



設定CA憑證

SnapCenter software

NetApp
February 20, 2026

目錄

設定CA憑證	1
產生CA認證CSR檔案	1
匯入CA憑證	1
取得CA憑證指紋	2
使用Windows主機外掛程式服務設定CA憑證	2
為 Linux 主機上的 NetApp 支援外掛程式服務設定 CA 憑證	3
管理插件金鑰庫的密碼以及正在使用的 CA 簽章金鑰對的別名	3
設定根憑證或中間憑證以插入信任庫	4
配置 CA 簽署金鑰對以插入信任庫	4
為插件配置憑證撤銷清單 (CRL)	5
為 Windows 主機上的 NetApp 支援外掛程式服務設定 CA 憑證	5
管理插件金鑰庫的密碼以及正在使用的 CA 簽章金鑰對的別名	5
設定根憑證或中間憑證以插入信任庫	6
配置 CA 簽署金鑰對以插入信任庫	6
為 SnapCenter 外掛程式設定憑證撤銷清單 (CRL)	7
啟用外掛程式的CA憑證	7

設定CA憑證

產生CA認證CSR檔案

您可以產生「憑證簽署要求」(CSR)、然後匯入可以使用產生的CSR從「憑證授權單位」(CA)取得的憑證。憑證將會有與其相關的私密金鑰。

CSR是編碼文字區塊、提供給授權憑證廠商以取得簽署的CA憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

如需產生CSR的資訊、請參閱 ["如何產生CA憑證CSR檔案"](#)。



如果您擁有網域 (*.domain.company.com) 或系統 (machine1.domain.company.com) 的CA憑證、您可以跳過產生CA憑證CSR檔案的步驟。您可以使用SnapCenter 效益管理程式來部署現有的CA憑證。

對於叢集組態、叢集名稱 (虛擬叢集FQDN) 和各自的主機名稱應在CA憑證中提及。您可以在取得憑證之前填寫「Subject Alternative Name (SAN) (主體替代名稱 (SAN))」欄位、以更新憑證。若為萬用字元憑證 (*.domain.company.com)、憑證將會隱含包含網域的所有主機名稱。

匯入CA憑證

您必須SnapCenter 使用Microsoft管理主控台 (MMC)、將CA憑證匯入到S倚賴者支援的伺服器和Windows主機外掛程式。

步驟

- 移至Microsoft管理主控台 (MMC)、然後按一下*檔案*>*新增/移除Snapin*。
- 在「新增或移除嵌入式管理單元」視窗中、選取「憑證」、然後按一下「新增」。
- 在「憑證」嵌入式管理單元視窗中、選取「電腦帳戶」選項、然後按一下「完成」。
- 按一下*主控台根目錄*>*憑證-本機電腦*>*信任的根憑證授權單位*>*憑證*。
- 在「Trusted Root Certification Authorities」(受信任的根憑證授權單位) 資料夾上按一下滑鼠右鍵、然後選取「* All Tasks」(所有工作) > 「Import」(匯入) 以啟動匯入精靈。
- 完成精靈、如下所示：

在此精靈視窗中...	請執行下列動作...
匯入私密金鑰	選取選項* Yes*、匯入私密金鑰、然後按一下* Next*。
匯入檔案格式	不做任何變更；按一下*下一步*。

在此精靈視窗中...	請執行下列動作...
安全性	指定匯出憑證所使用的新密碼、然後按一下*「下一步*」。
完成「憑證匯入精靈」	檢閱摘要、然後按一下「完成」開始匯入。



匯入憑證應與私密金鑰搭售（支援的格式為：`。pfx`、`。p12`和*`。p7b`）。

7. 對「Personal」資料夾重複步驟5。

取得CA憑證指紋

憑證指紋是用來識別憑證的十六進位字串。指紋是使用指紋演算法、從憑證內容中計算出來。

步驟

1. 在GUI上執行下列步驟：
 - a. 按兩下憑證。
 - b. 在「憑證」對話方塊中、按一下「詳細資料」索引標籤。
 - c. 捲動欄位清單、然後按一下* Thumbprint*。
 - d. 複製方塊中的十六進位字元。
 - e. 移除十六進位數字之間的空格。

例如、如果指紋為：「A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 d 42 77 A3 2a 7b」、則移除空格後、將會是：「a909502dd82ae41433e6f83886b00d4277a32a7b」。

2. 從PowerShell執行下列作業：
 - a. 執行下列命令、列出已安裝憑證的指紋、並依主體名稱識別最近安裝的憑證。

```
Get-ChildItem 路徑認證：\LocalComputer\My
```

- b. 複製指紋。

使用Windows主機外掛程式服務設定CA憑證

您應該使用Windows主機外掛程式服務來設定CA憑證、以啟動安裝的數位憑證。

請在SnapCenter 已部署CA憑證的所有插件主機上執行下列步驟。

步驟

1. 執行下列命令、以SMCore預設連接埠8145移除現有的憑證繫結：

```
'>netsh http DELETE sslcert ipport=0.00.0.0: _<SMCore Port>'
```

例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145  
· 執行下列命令、將新安裝的憑證與Windows主機外掛程式服務連結：
```

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

為 Linux 主機上的 NetApp 支援外掛程式服務設定 CA 憑證

您應該管理插件金鑰庫及其憑證的密碼，配置 CA 證書，將根或中間證書配置到插件信任庫，並使用 SnapCenter 插件服務將 CA 簽章金鑰對配置到插件信任庫以啟動已安裝的數位憑證。

插件使用位於 `/opt/NetApp/snapcenter/scc/etc` 的檔案「keystore.jks」作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 CA 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

這是對應至金鑰「keystore_pass」的值。

2. 變更Keystore密碼：

```
keytool -storepasswd -keystore keystore.jks  
· 將Keystore中私密金鑰項目的所有別名密碼變更為與Keystore相同的密碼：
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

在 `_agent.properties_` 檔案中更新 `keyKeystore_pass` 的相同更新。

3. 變更密碼後重新啟動服務。



插件金鑰庫的密碼和所有相關私鑰別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導航至包含插件金鑰庫的資料夾：`/opt/NetApp/snapcenter/scc/etc`。
2. 找到「`keystore .jks`」檔案。
3. 在Keystore中列出新增的憑證：

```
「keytool-list -v -keystore keystore .jks」
```

4. 新增根或中繼憑證：

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. 設定根憑證或中間憑證以插入信任庫後重新啟動服務。
```



您應該先新增根CA憑證、然後再新增中繼CA憑證。

配置 CA 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫中。

步驟

1. 導航至包含插件金鑰庫 `/opt/NetApp/snapcenter/scc/etc` 的資料夾。
2. 找到「`keystore .jks`」檔案。
3. 在Keystore中列出新增的憑證：

```
「keytool-list -v -keystore keystore .jks」
```

4. 新增具有私密金鑰和公開金鑰的CA憑證。

```
「keytool-importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype.kcs12  
-destkeystore keyKeystore .jks -deststoretype.jks」
```

5. 在Keystore中列出新增的憑證。

```
「keytool-list -v -keystore keystore .jks」
```

6. 驗證密鑰庫是否包含與新CA憑證對應的別名、該CA憑證已新增至金鑰庫。
7. 將CA憑證的新增私密金鑰密碼變更為金鑰庫密碼。

預設插件密鑰庫密碼是 agent.properties 檔案中密鑰 KEYSTORE_PASS 的值。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

• 如果CA憑證中的別名很長且包含空格或特殊字元（「*」、「」、「」）、請將別名變更為簡單名稱：

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

• 在agent.properties檔案中設定CA憑證的別名。

請根據SCC_IDATure_ALIAS金鑰更新此值。

8. 配置 CA 簽署的金鑰對以插入信任庫後重新啟動服務。

為插件配置憑證撤銷清單 (CRL)

關於這項工作

- SnapCenter 插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenter 插件的 CRL 檔案的預設目錄是「opt / NetApp / snapcenter / scc / etc / crl」。

步驟

1. 您可以根據金鑰CRP_path修改及更新agent.properties檔案中的預設目錄。

您可以在此目錄中放置多個CRL檔案。傳入的憑證會根據每個CRL進行驗證。

為 Windows 主機上的 NetApp 支援外掛程式服務設定 CA 憑證

您應該管理插件金鑰庫及其憑證的密碼，配置 CA 證書，將根或中間證書配置到插件信任庫，並使用 SnapCenter 插件服務將 CA 簽章金鑰對配置到插件信任庫以啟動已安裝的數位憑證。

外掛程式使用位於 C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc 的檔案 keystore.jks 作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 CA 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

它是對應於key_keystore_pass的值。

2. 變更Keystore密碼：

```
keytool-storepasswd -keystore keystore.jks
```



如果Windows命令提示字元無法辨識「keytool」命令、請將keytool命令替換為完整路徑。

```
C : \Program Files\Java\<JDK_VERSION>\BIN\keytool.exe"-storepasswd -keystore keyKeystore .jks
```

3. 將Keystore中私密金鑰項目的所有別名密碼變更為與Keystore相同的密碼：

```
keytool-keypasswd -alias "alias name_in_cert" -keystore keystore .jks
```

在_agent.properties_檔案中更新keyKeystore_pass的相同更新。

4. 變更密碼後重新啟動服務。



插件金鑰庫的密碼和所有相關私鑰別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc
2. 找到「keystore .jks」檔案。
3. 在Keystore中列出新增的憑證：

```
keytool-list -v -keystore keyKeystore .jks
```

4. 新增根或中繼憑證：

```
keytool-import -cactacerts -alias myRootCA -file /root/USERTrust_root.cer -keystore keyKeystore .jks
```

5. 設定根憑證或中間憑證以插入信任庫後重新啟動服務。



您應該先新增根CA憑證、然後再新增中繼CA憑證。

配置 CA 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫中。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc
2. 找到檔案_keystore °.jks_。
3. 在Keystore中列出新增的憑證：

```
keytool-list -v -keystore keyKeystore .jks
```

4. 新增具有私密金鑰和公開金鑰的CA憑證。

```
keytool-importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype.kcs12  
-destkeystore keyKeystore .jks -deststoretype.jks
```

5. 在Keystore中列出新增的憑證。

```
keytool-list -v -keystore keyKeystore .jks
```

6. 驗證密鑰庫是否包含與新CA憑證對應的別名、該CA憑證已新增至金鑰庫。
7. 將CA憑證的新增私密金鑰密碼變更為金鑰庫密碼。

預設插件密鑰庫密碼是 agent.properties 檔案中密鑰 KEYSTORE_PASS 的值。

```
keytool-keypasswd -alias "alias name_in_CA_cert "-keystore keyKeystore .jks
```

8. 在_agent.properties_ 檔案中設定CA憑證的別名。

請根據SCC_IDATure_ALIAS金鑰更新此值。

9. 配置 CA 簽署的金鑰對以插入信任庫後重新啟動服務。

為 SnapCenter 外掛程式設定憑證撤銷清單 (CRL)

關於這項工作

- 若要下載相關CA憑證的最新CRL檔案、請參閱 ["如何更新SnapCenter 「驗證CA憑證」 中的憑證撤銷清單檔案"](#)。
- SnapCenter 插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenter 外掛程式的 CRL 檔案的預設目錄是 'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\crl'_。

步驟

1. 您可以根據金鑰CRP_path修改及更新_agent.properties_ 檔案中的預設目錄。
2. 您可以在此目錄中放置多個CRL檔案。

傳入的憑證會根據每個CRL進行驗證。

啟用外掛程式的CA憑證

您應該設定CA憑證、並在SnapCenter 伺服器 and 對應的外掛程式主機上部署CA憑證。您應該為外掛程式啟用CA憑證驗證。

開始之前

- 您可以使用run `Set-SmCertificateSettings` Cmdlet來啟用或停用CA憑證。
- 您可以使用`_Get-SmCertificateSettings_`來顯示外掛程式的憑證狀態。

您可以執行`_Get-Help`命令name_來取得可搭配Cmdlet使用之參數及其說明的相關資訊。或者、您也可以參閱 ["《軟件指令程式參考指南》 SnapCenter"](#)。

步驟

1. 在左側導覽窗格中、按一下*主機*。

2. 在「主機」頁面中、按一下「託管主機」。
3. 選取單一或多個外掛程式主機。
4. 按一下*更多選項*。
5. 選取*啟用憑證驗證*。

完成後

「受管理的主機」標籤主機會顯示掛鎖、掛鎖的色彩則會指出SnapCenter「支援服務器」與外掛主機之間的連線狀態。

- *  *表示CA憑證既未啟用、也未指派給外掛程式主機。
- *  *表示CA憑證已成功驗證。
- *  *表示無法驗證CA憑證。
- *  *表示無法擷取連線資訊。



當狀態為黃色或綠色時、資料保護作業會成功完成。

版權資訊

Copyright © 2026 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。