# 設定LDAP over TLS

ONTAP 9

NetApp
June 19, 2024

# 目錄

# 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"

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"

完成後

在SVM上安裝憑證。

相關資訊

"Microsoft TechNet程式庫"

## 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



## 商標資訊