



# 設定 Windows 主機的 CA 憑證

## SnapCenter Software 6.0

NetApp  
July 23, 2024

# 目錄

設定 Windows 主機的 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
使用SnapCenter 站台設定CA憑證 .....	3
啟用CA認證SnapCenter 以供使用 .....	4

# 設定 Windows 主機的 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 金鑰長度至少應為 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

1. 移至Microsoft管理主控台 (MMC)、然後按一下\*檔案\*>\*新增/移除Snapin\*。
2. 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」。
3. 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」。
4. 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\*。
5. 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。
6. 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"
```

## 使用SnapCenter 站台設定CA憑證

您應該在SnapCenter Windows主機上使用站台來設定CA憑證。

步驟

1. 在SnapCenter 安裝了Windows\*的Windows Server上開啟「IIS管理員」。
2. 在左導覽窗格中、按一下\*連線\*。
3. 展開伺服器 and \*站台\* 的名稱。
4. 選取SnapCenter 您要在其中安裝SSL憑證的站台。
5. 瀏覽至\* Actions > Edit Site>、按一下\* Bindings \*。
6. 在「繫結」頁面中、選取「\*繫結https \*」。
7. 按一下 \* 編輯 \*。
8. 從SSL憑證下拉式清單中、選取最近匯入的SSL憑證。
9. 按一下「確定」。



SnapCenter 排程器站台（預設連接埠：8154、HTTPS）是以自我簽署的憑證進行設定。此連接埠正在 SnapCenter 伺服器主機內通訊、因此不一定要使用 CA 憑證進行設定。不過、如果您的環境要求您使用 CA 憑證、請使用 SnapCenter 排程器網站重複步驟 5 至 9。



如果下拉式功能表中未列出最近部署的CA憑證、請檢查CA憑證是否與私密金鑰相關聯。



請確定使用下列路徑新增憑證：主控台根目錄>憑證-本機電腦>信任的根憑證授權單位>憑證。

## 啟用CA認證SnapCenter 以供使用

您應該設定CA憑證、並啟用SnapCenter 適用於該伺服器的CA憑證驗證。

### 開始之前

- 您可以使用Set-SmCertificateSettings Cmdlet來啟用或停用CA憑證。
- 您可以SnapCenter 使用Get-SmCertificateSettings Cmdlet來顯示驗證伺服器的憑證狀態。





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「設定」頁面中、瀏覽至\*設定\*>\*全域設定\*>\* CA憑證設定\*。
2. 選取\*啟用憑證驗證\*。
3. 按一下「\*套用\*」。

### 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。

- \*  \*表示沒有啟用CA憑證或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 © 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。