



# 在 Linux 主機上設定並啟用雙向 SSL 通信

## SnapCenter software

NetApp  
November 06, 2025

# 目錄

在 Linux 主機上設定並啟用雙向 SSL 通信 . . . . .	1
在 Linux 主機上設定雙向 SSL 通信 . . . . .	1
在 Linux 主機上啟用 SSL 通信 . . . . .	2

# 在 Linux 主機上設定並啟用雙向 SSL 通信

## 在 Linux 主機上設定雙向 SSL 通信

您應該配置雙向 SSL 通訊以保護 Linux 主機上的SnapCenter伺服器與插件之間的相互通訊。

### 開始之前

- 您應該已經為 Linux 主機設定了 CA 憑證。
- 您必須在所有插件主機和SnapCenter伺服器上啟用雙向 SSL 通訊。

### 步驟

1. 將 **certificate.pem** 複製到 `/etc/pki/ca-trust/source/anchors/`。
  - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
  - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
  - `update-ca-trust extract`
3. 驗證證書是否已新增至信任清單。`trust list | grep "<CN of your certificate>"`
4. 更新SnapCenter **nginx** 檔案中的 **ssl\_certificate** 和 **ssl\_certificate\_key** 並重新啟動。
  - `vim /etc/nginx/conf.d/snapcenter.conf`
  - `systemctl restart nginx`
5. 刷新SnapCenter伺服器 GUI 連結。
6. 更新位於 `_ /<安裝路徑>/ NetApp/snapcenter/SnapManagerWeb_` 的 **\* SnapManager.Web.UI.dll.config\*** 和位於 `/<安裝路徑>/ NetApp/snapcenter/SMCore` 的 **SMCoreServiceHost.dll.config** 中的下列登錄項目的值。
  - `<add key="SERVICE_CERTIFICATE_PATH" value="<證書.pfx 的路徑>" />`
  - `<新增鍵="SERVICE_CERTIFICATE_PASSWORD"值="<密碼>"/>`
7. 重新啟動以下服務。
  - `systemctl restart smcore.service`
  - `systemctl restart snapmanagerweb.service`
8. 驗證憑證是否已附加至SnapManager Web 連接埠。`openssl s_client -connect localhost:8146 -brief`
9. 驗證憑證是否已附加到 smcore 連接埠。`openssl s_client -connect localhost:8145 -brief`
10. 管理 SPL 金鑰庫和別名的密碼。
  - a. 檢索指派給 SPL 屬性檔案中的 **SPL\_KEYSTORE\_PASS** 鍵的 SPL 金鑰庫預設密碼。
  - b. 更改密鑰庫密碼。`keytool -storepasswd -keystore keystore.jks`
  - c. 更改所有私鑰條目別名的密碼。`keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`

- d. 為 *spl.properties* 中的金鑰 **SPL\_KEYSTORE\_PASS** 更新相同的密碼。
  - e. 重新啟動服務。
11. 在插件 Linux 主機上，在 SPL 插件的金鑰庫中新增根憑證和中間憑證。
- keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in *spl.properties* file>
  - keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in *spl.properties* file> -deststoretype JKS
    - i. 檢查 keystore.jks 中的條目。keytool -list -v -keystore <path to keystore.jks>
    - ii. 如果需要，請重新命名任何別名。keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas
12. 使用儲存在 *keystore.jks* 中的 **certificate.pfx** 的別名更新 *spl.properties* 檔案中的 **SPL\_CERTIFICATE\_ALIAS** 的值，然後重新啟動 SPL 服務：systemctl restart spl
13. 驗證憑證是否已附加到 smcore 連接埠。openssl s\_client -connect localhost:8145 -brief

## 在 Linux 主機上啟用 SSL 通信

您可以啟用雙向 SSL 通信，以使用 PowerShell 命令保護 Linux 主機上的 SnapCenter 同伺服器與插件之間的相互通訊。

步

1. 執行以下操作以啟用單向 SSL 通訊。
  - a. 登入 SnapCenter GUI。
  - b. 按一下“設定”>“全域設定”，然後選擇“在 SnapCenter 同伺服器上啟用憑證驗證”。
  - c. 按一下“主機”>“託管主機”，然後選擇要啟用單向 SSL 的插件主機。
  - d. 點選  圖標，然後按一下\*啟用憑證驗證\*。
2. 從 SnapCenter Server Linux 主機啟用雙向 SSL 通訊。
  - Open-SmConnection
  - Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>
  - Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost
  - Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}

## 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。