



# 設定並啟用雙向 **SSL** 通訊

## SnapCenter Software 4.9

NetApp  
March 20, 2024

# 目錄

設定並啟用雙向 SSL 通訊 .....	1
設定雙向 SSL 通訊 .....	1
啟用雙向 SSL 通訊 .....	3

# 設定並啟用雙向 SSL 通訊

## 設定雙向 SSL 通訊

您應該設定雙向 SSL 通訊、以確保 SnapCenter 伺服器與外掛程式之間的相互通訊安全無虞。

開始之前

- 您應該已產生 CA 憑證 CSR 檔案、其支援金鑰長度下限為 3072 。
- CA 憑證應支援伺服器驗證和用戶端驗證。
- 您應該擁有內含私密金鑰和指紋詳細資料的 CA 憑證。
- 您應該已啟用單向 SSL 組態。

如需詳細資料、請參閱 ["設定 CA 憑證區段。"](#)

- 您必須在所有外掛主機和 SnapCenter 伺服器上啟用雙向 SSL 通訊。

不支援某些主機或伺服器未啟用雙向 SSL 通訊的環境。

步驟

1. 若要繫結連接埠、請在 SnapCenter 伺服器主機上針對 SnapCenter IIS 網頁伺服器連接埠 8146（預設）執行下列步驟、並使用 PowerShell 命令再次為 SMCore 連接埠 8145（預設）執行下列步驟。

- a. 使用下列 PowerShell 命令移除現有的 SnapCenter 自我簽署憑證連接埠繫結。

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
```

例如、

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

```
> netsh http delete sslcert ipport=0.0.0.0:8146
```

- b. 將新取得的 CA 憑證與 SnapCenter 伺服器和 SMCore 連接埠繫結。

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>  
certhash=$cert appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

例如、

```

> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

> netsh http show sslcert ipport=0.0.0.0:8145

```

2. 若要存取 CA 憑證的權限、請執行下列步驟、在憑證權限清單中新增 SnapCenter 的預設 IIS Web 伺服器使用者 "IIS AppPool、SnapCenter"、以存取新取得的 CA 憑證。
  - a. 移至 Microsoft 管理主控台 (MMC)、然後按一下 \* 檔案 \* > \* 新增 / 移除 Snapin \*。
  - b. 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」。
  - c. 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」。
  - d. 按一下\*主控台根目錄\*>\*憑證-本機電腦\*>\*個人\*>\*憑證\*。
  - e. 選取 SnapCenter 憑證。
  - f. 若要啟動新增使用者 \ 權限精靈、請在 CA 憑證上按一下滑鼠右鍵、然後選取 \* 所有工作 \* > \* 管理私密金鑰 \*。
  - g. 按一下 \* 新增 \*、在「Select Users and Groups」(選取使用者和群組) 精靈上、將位置變更為本機電腦名稱 (階層架構中最上層)。
  - h. 新增 IIS AppPool \ SnapCenter 使用者、賦予完全控制權限。
3. 對於 \*CA 證書 IIS 權限\*，請從以下路徑在 SnapCenter 服務器中添加新的雙字節註冊表項：

在 Windows 登錄編輯器中、遍歷下列路徑：

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
```

4. 在 SChannel 登錄組態的內容下建立新的 DWORD 登錄機碼項目。

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

## 設定 SnapCenter Windows 外掛程式進行雙向 SSL 通訊

您應該使用 PowerShell 命令設定 SnapCenter Windows 外掛程式、以進行雙向 SSL 通訊。

開始之前

確保 CA 憑證指紋可用。

## 步驟

1. 若要連結連接埠、請在 SMCore 連接埠 8145 的 Windows 外掛主機上執行下列動作（預設）。

- a. 使用下列 PowerShell 命令移除現有的 SnapCenter 自我簽署憑證連接埠繫結。

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
```

例如、

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- b. 將新取得的 CA 憑證與 SMCore 連接埠繫結。

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert  
appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
```

例如、

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

## 啟用雙向 SSL 通訊

您可以啟用雙向 SSL 通訊、以使用 PowerShell 命令保護 SnapCenter 伺服器與外掛程式之間的相互通訊。

開始之前

先執行所有外掛程式和 SMCore 代理程式的命令、然後再執行伺服器的命令。

## 步驟

1. 若要啟用雙向 SSL 通訊、請在 SnapCenter 伺服器上針對外掛程式、伺服器以及需要雙向 SSL 通訊的每個代理程式執行下列命令。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName <Plugin_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. 使用下列命令執行 IIS SnapCenter 應用程式集區資源回收作業。 > Restart-WebAppPool -Name "SnapCenter"

3. 對於 Windows 外掛程式、請執行下列 PowerShell 命令、重新啟動 SMCore 服務：

```
> Restart-Service -Name SnapManagerCoreService
```

## 停用雙向 SSL 通訊

您可以使用 PowerShell 命令停用雙向 SSL 通訊。

關於此工作

- 先執行所有外掛程式和 SMCore 代理程式的命令、然後再執行伺服器的命令。
- 停用雙向 SSL 通訊時、CA 憑證及其組態不會移除。
- 若要將新主機新增至 SnapCenter 伺服器、您必須停用所有外掛主機的雙向 SSL。
- NLB 和 F5 不受支援。

步驟

1. 若要停用雙向 SSL 通訊、請在 SnapCenter 伺服器上針對所有外掛主機和 SnapCenter 主機執行下列命令。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName <Agent_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. 使用下列命令執行 IIS SnapCenter 應用程式集區資源回收作業。 > Restart-WebAppPool -Name "SnapCenter"

3. 對於 Windows 外掛程式、請執行下列 PowerShell 命令、重新啟動 SMCore 服務：

```
> Restart-Service -Name SnapManagerCoreService
```

## 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。