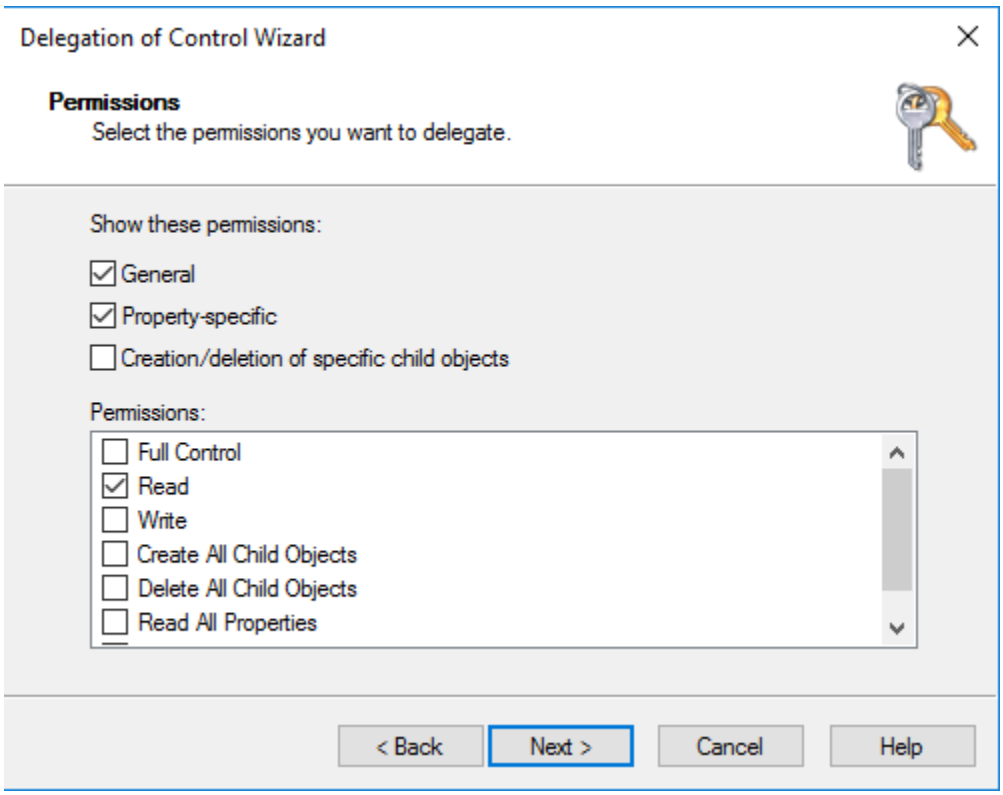
委派 Simple AD 目錄加入權限

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，使用者將擁有足夠的權限來連線 AWS Directory Service 至目錄。

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 選項設定指派給目錄所在的 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. 前往 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所提供目錄之 DNS 伺服器的 IP 位址。

> **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. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇您的 VPC
3. 選取 VPC，然後選擇動作、編輯 DHCP 選項集。

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。

維護您的 Simple AD 目錄

本節說明如何進行 Simple AD 環境的常見管理工作。

主題

- 刪除 Simple AD
- 建立目錄快照或還原目錄
- 檢視目錄資訊

刪除 Simple AD

刪除 Simple AD 時，會刪除所有目錄資料和快照集，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。確保您位於部署的 AWS 區域 Active Directory位置。如需詳細資訊，請參閱選擇區域。
2. 請確定您要刪除的目錄沒有啟用任何 AWS 應用程式。啟用的 AWS 應用程式會阻止您刪除 AWS 受管理的 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 [應用AWS 程式與服務] 區段中，您會看到目錄已啟用哪些 AWS 應用程式。

      - 停用 AWS Management Console 存取權。
      - 若要停用 Amazon WorkSpaces，您必須從 WorkSpaces 主控台中的目錄取消註冊服務。如需詳細資訊，請參閱 Amazon WorkSpaces 管理指南中的從目錄取消註冊。
      - 要禁用 Amazon WorkDocs，您必須在 Amazon WorkDocs 控制台中刪除 Amazon WorkDocs 網站。如需詳細資訊，請參閱 Amazon WorkDocs 管理指南中的刪除網站。
      - 要禁用 Amazon WorkMail，您必須在 Amazon WorkMail 控制台中刪除 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。

- 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 適用Active Directory於 Windows 檔案伺服器的使用者指南中的使 FSx for Windows File Server。
- 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 管理手冊》中的〈Active Directory驗證〉。
- 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 管理員指南》中的刪除 Amazon Connect 執行個體一節。
- 要禁用 Amazon QuickSight，您必須從 Amazon 退訂 QuickSight。如需詳細資訊，請參閱 Amazon QuickSight 使用者指南中的關閉 Amazon QuickSight 帳戶。

> **Note**
>
> 如果您正在使用 AWS IAM Identity Center 且之前已將其連線至您計劃刪除的 AWS 受管理 Microsoft AD 目錄，則必須先變更身分識別來源，然後才能刪除它。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。

建立目錄快照或還原目錄

AWS Directory Service 可讓您擷取 Simple AD 目錄資料的手動快照。這些快照可用來執行目錄的 point-in-time 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 Support 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。

對於目錄，可能需要幾分鐘的時間才能還原目錄。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。

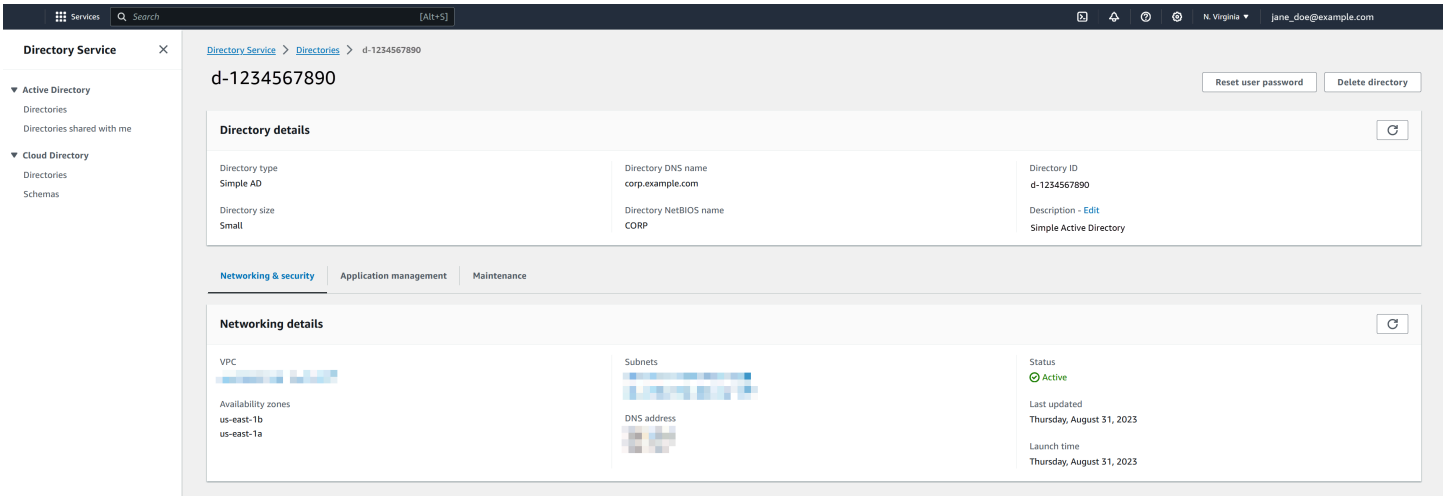
檢視目錄資訊

您可檢視關於目錄的詳細資訊。

檢視詳細目錄資訊

1. 在AWS Directory Service 主控台導覽窗格的下 Active Directory，選取 [目錄]。
2. 按一下目錄的目錄 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」。



啟用對應用 AWS 程式和服務的存取

用戶可以授權 Simple AD 給 AWS 應用程序和服務，如 Amazon WorkSpaces，訪問您的Active Directory. 您可以啟用或停用下列 AWS 應用程式和服務，以便與 Simple AD 搭配使用。

AWS 應用程式/服務	詳細資訊...
Amazon Chime	如需詳細資訊，請參閱《Amazon Chime 管理指南》。
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 管理員指南。
Amazon WorkSpaces	您可以直接從建立 Simple AD、 AWS 受管理的 Microsoft AD 或 AD 連接器 WorkSpaces。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 啟用 AD 憑證存取 AWS Management Console。

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，請參閱授權使用的 AWS 應用程式和服務 AWS Directory Service。

主題

- 建立存取 URL
- 單一登入

建立存取 URL

存取 URL 可用於 AWS 應用程式和服務 (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。

單一登入

AWS Directory Service提供允許您的使用者 WorkDocs 從加入目錄的電腦存取 Amazon 的功能，而無需單獨輸入其登入資料。

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體名稱屬性，您可以使用具有修改 AD Connector 服務帳戶權限的帳戶，從加入網域的電腦執行下列 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 Amazon 啟用或停用單一登入 WorkDocs

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 Amazon 的單一登入 WorkDocs。

   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. 如果您稍後想要停用 Amazon 的單一登入 WorkDocs，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。
- 啟用主動腳本 (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

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原則：

```
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 政策在網域中的電腦上管理 Chrome 網路瀏覽器，就必須將存取網址新增至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。

啟用 AD 憑證存取 AWS Management Console

AWS Directory Service 可讓您授予 AWS Management Console存取權給目錄成員。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，讓他們可以存取各種 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「檢視目錄資訊」。如需如何建立存取 URL 的詳細資訊，請參閱「建立存取 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 資源存取權給使用者與群組」。

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

相關的 AWS 安全性部落格文章

- 如何使用 AWS Managed Microsoft AD 和內部部署憑證來存取 AWS Management Console

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。

   在使用者可以使用存取 URL 登入主控台之前，您必須先將使用者新增至角色。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 AWS 資源存取對話方塊中，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)。

教學課程：建立簡單的 AD Active Directory

下面的教程將引導您完成所有必要的步驟來設置一個 Simple AD 活動目錄。它的目的是讓您Active Directory快速輕鬆地開始使用 Simple AD，但並非用於大規模的生產環境中。

教學課程事前準備

本教學課程的假設如下：

- 你有一個活躍的 AWS 帳戶。
- 在您要使用 Simple AD 的區域，您的帳戶尚未達到 Amazon VPC 的限制。如需 VPC 的詳細資訊，請參閱什麼是 Amazon V PC？ 以及您虛擬私人雲端中的子網路，請參閱 Amazon VPC 使用者指南。
- 您在區域中沒有 CIDR 的現有 VPC。`10.0.0.0/16`

如需詳細資訊，請參閱 Simple AD 先決條件。

步驟 1：建立和設定適用於 Simple AD 的 Amazon VPC Active Directory

建立和設定可搭配 Simple AD 使用的 Amazon VPC。開始此程序之前，請確定您已完成 教學課程事前準備。

為您的 Simple AD 建立 VPC Active Directory

建立具有兩個公用子網路的 VPC。 AWS Directory Service VPC 中需要兩個子網路，且每個子網路必須位於不同的可用區域中。

1. 前往 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。

第 2 步：創建您的 Simple AD 活動目錄

若要建立新的 Simple AD 作用中目錄，請執行下列步驟。開始此程序之前，請確定已完成教學課程事前準備和步驟 1：為 Simple AD Active Directory 建立和設定 Amazon VPC 中識別的先決條件。

要創建一個簡單的 AD 活動目錄

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 簡易 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。

只有當您在啟動過程中建立目錄時，才能使用此欄位 WorkSpaces。

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。

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

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)。

Simple AD 最佳實務

以下是您應該考慮的一些建議和指導方針，以避免出現問題並充分利用 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 提供多種與其他 AWS 服務搭配使用的方式。您可以依所需功能及成本預算，選擇目錄服務：

- AWS Directory Service 的 Microsoft 活動目錄是一個功能豐富的託管在雲上 AWS 託管。 AWS 如果您有 5,000 個以上的使用者，而且需要在 AWS 託管目錄與內部部署目錄之間設定信任關係，則受管理 Microsoft AD 是您的最佳選擇。
- AD 連接器只是將您現有的內部部署連接Active Directory到 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。
- S@@ imple AD 是具有基本Active Directory相容性的低規模、低成本的目錄。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。

如需更詳細的 AWS Directory Service 選項比較，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「AWS 管理 Microsoft AD 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 實例加入您的 AWS 受管 Microsoft AD 活動目錄」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」。

瞭解目錄的 AWS 安全性群組組態和使用方式

AWS 建立安全性群組，並將其附加至目錄的網域控制站彈性網路介面。 AWS 設定安全群組以封鎖目錄的不必要流量，並允許必要的流量。

修改目錄安全群組

如果您要修改目錄安全群組的安全，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。不當的變更可能會導致與預定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**
>
> 就技術而言，您可以將目錄的安全群組與您所建立的其他 EC2 執行個體產生關聯。但是，AWS 建議不要這種做法。 AWS 可能有理由修改安全性群組，恕不另行通知，以解決受管理目錄的功能或安全性需求。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 受管理的 Microsoft AD

Simple AD 不支援信任關係。如果您需要建立您的 AWS Directory Service 目錄和另一個目錄之間的信任，您應該使用 AWS Directory Service 的 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。

瞭解應用程式的使 AWS 用者名

AWS Directory Service 為可用於建構使用者名稱的大多數字元格式提供支援。但是，在用戶名上強制執行字符限制，這些用戶名將用於登錄 AWS 應用程序 WorkSpaces，例如 Amazon WorkDocs WorkMail，Amazon 或 Amazon 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 管理 Microsoft AD 的動態 DNS (DDNS) 服務來尋找網域控制站 (DC)。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。這種情況也可能會導致 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，您應該使 AWS Directory Service 用 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 部署其他網域控制器。

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。

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。如需更多彈性擴展選項和其他 Active Directory 功能，請考慮使用 AWS Directory Service for Microsoft Active Directory (標準版或企業版)。

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 地址附加至 AWS 彈性網路界面 (ENI)。

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。由於有大量自訂和商用的立即可用應用程式使用 Active Directory，AWS 不會且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 AWS 與客戶合作，嘗試克服任何可能在安裝應用程式時遇到的困難，我們無法保證所有應用程式是否 (或持續) 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

客戶可根據實際 Active Directory，選擇使用 AWS Directory Service for Microsoft Active Directory (AWS 管理 Microsoft AD) 以達更高層級的相容性。

Simple AD 疑難排解

以下可協助您針對建立或使用目錄時可能遇到的一些常見問題進行故障診斷。

主題

密碼復原

如果使用者忘記密碼，或在登入您的 Simple AD 或 AWS 受管理 Microsoft AD 目錄時遇到問題，您可以使用 AWS Management Console、Windows PowerShell或. AWS CLI

如需詳細資訊，請參閱 重設使用者密碼。

我在新增使用者至 Simple AD 時，接收到 "KDC can't fulfill requested option" 的錯誤

原因可能為 Samba CLI 用戶端並未正確傳送「net」命令至所有網域控制器。如果您在使用「net ads」新增使用者至 Simple AD 目錄時看到此錯誤訊息，請使用 -S 引數，並指定 IP 地址為您的其中一個網域控制器。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 的活動目錄管理工具。

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

如果您嘗試使用 SQL Server Management Studio (SSMS) 與 SQL Server 帳戶來登入 Windows 2012 R2 EC2 執行個體執行的 SQL Server，您可能會收到錯誤。當 SSMS 以域使用者身分執行時，就會發生此問題，並可能導致 "Login failed for user" 錯誤，即使提供有效的憑證也一樣。這是一個已知問題，並 AWS 正在積極解決它。

若要解決此問題，您可以使用 Windows 驗證登入 SQL Server，而不是 SQL 驗證。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 Support 中心 。

當我建立目錄時，收到 "AZ constrained" 錯誤

在 2012 年之前建立的某些 AWS 帳戶可能會存取不支援 AWS Directory Service 目錄的美國東部 (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。這是新使用者帳戶的預設設定，不應該予以修改。如需有關此設定的詳細資訊，請移至 Microsoft 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疑難排解 AWS。

- AWS 知識中心：尋找常見問題集和其他資源的連結，以協助您疑難排解問題。
- AWS S@@ upport 中心 — 取得技術支援。
- AWS 頂級 Support 中心 — 取得頂級技術支援。

主題

Simple AD 目錄狀態原因

當目錄受損或無法操作時，目錄狀態訊息會包含其他資訊。此狀態訊息會顯示在 AWS Directory Service 主控台中，或由 `DirectoryDescription.StageReason` API 以 `DescribeDirectories` 成員傳回。如需目錄狀態的詳細資訊，請參閱「了解您的目錄狀態」。

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

描述

在建立目錄期間代表您建立的用於與 VPC 建立網路連線的關鍵彈性網路介面 (ENI) 未連接到目錄執行個體。此目錄支援的 AWS 應用程式將無法運作。您的目錄無法連線至內部部署網路。

疑難排解

如果 ENI 已分離但仍然存在，請聯絡 AWS Support。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。

疑難排解

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。如果問題仍存在，請聯絡 AWS Support 尋求協助。

目錄中缺少重要的 AWS Directory Service 保留使用者

描述

建立 Simple AD 時，AWS Directory Service 會在目錄中建立名稱為 `AWSAdminD-xxxxxxxxxx` 的服務帳戶。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。

疑難排解

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。

重要的 AWS Directory Service 保留使用者必須屬於 Domain Admins 群組

描述

建立 Simple AD 時，AWS Directory Service 會在目錄中建立名稱為 `AWSAdminD-xxxxxxxxxx` 的服務帳戶。當此服務帳戶不是 `Domain Admins` 群組的成員時，就會收到此錯誤。您必須具備此群組的成員資格，才能將執行維護和復原操作所需的權限授予 AWS Directory Service，例如轉移 FSMO 角色、將新的目錄控制器加入網域，以及從快照還原。

疑難排解

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。

重要的 AWS Directory Service 保留使用者已停用

描述

建立 Simple AD 時，AWS Directory Service 會在目錄中建立名稱為 `AWSAdmin`*`D-xxxxxxxxx`* 的服務帳戶。當停用此服務帳戶時，就會收到此錯誤。您必須啟用此帳戶，AWS Directory Service 才能對目錄執行維護和復原操作。

疑難排解

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。

疑難排解

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 AWS Support 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。

疑難排解

如需 VPC 網路需求的詳細資訊，請參閱 AWS Managed Microsoft AD 的 AWS 管理 Microsoft AD 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 AWS Support 以取得更多協助。

中的安全性 AWS Directory Service

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。若要深入瞭解適用於的規範遵循計劃 AWS Directory Service，請參閱合規方案的AWS 服務範圍。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用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 以符合安全性與合規性目標。您還將學習如何使用其他 AWS 服務來幫助您監控和保護您的 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：

- 的身分識別與存取管理 AWS Directory Service
- 登錄和監控 AWS Directory Service
- 符合性驗證 AWS Directory Service
- 韌性 AWS Directory Service
- 基礎結構安全 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：

帳號、信任和 AWS 資源存取

- 管理員帳戶的權限
- 群組受管服務帳戶
- 建立信任關係
- Kerberos 限制委派

- 授予 AWS 資源存取權給使用者與群組
- 授權使用的 AWS 應用程式和服務 AWS Directory Service

保護您的目錄

- 保護您的 AWS Managed Microsoft AD 目錄
- 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

的身分識別與存取管理 AWS Directory Service

存取權 AWS Directory Service 需要 AWS 可用來驗證您的請求的憑證。這些認證必須具有存取 AWS 資源 (例如 AWS Directory Service 目錄) 的權限。以下各節詳細說明如何使用 AWS Identity and Access Management (IAM)，以及透過控制哪些人可以存取資源 AWS Directory Service 來協助保護資源的安全：

- 身分驗證
- 存取控制

身分驗證

了解如何 AWS 使用 IAM 身分進行存取。

存取控制

您可以擁有有效的認證來驗證您的請求，但除非您擁有權限，否則您無法建立或存取 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權限。

下列各節說明如何管理的權限 AWS Directory Service。我們建議您先閱讀概觀。

- 管理資 AWS Directory Service 源存取權限概觀
- 使用以身分為基礎的政策 (IAM 政策) AWS Directory Service
- AWS Directory Service API 權限：動作、資源和條件參考

管理資 AWS Directory Service 源存取權限概觀

每個 AWS 資源都由一個 AWS 帳號擁有，建立或存取資源的權限由權限原則控制。帳戶管理員可以將許可政策附加到 IAM 身分 (即使用者、群組和角色)，而某些服務 (例如 AWS Lambda) 也支援將權限政策附加至資源。

> **Note**
>
> 帳戶管理員 (或管理員使用者) 是具有管理員權限的使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 最佳實務。

主題

- AWS Directory Service 資源與營運
- 了解資源所有權
- 管理資源存取
- 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 資源與營運

在中 AWS Directory Service，主要資源是一個目錄。 AWS Directory Service 也支援目錄快照資源。但是您只能在現有的目錄中建立快照。因此，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*
快照	arn:aws:ds: *region*:*account-id* :snapshot/ *external-snapshot-id*

AWS Directory Service 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。

了解資源所有權

資源擁有者是建立資源的 AWS 帳號。也就是說，資源擁有者是驗證建立資源之請求的主體實體 (根帳戶、IAM 使用者或 IAM 角色) 的帳戶。 AWS 下列範例說明其如何運作：

- 如果您使用帳號的根帳號認證來建立 AWS Directory Service 資源 (例如目錄)，則您的 AWS 帳號就是該資源的擁有者。 AWS
- 如果您在 AWS 帳戶中建立 IAM 使用者，並授與建立 AWS Directory Service 資源的權限給該使用者，該使用者也可以建立 AWS Directory Service 資源。不過，您的 AWS 帳戶 (使用者所屬) 擁有資源。
- 如果您在具有建立 AWS Directory Service 資源權限的 AWS 帳戶中建立 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。您的 AWS 帳戶 (角色所屬) 擁有資 AWS Directory Service 源。

管理資源存取

許可政策描述誰可以存取哪些資源。下一節說明可用來建立許可政策的選項。

> **Note**
>
> 本節討論在的內容中使用 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。

附加至 IAM 身分的政策稱為身分型政策 (IAM 政策)，而附加至資源的政策則稱為以資源為基礎的政策。 AWS Directory Service 僅支援以身分識別為基礎的政策 (IAM 政策)。

主題

- 身分類型政策 (IAM 政策)
- 資源型政策

身分類型政策 (IAM 政策)

您可以將政策連接到 IAM 身分。例如，您可以執行下列動作：

- 將權限原則附加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權限原則來授與該使用者建立 AWS Directory Service 資源的權限，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。這些動作會顯示資 AWS Directory Service 源的相關資訊，例如目錄或快照集。請注意，元素中的萬用字`Resource`元 (*) 表示該帳號擁有的所有 AWS Directory Service 資源都允許執行這些動作。

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

如需搭配使用以身分識別為基礎的原則的詳細資訊 AWS Directory Service，請參閱。使用以身分為基礎的政策 (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，您可以將政策附加到 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

服務會針對每個 AWS Directory Service 資源定義一組 API 作業。如需詳細資訊，請參閱 AWS Directory Service 資源與營運。如需可用的 API 操作清單，請參閱 Directory Service 動作。

若要授與這些 API 作業的權限，請 AWS Directory Service 定義您可以在政策中指定的一組動作。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，您一律在 IAM 政策中使用萬用字元 (*)。如需詳細資訊，請參閱 AWS Directory Service 資源與營運。
- 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策略，您可以指定要接收權限的使用者、帳戶、服務或其他實體 (僅適用於以資源為基礎的策略)。 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 動作及其套用資源的表格，請參閱AWS Directory Service API 權限：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。但是，您可以視需要使用 AWS 條件索引鍵。如需完整 AWS 金鑰清單，請參閱 IAM 使用者指南中的可用全域條件金鑰。

使用以身分為基礎的政策 (IAM 政策) AWS Directory Service

這個主題提供以身分為基礎的政策範例，在該政策中帳戶管理員可以將許可政策連接至 IAM 身分 (即使用者、群組和角色)。

> **Important**
>
> 我們建議您先檢閱介紹性主題，其中說明可用於管理 AWS Directory Service 資源存取權的基本概念和選項。如需詳細資訊，請參閱 管理資 AWS Directory Service 源存取權限概觀。

本主題中的各節涵蓋下列內容：

- 使用 AWS Directory Service 主控台所需的權限
- AWS 的管理 (預先定義) 策略 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。

```
{
   "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": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudwatch.amazonaws.com"
                }
            }
        }
    ]
}
```

該政策內容如下：

- 第一個陳述式會授與建立 AWS Directory Service 目錄的權限。 AWS Directory Service 在資源層級不支援此特定動作的權限。因此，該政策指定萬用字元 (*) 做為 `Resource` 值。
- 第二個陳述式授予特定 IAM 動作的許可。需要存取 IAM 動作，才 AWS Directory Service 能代表您讀取和建立 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。
- 第三個陳述式授予許可給一組特定的 Amazon EC2 資源，這些資源是 AWS Directory Service 允許建立、設定和銷毀其目錄所必需的。`Resource` 值結尾的萬用字元 (*) 表示該陳述式允許對任何 EC2

資源或子資源執行 EC2 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 (*) 更換為特定資源或子資源。如需詳細資訊，請參閱 Amazon EC2 動作

此政策不指定 `Principal` 元素，因為您不會在以身分為基礎的政策中，指定取得許可的主體。當您將政策連接至使用者時，這名使用者即為隱含主體。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 動作及其套用資源的表格，請參閱AWS Directory Service API 權限：動作、資源和條件參考。

使用 AWS Directory Service 主控台所需的權限

若要使用 AWS Directory Service 主控台的使用者，該使用者必須具有上述原則中所列的權限，或是「Directory Service 完整存取角色」或「Directory Service 唯讀」角色所授與的權限，如中所述AWS 的管理 (預先定義) 策略 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 的管理 (預先定義) 策略 AWS Directory Service

AWS 透過提供由建立和管理的獨立 IAM 政策來解決許多常見使用案例 AWS。受管政策授與常見使用案例中必要的許可，讓您免於查詢需要哪些許可。如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

下列 AWS 受管理的策略 (您可以附加到帳戶中的使用者) 專用於 AWS Directory Service：

- AWSDirectoryServiceReadOnlyAccess— 授予使用者或群組對根 AWS 帳戶的所有 AWS Directory Service 資源、EC2 子網路、EC2 網路界面以及 Amazon Simple Notification Service (Amazon SNS) 主題和訂閱的唯讀存取權。如需詳細資訊，請參閱 對 AWS Directory Service 使用 AWS 受管政策。
- AWSDirectoryServiceFullAccess - 授予使用者或群組以下權限：
  - 完全存取 AWS Directory Service
  - 存取使用所需的主要 Amazon EC2 服務 AWS Directory Service
  - 能夠列出 Amazon SNS 主題
  - 能夠建立、管理和刪除名稱以「DirectoryMonitoring」開頭的 Amazon SNS 主題

  如需詳細資訊，請參閱 對 AWS Directory Service 使用 AWS 受管政策。

此外，還有其他 AWS 受管政策適合與其他 IAM 角色搭配使用。這些原則會指派給與 AWS Directory Service 目錄中使用者相關聯的角色。這些使用者需要這些政策才能存取其他 AWS 資源，例如 Amazon EC2。如需詳細資訊，請參閱 授予 AWS 資源存取權給使用者與群組。

您也可以建立自訂 IAM 政策，讓使用者可存取所需的 API 動作和資源。您可以將這些自訂政策連接至需要這些許可的 IAM 使用者或群組。

客戶受管政策範例

在本節中，您可以找到授與各種 AWS Directory Service 動作權限的範例使用者策略。

> **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。這些動作會顯示資 AWS Directory Service 源的相關資訊，例如目錄或快照集。請注意，元素中的萬用字Resource元 (*) 表示該帳號擁有的所有 AWS Directory Service 資源都允許執行這些動作。

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

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。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                "ds:Create*",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
                  ],
         "Resource":"*"
         ]
      }
   ]
}
```

搭配 IAM 政策使用標籤

您可以在用於大多 AWS Directory Service 數 API 動作的 IAM 政策中套用以標籤為基礎的資源層級許可。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。

只要標籤包含標籤金鑰對「fooKey」:「fooValue」，以下標籤政策範例即允許所有 ds 呼叫。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/fooKey":"fooValue"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

只要資源包含目錄 ID「d-1234567890」，以下資源政策範例即允許所有 ds 呼叫。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"arn:aws:ds:us-east-1:123456789012:directory/d-1234567890"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

如需 ARN 的詳細資訊，請參閱 Amazon 資源名稱 (ARN) 和 AWS 服務命名空間。

下列 AWS Directory Service API 作業清單支援以標籤為基礎的資源層級權限：

- 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 權限：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 權限：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：

- AWS Directory Service API 作業的名稱
- 可由您授予執行此動作之許可的相對應動作。
- 您可以授與權限的 AWS 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`)。某些 AWS 應用程式可能需要`ds:UnauthorizeApplication`在其政策中使用非公開 AWS Directory Service API 作業 `ds:AuthorizeApplication` `ds:CheckAlias` `ds:CreateIdentityPoolDirectory`、`ds:UpdateAuthorizedApplication`，例如、、和。

某些 AWS Directory Service API 只能透過 AWS Management Console. 它們不是公共 API，從某種意義上講，它們不能以編程方式調用，並且它們不是由任何 SDK 提供的。他們接受使用者憑證。這些 API 作業包括`ds:DisableRoleAccess`、`ds:EnableRoleAccess`和`ds:UpdateDirectory`。

您可以在 AWS Directory Service 原則中使用 AWS 全域條件金鑰來表示條件。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。

相關主題

- 存取控制

授權使用的 AWS 應用程式和服務 AWS Directory Service

授權作用中目 AWS 錄上的應用程式

AWS Directory Service 授予所選應用程式的特定權限，以便在您授權應用 AWS 程式時與 Active Directory 無縫整合。 AWS 應用程式僅授與其使用案例所需的存取權。下面提供了授權後授予應用程式和應用程式管理員的內部許可集：

> **Note**
>
> 需要`ds:AuthorizationApplication`權限才能授權新的 AWS 應用程序活動目錄。僅應向設定目錄服務整合的管理員提供此動作的許可。

- 存取 Active Directory 使用者、群組、組織單位、電腦或憑證授權單位資料的受管理 Microsoft AD、簡易 AD、AD AD Connector 目錄，以及 AWS 受管理 Microsoft AD 的受信任網域 (如果 AWS 受信任關係允許) 的所有組織單位 (OU) 中的資料。
- 寫入使用者、群組、群組成員資格、電腦或憑證授權單位資料的存取權限 (AWS Managed Microsoft AD) 的組織單位中。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。

某些 AWS 受管 Microsoft AD 應用程序，如 Amazon RDS 和 Amazon FSx 通過直接網絡連接到您的活動目錄集成。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 應用程式的權限是由在應用程式授權期間在 AWS 保留組織單位 (OU) 中建立的目錄使用者帳戶所控制，其中包括 DNS 管理和針對應用程式建立之自訂 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 權限的詳細資訊，請參閱AWS Directory Service API 權限：動作、資源和條件參考。

如需針對 AWS 受管理的 Microsoft AD 啟 AWS 用應用程式和服務的詳細資訊，請參閱啟用對應用 AWS 程式和服務的存取。如需啟 AWS 用 AD Connector 之應用程式和服務的詳細資訊，請參閱啟用對應用 AWS 程式和服務的存取。如需啟 AWS 用 Simple AD 應用程式和服務的詳細資訊，請參閱啟用對應用 AWS 程式和服務的存取。

取消授權作用中目錄上的 AWS 應用程式

若要移除 AWS 應用程式存取 Active Directory 的權限，需要該`ds:UnauthorizedApplication`權限。按照應用程式提供的步驟將其停用。

登錄和監控 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。這有助於您確保可以調查任何未預期的變更，並且可以復原不想要的變更。 AWS Directory Service 目前支援下列兩項 AWS 服務，因此您可以監視組織及其中發生的活動。

- Amazon CloudWatch -您可以將 CloudWatch 事件與 AWS 受管 Microsoft AD 目錄類型搭配使用。如需詳細資訊，請參閱 啟用日誌轉發。此外，您可以使用 CloudWatch指標來監視網域控制站效能。如需詳細資訊，請參閱 判斷何時新增含 CloudWatch 量度的網域控制站。
- AWS CloudTrail -您可以使用所 CloudTrail 有 AWS Directory Service 目錄類型。如需詳細資訊，請 AWS Directory Service 參閱使用 CloudTrail.

符合性驗證 AWS Directory Service

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

韌性 AWS Directory Service

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需區域和可用區域的詳 AWS 細資訊，請參閱AWS 全域基礎結構。

除了 AWS 全球基礎架構之外，還 AWS Directory Service 提供在任何時間點手動擷取資料快照的功能，以協助支援您的資料恢復能力和備份需求。如需詳細資訊，請參閱 建立目錄快照或還原目錄。

基礎結構安全 AWS Directory Service

身為受管服務， AWS Directory Service 受 Amazon Web Services：安 AWS 全程序概觀白皮書中所述的全球網路安全程序保護。

您可以使用 AWS 已發佈的 API 呼叫透 AWS Directory Service 過網路進行存取。用戶端必須支援 Transport Layer Security (TLS)。建議使用 TLS 1.2 或更新版本。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。

如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140–2 概觀。

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的副問題。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。

我們建議您在資源原則中使用`aws:SourceArn`和`aws:SourceAccount`全域條件內容索引鍵，以限制 Microsoft Active AWS Directory 的 Directory Service 為資源提供其他服務的權限。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。

在下列範例中，的值aws:SourceArn必須是 CloudWatch 記錄群組。

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全域條件內容索引鍵，以防止混淆的副問題。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
    "Resource": [
      "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/
directoryservice/YOUR_LOG_GROUP:*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

對於下列範例，aws:SourceArn 的值必須是您帳戶中的 SNS 主題。例如，您可以使用類似 arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f「ap-東南 -1」是您的區域，「123456789012」是您的客戶識別碼，而「_d-966739499f」是您建立的 Amazon SNS 主題名稱。DirectoryMonitoring

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全域條件內容索引鍵，以防止混淆的副問題。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "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:YOUR_REGION:YOUR_ACCOUNT_NUMBER:YOUR_SNS_TOPIC_NAME"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_EXTERNAL_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
```

```
  }
}
```

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，請參閱由定義的資源類型 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。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
                "sts:AssumeRole"
            ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

使用接口端點訪問 AWS Directory Service API- AWS PrivateLink

您可以使 AWS PrivateLink 用在 VPC 和 AWS Directory Service API 之間建立私人連線。您可以像在 VPC 中一樣存取 AWS Directory Service API，而無需使用網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線。VPC 中的執行個體不需要公有 IP 位址即可存取 AWS Directory Service API。

您可以建立由 AWS PrivateLink提供支援的介面端點來建立此私有連線。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。這些是請求者管理的網路介面，可作為目的地為 AWS Directory Service之流量的進入點。

如需詳細資訊，請參閱AWS PrivateLink 指南 AWS PrivateLink中的 AWS 服務 透過存取。

的注意事項 AWS Directory Service

在為 AWS Directory Service API 端點設定介面端點之前，請先參閱AWS PrivateLink 指南中的考量事項。

AWS Directory Service 支援透過介面端點呼叫其所有 API 動作。

可用性

AWS Directory Service 在下列情況下支援 VPC 端點： AWS 區域

- 美國東部 (維吉尼亞北部)
- AWS GovCloud (美國西部)
- AWS GovCloud (美國東部)

建立的介面端點 AWS Directory Service

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface (AWS CLI) 建立 AWS Directory Service API 的介面端點。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的建立介面端點。

使用下列服務名稱建立 AWS Directory Service API 的介面端點：

```
com.amazonaws.region.ds
```

為您的介面端點建立端點政策

端點政策為 IAM 資源，您可將其連接至介面端點。預設端點策略允許透過介面端點完整存取 AWS Directory Service API。若要控制允許從 VPC 存取 AWS Directory Service API，請將自訂端點原則附加到介面端點。

端點政策會指定以下資訊：

- 可執行動作 (AWS 帳戶、IAM 使用者和 IAM 角色) 的主體。
- 可執行的動作。
- 可供執行動作的資源。

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。

範例：適用於 AWS Directory Service API 動作的 VPC 端點原則

以下是自訂端點政策的範例。當您將此原則附加至介面端點時，它會授與所有資源上所有主參與者所列 AWS Directory Service 動作的存取權。將*## -1*、*## -2* 和*## -3* 取代為您要包含在原則中之 AWS Directory Service API 的必要權限。如需完整清單，請參閱AWS Directory Service API 權限：動作、資源和條件參考。

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds:action-1",
            "ds:action-2",
            "ds:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

AWS Directory Service 服務水準協議

AWS Directory Service 是一項高可用性服務，建置在 AWS 受管基礎設施上。其獲得的服務水準協議用以定義我們的服務可用性政策。

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 管理 Microsoft AD	AD Connect	Simple AD
美國東部 (俄亥俄)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	是	是	否
美國東部 (維吉尼亞北部)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	是	是	是
美國西部 (加利佛尼亞北部)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	是	是	否
美國西部 (奧勒岡)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	是	是	是
Africa (Cape Town)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	是	是	否
亞太區域 (香港)	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	是	是	否

區域名稱	區域	端點	通訊協定	AWS 管理 Microsoft AD	AD Connector	Simple AD
亞太區域 (孟買)	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	是	是	否
亞太區域 (海德拉巴)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	是	是	否
亞太區域 (大阪)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	是	是	否
亞太區域 (首爾)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	是	是	否
亞太區域 (新加坡)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	是	是	是
亞太區域 (雪梨)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	是	是	是
亞太區域 (雅加達)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	是	是	否

區域名稱	區域	端點	通訊協定	AWS 管理 Microsoft AD	AD Connector	Simple AD
亞太區域 (墨爾本)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	是	是	否
亞太區域 (東京)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	是	是	是
加拿大 (中部)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	是	是	否
加拿大西部 (卡加利)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	是	是	否
中國 (北京)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	是	是	否
中國 (寧夏)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	是	是	否
歐洲 (法蘭克福)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	是	是	否

區域名稱	區域	端點	通訊協定	AWS 管理 Microsoft AD	AD Connector	Simple AD
歐洲 (蘇黎世)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	是	是	否
歐洲 (愛爾蘭)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	是	是	是
歐洲 (倫敦)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	是	是	否
Europe (Paris)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	是	是	否
歐洲 (斯德哥爾摩)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	是	是	否
歐洲 (米蘭)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	是	是	否
歐洲 (西班牙)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	是	是	否

區域名稱	區域	端點	通訊協定	AWS 管理 Microsoft AD	AD Connector	Simple AD
以色列 (特拉維夫)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	是	是	否
中東 (巴林)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	是	是	否
中東 (阿拉伯聯合大公國)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	是	是	否
南美洲 (聖保羅)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	是	是	否
AWS GovCloud (美國西部)	us-gov-west-1	ds. us-gov-west-1. 亞馬遜	HTTPS	是	是	否
AWS GovCloud (美國東部)	us-gov-east-1	ds. us-gov-east-1. 亞馬遜	HTTPS	是	是	否

如需 AWS Directory Service 在 AWS GovCloud (美國西部) 區域和 AWS GovCloud (美國東部) 區域中使用的相關資訊，請參閱服務端點。

如需 AWS Directory Service 在北京和寧夏區域使用的相關資訊，請參閱中國 Amazon Web Services 的端點和 ARN。

瀏覽器相容性

AWS 應用程式和服務 (例如 Amazon WorkSpaces、Amazon Connect WorkMail、Amazon Chime、Amazon) 以及所有應用程式和服務 AWS IAM Identity Center 都需要從相容瀏覽器有效的登入登入資料 WorkDocs，才能存取這些資料。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 Internet Explorer	Desktop IE 第 7 版和較舊版本	不相容
	Desktop IE 第 8、9 和 10 版	僅有在執行 Windows 7 或更新版本，且啟用 TLS 1.1 的情況下才相容。如需詳細資訊，請參閱什麼是 TLS？。
	Desktop IE 第 11 版和更新版本	相容
	Mobile IE 第 10 版和較舊版本	不相容
	Mobile IE 第 11 版和更新版本	相容
Microsoft Edge	所有版本	相容
Mozilla Firefox	Firefox 23 和較舊版本	不相容
	Firefox 24 至 26	相容，但預設為不相容。
	Firefox 27 和更新版本	相容
Google Chrome	Google Chrome 21 和較舊版本	不相容
	Google Chrome 22 至 37	相容，但預設為不相容。
	Google Chrome 38 和更新版本	相容
Apple Safari	適用於 OS X 10.8 (Mountain Lion) 及較舊版本的 Desktop Safari 第 6 版和較舊版本	不相容

瀏覽器	版本	相容性
	適用於 OS X 10.9 (Mavericks) 及更新版本的 Desktop Safari 第 7 版和更新版本	相容
	適用於 iOS 4 及較舊版本的 Mobile Safari	不相容
	適用於 iOS 5 及更新版本的 Mobile Safari 第 5 版和更新版本	相容

現在您已確認正在使用受支援的瀏覽器版本，我們建議您也檢閱下方章節，確定瀏覽器已設定成使用 AWS要求的 Transport Layer Security (TLS) 設定。

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 以進行安全登入。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。舉例來說，在 Internet Explorer 中，您可以移至 Internet Properties (網際網路內容) 的 Advanced (進階) 索引標籤，並在 Security (安全性) 區段中找到各種 TLS 選項。如需特定說明，請查看瀏覽器製造商的說明網站。

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
以憑證為基礎的身分驗證設定	已新增有關受 AWS 管理 Microsoft AD 兩個新安全性設定的相關內容。	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 AWS GovCloud (美國西部) 區域支援智慧卡和 Amazon WorkSpaces 應用程式管理員的相關內容	2020 年 12 月 1 日
密碼重設	已新增有關如何使用 AWS Management Console、Windows PowerShell和重設使用者密碼的內容 AWS CLI。	2019 年 1 月 2 日
目錄共享	已新增有關如何透過 AWS 受管理的 Microsoft AD 使用目錄共用的內容。	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 委派群組	已新增可指 AWS 派給內部部署使用者的委派群組清單。	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	已新增有關如何在 AWS 受管理 Microsoft AD 中將更多網域控制站新增至目錄的內容。	2017 年 6 月 30 日
教學課程	已新增測試 AWS 受管理 Microsoft AD 實驗室環境的新教學課程。	2017 年 6 月 21 日
MFA 與 AWS 管理 Microsoft AD	已新增與 AWS 受管理 Microsoft AD 搭配使用 MFA 的相關內容。	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	已新增關於具有 AWS Directory Service 的結構描述延伸模組的內容。	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	已新增有關如何搭配使用 IAM 的內容 AWS Directory Service。	2016 年 2 月 25 日
AWS 管理 Microsoft AD	將有關 AWS 受管理 Microsoft AD 的內容以及合併指南新增至單一指南。	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。