



設定LDAP over TLS

ONTAP 9

NetApp
June 19, 2024

目錄

設定LDAP over TLS	1
匯出自我簽署根CA憑證的複本	1
在SVM上安裝自我簽署的根CA憑證	1
在伺服器上啟用LDAP over TLS	2

設定LDAP over TLS

匯出自我簽署根CA憑證的複本

若要使用LDAP over SSL/TLS來保護Active Directory通訊安全、您必須先將Active Directory憑證服務的自我簽署根CA憑證複本匯出至憑證檔案、然後將其轉換成Ascii文字檔。這個文字檔是ONTAP 由SITALL用來在儲存虛擬機器（SVM）上安裝憑證。

開始之前

Active Directory憑證服務必須已針對CIFS伺服器所屬的網域進行安裝和設定。如需安裝及設定Active Director憑證服務的相關資訊、請參閱Microsoft TechNet程式庫。

["Microsoft TechNet程式庫：technet.microsoft.com"](https://technet.microsoft.com)

步驟

1. 取得中網域控制站的根 CA 憑證 .pem 文字格式。

["Microsoft TechNet程式庫：technet.microsoft.com"](https://technet.microsoft.com)

完成後

在SVM上安裝憑證。

相關資訊

["Microsoft TechNet程式庫"](https://technet.microsoft.com)

在SVM上安裝自我簽署的根CA憑證

如果在連結至LDAP伺服器時需要使用TLS進行LDAP驗證、您必須先在SVM上安裝自我簽署的根CA憑證。

關於這項工作

啟用LDAP over TLS時、ONTAP SVM上的SVM上的SfyLDAP用戶端不支援ONTAP 使用版本為9.0和9.1的撤銷憑證。

從ONTAP 功能支援的9.2開始、ONTAP 所有使用TLS通訊的應用程式都可以使用線上憑證狀態傳輸協定（OCSP）來檢查數位憑證狀態。如果在TLS上為LDAP啟用OCSP、則撤銷的憑證會遭到拒絕、連線也會失敗。

步驟

1. 安裝自我簽署的根CA憑證：

- a. 開始安裝憑證：`security certificate install -vserver vserver_name -type server-ca`

主控台輸出會顯示下列訊息：Please enter Certificate: Press <Enter> when done

- b. 開啟憑證 .pem 使用文字編輯器檔案、複製憑證、包括開頭的行 -----BEGIN CERTIFICATE-----

並以結束 -----END CERTIFICATE-----，然後在命令提示字元之後貼上憑證。

- c. 確認已正確顯示憑證。
- d. 按Enter完成安裝。

2. 確認已安裝憑證：`security certificate show -vserver vserver_name`

在伺服器上啟用LDAP over TLS

您的SMB伺服器必須先修改SMB伺服器安全性設定、才能使用TLS與Active Directory LDAP伺服器進行安全通訊。

從ONTAP 《支援範圍》9.10.1開始、Active Directory (AD) 和名稱服務LDAP連線預設都支援LDAP通道繫結。僅當啟用Start-TLS或LDAPS並將工作階段安全性設定為簽署或密封時、才能嘗試透過LDAP連線進行通道繫結。ONTAP若要停用或重新啟用與AD伺服器的LDAP通道繫結、請使用 `-try-channel-binding-for-ad-ldap` 參數 `vserver cifs security modify` 命令。

若要深入瞭解、請參閱：

- ["LDAP 概述"](#)
- ["2020 LDAP通道繫結和LDAP簽署要求、適用於Windows"](#)。

步驟

1. 設定 SMB 伺服器安全性設定、以允許與 Active Directory LDAP 伺服器進行安全的 LDAP 通訊：`vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. 確認 LDAP over TLS 安全性設定已設定為 true：`vserver cifs security show -vserver vserver_name`



如果 SVM 使用相同的 LDAP 伺服器來查詢名稱對應或其他 UNIX 資訊（例如使用者、群組和網路群組）、則您也必須修改 `-use-start-tls` 選項：使用 `vserver services name-service ldap client modify` 命令。

版權資訊

Copyright © 2024 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 保留隨時變更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。