



配置 **Active Directory**、**LDAP** 和 **LDAPS** SnapCenter software

NetApp
November 06, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/snapcenter-61/install/task_register_untrusted_active_directory_domains.html on November 06, 2025. Always check docs.netapp.com for the latest.

目錄

配置 Active Directory、LDAP 和 LDAPS	1
註冊不受信任的 Active Directory 網域	1
設定 IIS 應用程式集區以啟用 Active Directory 讀取權限	2
為 LDAPS 設定 CA 用戶端憑證	3

配置 Active Directory、LDAP 和 LDAPS

註冊不受信任的 Active Directory 網域

您應該向 SnapCenter Server 註冊 Active Directory，以管理來自多個不受信任的 Active Directory 網域的主機、使用者和群組。

開始之前

LDAP 和 LDAPS 協議

- 您可以使用 LDAP 或 LDAPS 協定註冊不受信任的活動目錄網域。
- 您應該已經啟用插件主機和 SnapCenter 伺服器之間的雙向通訊。
- 應設定從 SnapCenter 伺服器到插件主機的 DNS 解析，反之亦然。

LDAP 協定

- 完全限定網域名稱 (FQDN) 應該可以從 SnapCenter Server 解析。

您可以使用 FQDN 註冊不受信任的網域。如果無法從 SnapCenter 伺服器解析 FQDN，則可以使用網域控制器 IP 位址進行註冊，並且該位址應該可以從 SnapCenter 伺服器解析。

LDAPS 協定

- LDAPS 需要 CA 憑證來在活動目錄通訊期間提供端對端加密。

"為 LDAPS 設定 CA 用戶端憑證"

- 網域控制器主機名稱 (DCHostName) 應該可以從 SnapCenter 伺服器存取。

關於此任務

- 您可以使用 SnapCenter 使用者介面、PowerShell cmdlet 或 REST API 來註冊不受信任的網域。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「全域設定」。
3. 在全域設定頁面中，按一下「網域設定」。
4. 點選  註冊一個新網域。
5. 在註冊新網域頁面中，選擇 **LDAP** 或 **LDAPS**。
 - a. 如果選擇 **LDAP**，請指定為 LDAP 註冊不受信任網域所需的資訊：

對於這個領域...	這樣做...
網域	指定網域的 NetBIOS 名稱。
域 FQDN	指定 FQDN 並按一下 解析。
網域控制器 IP 位址	如果無法從SnapCenter伺服器解析網域 FQDN，請指定一個或多個網域控制器 IP 位址。 有關更多信息，請參閱 "從 GUI 為不受信任的網域新增網域控制器 IP"。

b. 如果選擇 **LDAPS**，請指定為 LDAPS 註冊不受信任網域所需的資訊：

對於這個領域...	這樣做...
網域	指定網域的 NetBIOS 名稱。
域 FQDN	指定 FQDN。
網域控制器名稱	指定一個或多個網域控制站名稱，然後按一下「解析」。
網域控制器 IP 位址	如果網域控制站名稱無法從SnapCenter Server 解析，則應修正 DNS 解析。

6. 按一下“確定”。

設定 IIS 應用程式集區以啟用 **Active Directory** 讀取權限

當您需要為SnapCenter啟用 Active Directory 讀取權限時，您可以在 Windows Server 上設定 Internet 資訊服務 (IIS) 來建立自訂應用程式集區帳戶。

步驟

1. 在安裝了SnapCenter的 Windows Server 上開啟 IIS 管理員。
2. 在左側導覽窗格中，按一下「應用程式集區」。
3. 在應用程式集區清單中選擇SnapCenter，然後按一下操作窗格中的「進階設定」。
4. 選擇“身分”，然後按一下“...”以編輯SnapCenter應用程式集區身分。
5. 在自訂帳戶欄位中，輸入具有 Active Directory 讀取權限的網域使用者或網域管理員帳戶名稱。
6. 按一下“確定”。

自訂帳戶取代了SnapCenter應用程式集區的內建 ApplicationPoolIdentity 帳戶。

為 LDAPS 設定 CA 用戶端憑證

當 Windows Active Directory LDAPS 配置了 CA 憑證時，您應該在SnapCenter伺服器上為 LDAPS 設定 CA 用戶端憑證。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
在嚮導的第二頁	按一下“瀏覽”，選擇“根憑證”，然後按一下“下一步”。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。

7. 對中間證書重複步驟 5 和 6。

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。