



安裝**SnapCenter** 適用於**Microsoft Windows**的功能性外掛程式

SnapCenter Software 4.7

NetApp
January 18, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/snapcenter-47/protect-scw/concept_install_snapcenter_plug_in_for_microsoft_windows.html on January 18, 2024. Always check docs.netapp.com for the latest.

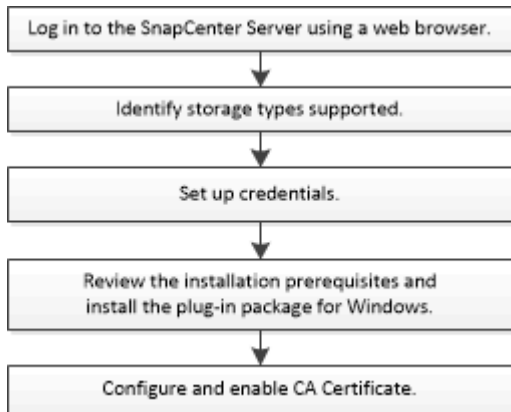
目錄

安裝SnapCenter 適用於Microsoft Windows的功能性外掛程式	1
適用於Microsoft Windows的安裝流程SnapCenter	1
適用於Microsoft Windows的安裝需求SnapCenter	1
在Windows Server 2012或更新版本上設定GMSA	5
新增主機並安裝SnapCenter 適用於Microsoft Windows的解決方案	6
使用PowerShell Cmdlet在SnapCenter 多個遠端主機上安裝適用於Microsoft Windows的支援功能外掛程式	9
從命令列以無訊息方式安裝SnapCenter 適用於Microsoft Windows的功能	10
監控SnapCenter 程式套件安裝狀態	11
設定CA憑證	12

安裝**SnapCenter** 適用於**Microsoft Windows**的功能性外掛程式

適用於**Microsoft Windows**的安裝流程**SnapCenter**

如果您想要保護非資料庫檔案的Windows檔案、則必須安裝並設定SnapCenter 適用於Microsoft Windows的還原外掛程式。



適用於**Microsoft Windows**的安裝需求**SnapCenter**


在安裝Windows外掛程式之前、您應該瞭解某些安裝需求。

開始使用Windows外掛程式之前SnapCenter、管理員必須先安裝及設定SnapCenter VMware Server、並執行必要的工作。

- 您必須擁有SnapCenter for Windows外掛程式的管理員權限才能安裝。
這個職務必須具有管理員權限。SnapCenter
- 您必須已安裝並設定SnapCenter 了此伺服器。
- 在Windows主機上安裝外掛程式時、如果您指定的認證不是內建的、或是使用者屬於本機工作群組使用者、則必須停用主機上的UAC。
- 如果您想要備份複寫、則必須設定SnapMirror和SnapVault SnapMirror。

安裝**SnapCenter** 適用於**Windows**的功能性外掛程式套件的主機需求

在安裝SnapCenter 適用於Windows的整套解決方案之前、您應該先熟悉一些基本的主機系統空間需求和規模調整需求。

項目	需求
作業系統	Microsoft Windows 如需支援版本的最新資訊、請參閱 "NetApp 互通性對照表工具" 。
主機上安裝的不需使用的RAM SnapCenter	1 GB
主機上安裝及記錄SnapCenter 插件的最低空間	5 GB <div>  <p>您應該配置足夠的磁碟空間、並監控logs資料夾的儲存使用量。所需的記錄空間會因受保護的實體數量和資料保護作業的頻率而有所不同。如果沒有足夠的磁碟空間、將不會針對最近執行的作業建立記錄。</p> </div>
必要的軟體套件	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.2或更新版本 • Windows管理架構（WMF4.0或更新版本） • PowerShell 4.0或更新版本 <p>如需支援版本的最新資訊、請參閱 "NetApp 互通性對照表工具"。</p> <p>如需 .NET 疑難排解資訊、請參閱 "對於沒有網際網路連線的舊版系統、SnapCenter 升級或安裝失敗"。</p>

設定適用於Windows的外掛程式認證

使用認證資料驗證使用者執行的不中斷作業。SnapCenter SnapCenter您應該建立認證、以安裝SnapCenter 更新程式、以及在Windows檔案系統上執行資料保護作業的其他認證資料。

您需要的是什麼

- 您必須先設定Windows認證、才能安裝外掛程式。
- 您必須在遠端主機上設定具有系統管理員權限（包括系統管理員權限）的認證。
- 如果您為個別資源群組設定認證、但使用者沒有完整的管理權限、則必須至少將資源群組和備份權限指派給使用者。

步驟

1. 在左側導覽窗格中、按一下*設定*。
2. 在「設定」頁面中、按一下「認證」。
3. 按一下「新增」。
4. 在「認證」頁面中、執行下列動作：

針對此欄位...	執行此動作...
認證名稱	輸入認證的名稱。
使用者名稱/密碼	<p>輸入用於驗證的使用者名稱和密碼。</p> <ul style="list-style-type: none"> 網域管理員或系統管理員群組的任何成員 <p>在您要安裝SnapCenter 此插件的系統上、指定網域管理員或任何系統管理員群組成員。「使用者名稱」欄位的有效格式如下：</p> <ul style="list-style-type: none"> ◦ NetBIOS\UserName ◦ Domain FQDN\UserName ◦ UserName@upn <ul style="list-style-type: none"> 本機管理員（僅適用於工作群組） <p>對於屬於工作群組的系統、請在安裝SnapCenter 此插件的系統上指定內建的本機管理員。如果使用使用者帳戶擁有較高的權限、或主機系統上的使用者存取控制功能已停用、您可以指定屬於本機系統管理員群組的本機使用者帳戶。「使用者名稱」欄位的有效格式如下：UserName</p> <p>請勿在密碼中使用雙引號 (") 或反引號 (`) 。請勿使用小於 (<) 和驚嘆號 (!) 密碼中的符號。例如、less-than<!10、less-than10<!、backtick'12。</p>
密碼	輸入用於驗證的密碼。

5. 按一下「確定」。

完成認證設定之後、您可能會想要在「使用者與存取」頁面上、將認證維護指派給使用者或使用者群組。

在Windows Server 2012或更新版本上設定GMSA

Windows Server 2012或更新版本可讓您建立群組託管服務帳戶（GMSA）、以便從託管網域帳戶提供自動化服務帳戶密碼管理。

您需要的是什麼

- 您應該擁有Windows Server 2012或更新版本的網域控制器。
- 您應該擁有Windows Server 2012或更新版本的主機、該主機是網域的成員。

步驟

1. 建立KDS根金鑰、為GMSA中的每個物件產生唯一的密碼。
2. 對於每個網域、請從Windows網域控制器執行下列命令：add-KDSRootKey -EffectiveImmedia
3. 建立及設定GMSA：
 - a. 以下列格式建立使用者群組帳戶：

```
domainName\accountName$
.. 新增電腦物件至群組。
.. 使用您剛建立的使用者群組來建立GMSA。
```

例如、

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. 執行 `Get-ADServiceAccount` 驗證服務帳戶的命令。
```

4. 在主機上設定GMSA：
 - a. 在您要使用GMSA帳戶的主機上啟用Windows PowerShell的Active Directory模組。

若要這麼做、請從PowerShell執行下列命令：

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 重新啟動主機。
- b. 從PowerShell命令提示字元執行下列命令、在主機上安裝GMSA： Install-AdServiceAccount <gMSA>

- c. 執行下列命令來驗證GMSA帳戶：`Test-AdServiceAccount <gmsa>`
5. 將管理權限指派給主機上已設定的GMSA。
6. 在SnapCenter 支援服務器中指定已設定的GMSA帳戶、以新增Windows主機。

在安裝外掛程式的過程中、將會在主機上安裝所選的外掛程式、並使用指定的GMSA作為服務登入帳戶。SnapCenter

在Windows Server 2012或更新版本上設定GMSA

Windows Server 2012或更新版本可讓您建立群組託管服務帳戶（GMSA）、以便從託管網域帳戶提供自動化服務帳戶密碼管理。

您需要的是什麼

- 您應該擁有Windows Server 2012或更新版本的網域控制器。
- 您應該擁有Windows Server 2012或更新版本的主機、該主機是網域的成員。

步驟

1. 建立KDS根金鑰、為GMSA中的每個物件產生唯一的密碼。
2. 對於每個網域、請從Windows網域控制器執行下列命令：`add-KDSRootKey -EffectiveImmedia`
3. 建立及設定GMSA：
 - a. 以下列格式建立使用者群組帳戶：

```
domainName\accountName$  
.. 新增電腦物件至群組。  
.. 使用您剛建立的使用者群組來建立GMSA。
```

例如、

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 執行 `Get-ADServiceAccount` 驗證服務帳戶的命令。
```

4. 在主機上設定GMSA：
 - a. 在您要使用GMSA帳戶的主機上啟用Windows PowerShell的Active Directory模組。

若要這麼做、請從PowerShell執行下列命令：

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 重新啟動主機。
 - b. 從PowerShell命令提示字元執行下列命令、在主機上安裝GMSA： `Install-AdServiceAccount <gMSA>`
 - c. 執行下列命令來驗證GMSA帳戶： `Test-AdServiceAccount <gMSA>`
5. 將管理權限指派給主機上已設定的GMSA。
6. 在SnapCenter 支援服務器中指定已設定的GMSA帳戶、以新增Windows主機。

在安裝外掛程式的過程中、將會在主機上安裝所選的外掛程式、並使用指定的GMSA作為服務登入帳戶。SnapCenter

新增主機並安裝SnapCenter 適用於Microsoft Windows的解決方案

您可以使用SnapCenter 「更新主機」 頁面來新增Windows主機。適用於Microsoft Windows的支援功能外掛程式會自動安裝在指定的主機上。SnapCenter這是安裝外掛程式的建議方法。您可以為個別主機或叢集新增主機並安裝外掛程式。

您需要的是什麼

- 您必須是指派給具有外掛安裝和解除安裝權限之角色的使用者、例如SnapCenter 「支援管理員」 角色。
- 在Windows主機上安裝外掛程式時、如果您指定的認證不是內建的、或是使用者屬於本機工作群組使用者、則必須停用主機上的UAC。
- 應將此使用者新增至Windows Server的「登入即服務」 角色。SnapCenter
- 您應確保訊息佇列服務處於執行中狀態。
- 如果您使用群組託管服務帳戶（GMSA）、則應該使用管理權限來設定GMSA。

關於此工作

- 您無法將SnapCenter 某個支援服務器作為外掛主機新增至另SnapCenter 一個支援服務器。
- Windows外掛程式
 - Microsoft Windows
 - Microsoft Exchange Server
 - Microsoft SQL Server
 - SAP HANA
 - 自訂外掛程式
- 在叢集上安裝外掛程式

如果您在叢集（WSFC、Oracle RAC或Exchange DAG）上安裝外掛程式、這些外掛程式會安裝在叢集的所有節點上。

- E系列儲存設備

您無法在連接至E系列儲存設備的Windows主機上安裝Windows外掛程式。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 確保在頂端選擇*託管主機*。
3. 按一下「* 新增 *」。
4. 在「hosts」頁面中、執行下列動作：


針對此欄位...	執行此動作...
主機類型	選擇* Windows *類型的主機。 如果主機尚未安裝Windows外掛程式、則支援使用者可新增主機、然後安裝該外掛程式。SnapCenter


針對此欄位...	執行此動作...
主機名稱	<p>輸入主機的完整網域名稱（FQDN）或IP位址。</p> <p>取決於DNS的正確組態。SnapCenter因此、最佳做法是輸入完整網域名稱（FQDN）。</p> <p>您可以輸入下列其中一項的IP位址或FQDN：</p> <ul style="list-style-type: none"> • 獨立式主機 • Windows伺服器容錯移轉叢集（WSFC） <p>如果您要使用SnapCenter 支援功能來新增主機、而且主機是子網域的一部分、則必須提供FQDN。</p>
認證資料	<p>選取您建立的認證名稱、或建立新認證資料。</p> <p>認證資料必須具有遠端主機的管理權限。如需詳細資訊、請參閱建立認證的相關資訊。</p> <p>如需認證的詳細資料、包括使用者名稱、網域和主機類型、請將游標放在您提供的認證名稱上方、即可顯示。</p> <div>  <p>驗證模式取決於您在「新增主機」精靈中指定的主機類型。</p> </div>

5. 在選取要安裝的外掛程式區段中、選取要安裝的外掛程式。

對於新部署、未列出外掛套件。

6. （可選）單擊*更多選項*。

針對此欄位...	執行此動作...
連接埠	<p>保留預設連接埠號碼或指定連接埠號碼。</p> <p>預設連接埠號碼為8145。如果SnapCenter 將該伺服器安裝在自訂連接埠上、該連接埠編號將會顯示為預設連接埠。</p> <div>  <p>如果您手動安裝外掛程式並指定自訂連接埠、則必須指定相同的連接埠。否則、作業將會失敗。</p> </div>

針對此欄位...	執行此動作...
安裝路徑	預設路徑為C:\Program Files\NetApp\SnapCenter。 您可以選擇性地自訂路徑。針對適用於Windows的「版本套件」、預設路徑為C:\Program Files\NetApp\SnapCenter。SnapCenter不過、如果需要、您可以自訂預設路徑。
新增叢集中的所有主機	選取此核取方塊可新增WSFC中的所有叢集節點。
跳過預先安裝檢查	如果您已手動安裝外掛程式、但不想驗證主機是否符合安裝外掛程式的需求、請選取此核取方塊。
使用群組託管服務帳戶（GMSA）來執行外掛程式服務	如果您要使用群組託管服務帳戶（GMSA）來執行外掛程式服務、請選取此核取方塊。 請以下列格式提供GMSA名稱： ：domainName\accountName\$。 <div>  <p>GMSA僅會做為SnapCenter Windows版的更新外掛程式服務的登入服務帳戶。</p> </div>

7. 按一下*提交*。

如果您尚未選取「跳過預先檢查」核取方塊、系統會驗證主機是否符合安裝外掛程式的需求。磁碟空間、RAM、PowerShell版本、.NET版本和位置均會根據最低需求進行驗證。如果不符合最低要求、則會顯示適當的錯誤或警告訊息。

如果錯誤與磁碟空間或RAM有關、您可以更新上的網路組態檔案 C:\Program Files\NetApp\SnapCenter Webapp以修改預設值。如果錯誤與其他參數有關、您必須修正問題。



在HA設定中、如果您要更新web.config檔案、則必須更新兩個節點上的檔案。

8. 監控安裝進度。

使用PowerShell Cmdlet在SnapCenter 多個遠端主機上安裝適用於Microsoft Windows的支援功能外掛程式

如果您想要同時在SnapCenter 多部主機上安裝適用於Microsoft Windows的效能測試外掛程式、您可以使用來執行此作業 Install-SmHostPackage PowerShell Cmdlet：

您必須以SnapCenter 網域使用者的身分登入到支援安裝外掛程式的每個主機、並擁有本機系統管理員權限。

步驟

1. 啟動PowerShell。

2. 在支援服務器主機上SnapCenter、使用建立工作階段 `Open-SmConnection Cmdlet`、然後輸入您的認證資料。
3. 使用將獨立主機或叢集新增SnapCenter 至 `Add-SmHost Cmdlet`和必要參數。

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](#)"。

4. 使用在多個主機上安裝外掛程式 `Install-SmHostPackage Cmdlet`和必要參數。

您可以使用 `-skipprecheck` 當您手動安裝外掛程式、但不想驗證主機是否符合安裝外掛程式的需求時、請選擇此選項。

從命令列以無訊息方式安裝SnapCenter 適用於Microsoft Windows的功能

如果無法從Windows GUI遠端安裝外掛程式、您可以SnapCenter 在Windows主機本機上安裝適用於Microsoft Windows的支援功能。SnapCenter您可以SnapCenter 從Windows命令列、以無訊息模式在無人值守的情況下執行Microsoft Windows安裝程式的功能。

您需要的是什麼

- 您必須安裝Microsoft Net 4.7.2或更新版本。
- 您必須安裝PowerShell 4.0或更新版本。
- 您必須開啟Windows訊息佇列。
- 您必須是主機上的本機管理員。

步驟

1. 從SnapCenter 您的安裝位置下載適用於Microsoft Windows的功能更新外掛程式。

例如、預設安裝路徑為C:\ProgramData\NetApp\SnapCenter\Package儲存庫。

此路徑可從SnapCenter 安裝了此伺服器的主機存取。

2. 將安裝檔案複製到您要安裝外掛程式的主機。
3. 在命令提示字元中、瀏覽至您下載安裝檔案的目錄。
4. 輸入下列命令、以資料取代變數：

```
"snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""  
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=  
ISFeatureInstall=SCW
```

例如：

```
`"C:\ProgramData\NetApp\SnapCenter\Package Repository
\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
\HPPW_SCW_Install.log" /log"C:\\" BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW`
```



安裝Windows外掛程式期間所傳遞的所有參數均區分大小寫。

輸入下列變數的值：

變動	價值
/debuglog"<debug_Log_Path>	指定套件安裝程式記錄檔的名稱和位置、如下列範例所示：setup.exe /debuglog" C : \PathToLog\setupexe.log"。
BI_SNAPCENTIER_port	指定SnapCenter 用來與SMCore進行通訊的連接埠。
套件_INSTALLDIR	指定主機外掛程式套件安裝目錄。
BI_ServiceAccount	指定SnapCenter Microsoft Windows Web服務帳戶的功能外掛程式。
BI_SERVERICEPWD	指定SnapCenter Microsoft Windows Web服務帳戶的密碼。
ISfeatureInstall	指定SnapCenter 要在遠端主機上部署的解決方案。

_debuglog_參數包括用於SnapCenter 資訊的記錄檔路徑。寫入此記錄檔是取得疑難排解資訊的慣用方法、因為檔案包含安裝針對外掛程式先決條件所執行的檢查結果。

如有必要、您可以在適用於SnapCenter Windows的資訊套件的記錄檔中找到其他疑難排解資訊。套件的記錄檔會列在_%Temp %資料夾中（最舊的優先）、例如_C:\臨時\。








安裝Windows外掛程式時、會在主機上登錄外掛程式、而非SnapCenter 在伺服器上登錄外掛程式。您可以SnapCenter 透過SnapCenter 使用支援程式介面或PowerShell Cmdlet新增主機、在支援服務器上登錄外掛程式。新增主機之後、即會自動探索外掛程式。

監控SnapCenter 程式套件安裝狀態

您SnapCenter 可以使用「工作」頁面來監控安裝過程。您可能需要檢查安裝進度、以判斷何時完成或是否有問題。

關於此工作

「工作」頁面上會出現下列圖示、並指出作業狀態：

-  進行中
-  已成功完成
-  失敗
-  已完成但有警告、或由於警告而無法啟動
-  已佇列

步驟

1. 在左導覽窗格中、按一下*監控*。
2. 在「監控」頁面中、按一下「工作」。
3. 在「工作」頁面中、若要篩選清單以便只列出外掛程式安裝作業、請執行下列步驟：
 - a. 按一下*篩選*。
 - b. 選用：指定開始和結束日期。
 - c. 從類型下拉式功能表中、選取*外掛程式安裝*。
 - d. 從「狀態」下拉式功能表中、選取安裝狀態。
 - e. 按一下「*套用*」。
4. 選取安裝工作、然後按一下*詳細資料*以檢視工作詳細資料。
5. 在「工作詳細資料」頁面中、按一下*檢視記錄*。

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。

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*。
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=0.0.0.0: <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=0.0.0.0:8145 certhash=$cert  
appid="$guid"
```

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。

您需要的是什麼

- 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 © 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。