準備安裝SnapCenter 「精選」外掛程式

SnapCenter Software 5.0

NetApp
April 04, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/snapcenter/protect-scc/task_install_snapcenter_custom_plug_in.html on April 04, 2024. Always check docs.netapp.com for the latest.

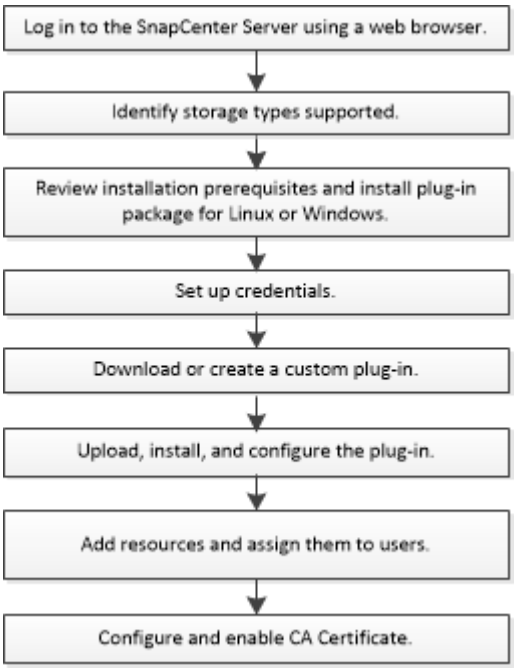
目錄

準備安裝SnapCenter 「精選」外掛程式 . . . 1
安裝流程：不需安裝程式SnapCenter . . . 1
新增主機和安裝SnapCenter 「更新自訂」外掛程式的先決條件 . . . 1
安裝SnapCenter 適用於Windows的功能性外掛程式套件的主機需求 . . . 3
安裝SnapCenter 適用於Linux的支援功能外掛套件的主機需求 . . . 4
設定SnapCenter 認證資料以供「不一樣的自訂外掛程式」使用 . . . 5
在Windows Server 2012或更新版本上設定GMSA . . . 7
安裝SnapCenter 「不一樣的自訂外掛程式」 . . . 8
設定CA憑證 . . . 14

準備安裝SnapCenter 「精選」外掛程式

安裝流程：不需安裝程式SnapCenter

如果您想要保護自訂外掛程式資源、請安裝並設定SnapCenter 「支援」功能。



"為應用程式開發外掛程式"

新增主機和安裝SnapCenter 「更新自訂」外掛程式的先決條件

在新增主機並安裝外掛程式套件之前、您必須先完成所有需求。自訂外掛程式可在Windows和Linux環境中使用。

- 您必須已建立自訂外掛程式。如需詳細資訊、請參閱開發人員資訊。

  "為應用程式開發外掛程式"

- 如果您想要管理MySQL或DB2應用程式、必須下載NetApp提供的MySQL和DB2自訂外掛程式。
- 您必須在Linux或Windows主機上安裝Java 1.8或Java 11（64位元）。
- 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.
- 自訂外掛程式必須在執行新增主機作業的用戶端主機上可用。

一般

如果您使用iSCSI、iSCSI服務應該會執行。

SHA512雜湊

- 對於NetApp提供的自訂外掛程式、您應該確定已將自訂外掛程式檔案的SHA512雜湊新增至_custom_plugin_checksum _list_檔案。

  - 對於Linux主機、SHA512雜湊位於_/var/opt/snapcenter/scc/cust_plugin_checksum *list.txt*
  - 對於Windows主機、SHA512雜湊位於_C:\Program Files\NetApp\SnapCenter Plug-in Creator\etc\custom_plugin_checksum *list.txt*

    對於自訂安裝路徑、SHA512雜湊位於_<CUSTOM路徑>\NetApp\SnapCenter\Snapcenter Plug-In Creator\etc\custom_plugin_checksum list.txt_

  custom_plugin_checksum清單是主機SnapCenter 上自訂外掛程式安裝的一部分、作者為

- 針對為應用程式建立的自訂外掛程式、您應該已執行下列步驟：

  a. 已產生外掛程式壓縮檔的SHA512雜湊。

     您可以使用像這樣的線上工具 "SHA512雜湊"。

  b. 將產生的SHA512雜湊新增至custom_plugin_checksum清單檔案的新行。

     註解以#符號開頭、以識別雜湊所屬的外掛程式。

     以下是Checksum檔案中SHA512雜湊項目的範例：

```
#ORASCPM
03721f567a1e4a1cb5569066b9a58af619ee12b1f8713108f81b696cfbdb81c25232fa63
d6e6777a2b2a1ec068bb0a93a59a8ade71587182f8bccbe81f7e0ba6
```

Windows主機

- 您必須擁有具有本機系統管理員權限的網域使用者、並在遠端主機上具有本機登入權限。
- 如果您管理SnapCenter 的是叢集節點、則必須有擁有叢集中所有節點管理權限的使用者。

Linux主機

- 您必須為root或非root使用者啟用密碼型SSH連線。
- 您必須在Linux主機上安裝Java 1.8或Java 11（64位元）。

  如果您將Windows Server 2019或Windows Server 2016用於SnapCenter 支援此功能的伺服器主機、則必須安裝Java 1.8或Java 11（64位元）。互通性對照表工具IMT （英文）包含有關需求的最新資訊。

  "適用於所有作業系統的Java下載"

  "NetApp 互通性對照表工具"

- 您必須為非root使用者設定Sudo權限、才能存取多個路徑。使用visudo Linux公用程式、將下列行新增

至/etc/udoers檔案。

請確定您使用的是Sudo 1.8.7版或更新版本。

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

_Linux使用者_是您所建立的非root使用者名稱。

您可以從* oracle_checksum・txt*檔案取得_checksum值_、該檔案位於_C：\ProgramData\NetApp\SnapCenter\Package_。

此範例只能做為建立自己資料的參考。

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

項目	需求
主機上安裝及記錄SnapCenter 插件的最低空間	5 GB 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。
必要的軟體套件	• 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 如需支援版本的最新資訊、請參閱 "NetApp 互通性對照表工具"。 如需 .NET 特定疑難排解資訊、請參閱 "無法升級或安裝不適用於沒有網際網路連線的舊系統。SnapCenter"

安裝SnapCenter 適用於Linux的支援功能外掛套件的主機需求

在安裝SnapCenter 適用於Linux的支援套件之前、您應確保主機符合要求。

項目	需求
作業系統	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server（SLES）
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	2 GB 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。

項目	需求
必要的軟體套件	Java 1.8 （64 位元） Oracle Java 或 OpenJDK 如果您已將Java升級至最新版本、則必須確定位於/var/opt/snapcenter/spl/etc/spl.properties的Java_home選項已設定為正確的Java版本和正確的路徑。

如需支援版本的最新資訊、請參閱 "NetApp 互通性對照表工具"

設定SnapCenter 認證資料以供「不一樣的自訂外掛程式」使用

使用認證資料驗證使用者執行的不中斷作業。SnapCenter SnapCenter您應該建立認證資料、以便在SnapCenter 資料庫或Windows檔案系統上安裝資訊更新外掛程式和執行資料保護作業的其他認證資料。

開始之前

- Linux主機

  您必須設定認證、才能在Linux主機上安裝外掛程式。

  您必須為root使用者或具有Sudo權限的非root使用者設定認證、才能安裝及啟動外掛程式程序。

  *最佳實務做法：*雖然您可以在部署主機和安裝外掛程式之後、為Linux建立認證、但最佳實務做法是在新增SVM之後、在部署主機和安裝外掛程式之前建立認證。

- Windows主機

  您必須先設定Windows認證、才能安裝外掛程式。

  您必須以系統管理員權限設定認證、包括遠端主機的系統管理員權限。

- 自訂外掛程式應用程式

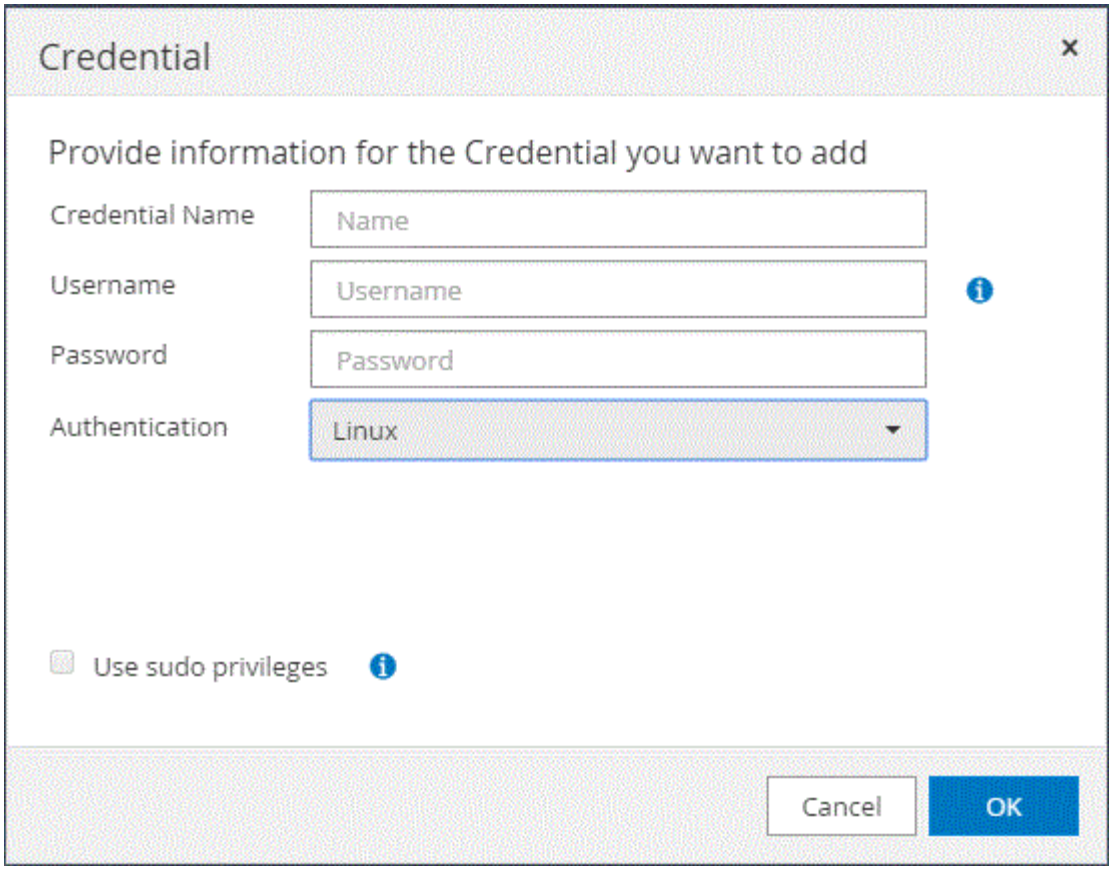
  外掛程式會使用新增資源時所選取或建立的認證資料。如果資源在資料保護作業期間不需要認證資料、您可以將認證資料設為*無*。

關於這項工作

如果您為個別資源群組設定認證、但使用者名稱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名稱。

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、指定設定認證所需的資訊：

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	輸入用於驗證的使用者名稱和密碼。 • 網域管理員或系統管理員群組的任何成員 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」欄位的有效格式為： ◦ *netbios*\使用者名稱 ◦ 網域FQDN \使用者名稱_ • 本機管理員（僅適用於工作群組） 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」欄位的有效格式為：*username*

針對此欄位...	執行此動作...
密碼	輸入用於驗證的密碼。
驗證模式	選取您要使用的驗證模式。
使用Sudo權限	如果您要為非root使用者建立認證、請選取「使用**Sudo**權限」核取方塊。 僅適用於Linux使用者。

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。

開始之前

- 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」命令來驗證服務帳戶。
```

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. 執行下列命令驗證您的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

安裝SnapCenter 「不一樣的自訂外掛程式」

新增主機並在遠端主機上安裝外掛程式套件

您必須使用SnapCenterAdd Host頁面來新增主機、然後安裝外掛程式套件。外掛程式會自動安裝在遠端主機上。您可以為個別主機或叢集新增主機並安裝外掛程式套件。

開始之前

- 您應該是指派給角色的使用者、該角色具有外掛程式安裝和解除安裝權限、例如SnapCenter 「支援管理員」角色。
- 您應確保訊息佇列服務正在執行中。
- 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。

"在Windows Server 2012或更新版本上為自訂應用程式設定群組託管服務帳戶"

關於這項工作

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。

如果您在叢集（WSFC）上安裝外掛程式、則外掛程式會安裝在叢集的所有節點上。

步驟

1. 在左側導覽窗格中、選取*主機*。
2. 驗證頂端是否已選取*託管主機*索引標籤。
3. 選取*「Add*」。
4. 在「hosts」（主機）頁面中、執行下列動作：

針對此欄位...	執行此動作...
主機類型	選取主機類型： • Windows • Linux 自訂外掛程式可在Windows和Linux環境中使用。
主機名稱	輸入主機的完整網域名稱（FQDN）或IP位址。 取決於DNS的正確組態。SnapCenter因此、最佳做法是輸入FQDN。 在Windows環境中、只有當不受信任的網域主機解析為FQDN時、才支援IP位址。 您可以輸入獨立主機的IP位址或FQDN。 如果您使用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。
認證資料	選取您建立的認證名稱、或建立新認證。 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。 您可以將游標放在指定的認證名稱上、以檢視認證資料的詳細資料。 認證驗證模式取決於您在「新增主機」精靈中指定的主機類型。

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。
6. （可選）選擇 * 更多選項 * 。

針對此欄位...	執行此動作...
連接埠	保留預設連接埠號碼、或指定連接埠號碼。 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。 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。

針對此欄位...	執行此動作...
安裝路徑	自訂外掛程式可安裝在Windows系統或Linux系統上。 • 針對適用於Windows的「更新程式套件」、預設路徑為C:\Program Files\NetApp\SnapCenter。SnapCenter 您也可以自訂路徑。 • 對於 SnapCenter Plug-in 套件 for Linux 、預設路徑為 `/opt/NetApp/snapcenter`。 您也可以自訂路徑。 • 針對「不需要自訂的外掛程式」SnapCenter ： i. 在「自訂外掛程式」區段中、選取 * 瀏覽 * 、然後選取壓縮的自訂外掛程式資料夾。 壓縮資料夾包含自訂外掛程式碼和描述元.xml檔案。 若為儲存外掛程式、請瀏覽至 *C:\ProgramData\NetApp\SnapCenter\Package Repository* 然後選擇 `Storage.zip` 資料夾。 ii. 選取 * 上傳 * 。 壓縮自訂外掛程式資料夾中的描述元.xml檔案會在上傳套件之前驗證。 會列出上傳至SnapCenter Sfor the Sfor the Sfor the Server的自訂外掛程式。 如果您想要管理MySQL或DB2應用程式、可以使用NetApp提供的MySQL和DB2自訂外掛程式。MySQL和DB2自訂外掛程式可從取得 "NetApp Automation Store"
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。

針對此欄位...	執行此動作...
使用群組託管服務帳戶（GMSA）來執行外掛程式服務	如果您想要使用群組託管服務帳戶（GMSA）來執行外掛程式服務、請針對Windows主機選取此核取方塊。 請以下列格式提供GMSA名稱：domainname\accountName$。 GMSA僅會做為SnapCenter Windows版的更新外掛程式服務的登入服務帳戶。

7. 選擇*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、位置（適用於Windows外掛程式）和Java版本（適用於Linux外掛程式）均已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、您可以更新位於C:\Program Files\NetApp\SnapCenter Webapp的Web.config檔案、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. 如果主機類型為 Linux 、請驗證指紋、然後選取 * 確認並提交 * 。

   即使先前已將同一部主機新增至SnapCenter 更新版本、而且指紋已確認、指紋驗證也是必要的。

9. 監控安裝進度。

   安裝特定的記錄檔位於 `/custom_location/snapcenter/` 記錄。

使用**Cmdlet**在**SnapCenter** 多個遠端主機上安裝適用於**Linux**或**Windows**的支援功能外掛套件

您SnapCenter 可以使用Install-SmHostPackage PowerShell Cmdlet、同時在多個主機上安裝適用於Linux或Windows的VMware®更新套件。

開始之前

新增主機的使用者應擁有主機的管理權限。

步驟

1. 啟動PowerShell。
2. 在支援服務器主機上SnapCenter 、使用Open-SmConnection Cmdlet建立工作階段、然後輸入您的認證資料。
3. 使用Install-SmHostPackage Cmdlet和必要參數、在多個主機上安裝外掛程式。

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"。

您可以在手動安裝外掛程式時使用-skipprecheck選項、而且不想驗證主機是否符合安裝外掛程式的需求。

4. 輸入遠端安裝的認證資料。

使用命令列介面、在**SnapCenter Linux**主機上安裝《程式集指令集自訂外掛程式」

您應該SnapCenter 使用SnapCenter 「版本資訊」使用者介面（UI）來安裝「版本資訊」自訂外掛程式。如果您的環境不允許從SnapCenter SIUI遠端安裝外掛程式、您可以使用命令列介面（CLI）、在主控台模式或無聲模式下安裝自訂外掛程式。

步驟

1. 將SnapCenter 適用於Linux的支援功能套件安裝檔案（snapcenter_Linux _host_plugin.bin）從C：\ProgramData \NetApp\SnapCenter\Package儲存庫複製到您要安裝自訂外掛程式的主機。

   您可以從SnapCenter 安裝了該伺服器的主機存取此路徑。

2. 在命令提示字元中、瀏覽至您複製安裝檔案的目錄。
3. 安裝外掛程式：「path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -dserver_ip=server_name_or ip_address -dserver_https_port=port_number_for_server'

   - -DPORT指定SMCore HTTPS通訊連接埠。
   - -dserver_IP會指定SnapCenter 「伺服器IP位址」。
   - -dserver_https_port指定SnapCenter 了「伺服器HTTPS連接埠」。
   - -Duser_install_DIR會指定您要安裝SnapCenter 適用於Linux的《SKED Plug-ins套件》的目錄。
   - DINSTALL_LOD_NAME指定記錄檔的名稱。

   ```
   /tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
   -DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
   -DUSER_INSTALL_DIR=/opt
   -DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
   -DCHOSEN_FEATURE_LIST=CUSTOM
   ```

4. 使用Add-Smhost Cmdlet和必要參數、將主機新增SnapCenter 至SetcServer。

   執行_Get-Help命令名稱_可取得有關可與命令搭配使用之參數及其說明的資訊。或者、您也可以參閱 "《軟件指令程式參考指南》SnapCenter"。

5. 登入SnapCenter 以供使用者介面或PowerShell Cmdlet上傳自訂外掛程式。

   您可以參考、從UI上傳自訂外掛程式 "新增主機並在遠端主機上安裝外掛程式套件" 區段。

   Cmdlet說明及Cmdlet參考資訊包含更多PowerShell Cmdlet的相關資訊。SnapCenter

"《軟件指令程式參考指南》SnapCenter"。

監控安裝自訂外掛程式的狀態

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。

關於這項工作

「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 **Jobs** 頁面中、若要篩選清單以僅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。

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*。
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"
```

在SnapCenter Linux主機上設定「CA憑證」以使用「支援整套自訂外掛程式」服務

您應該管理自訂外掛程式Keystore的密碼及其憑證、設定CA憑證、設定根或中繼憑證至自訂外掛程式信任存放區、以及設定CA簽署金鑰配對至自訂外掛程式信任存放區、並使用SnapCenter 「依賴自訂外掛程式」服務啟動已安裝的數位憑證。

自訂外掛程式會使用位於_/opt /NetApp/snapcenter/sccc/etc_的「keystore .jks」檔案做為其信任存放區和金鑰存放區。

管理自訂外掛程式**Keystore**的密碼、以及使用中的**CA**簽署金鑰配對別名

步驟

1. 您可以從自訂外掛程式代理程式內容檔擷取自訂外掛程式Keystore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。

自訂外掛程式Keystore的密碼、以及私密金鑰的所有相關別名密碼均應相同。

將根或中繼憑證設定為自訂外掛程式信任存放區

您應該設定根或中繼憑證、而不使用私密金鑰、以自訂外掛程式信任存放區。

步驟

1. 瀏覽至包含自訂外掛程式Keystore的資料夾：/opp/NetApp/snapcenter/scc/等
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
. 將根或中繼憑證設定為自訂外掛程式信任存放區之後、請重新啟動服務。
```

您應該先新增根CA憑證、然後再新增中繼CA憑證。

將**CA**簽署金鑰配對設定為自訂外掛程式信任存放區

您應該將CA簽署金鑰配對設定為自訂外掛程式信任存放區。

步驟

1. 瀏覽至包含自訂外掛程式Keystore /opp/NetApp/snapcenter/scc/等的資料夾
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。

   預設的自訂外掛程式Keystore密碼是agent.properties檔案中KeyKeyKeystore _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. 將CA簽署金鑰配對設定為自訂外掛程式信任存放區之後、請重新啟動服務。

針對**SnapCenter** 「不一樣的自訂外掛程式」設定憑證撤銷清單（**CRL**）

關於這項工作

- 「自訂外掛程式」會在預先設定的目錄中搜尋CRL檔案。SnapCenter
- 適用於「SetcCustom Plug-in」的CRL檔案預設目錄SnapCenter 為「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。

在**SnapCenter Windows**主機上設定「**CA**憑證」以使用「更新自訂外掛程式」服務

您應該管理自訂外掛程式Keystore的密碼及其憑證、設定CA憑證、設定根或中繼憑證至自訂外掛程式信任存放區、以及設定CA簽署金鑰配對至自訂外掛程式信任存放區、並使用SnapCenter 「依賴自訂外掛程式」服務啟動已安裝的數位憑證。

自訂外掛程式使用檔案_keyKeystore。jks_、位於_C：\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_、兩者都是其信任存放區和金鑰存放區。

管理自訂外掛程式**Keystore**的密碼、以及使用中的**CA**簽署金鑰配對別名

步驟

1. 您可以從自訂外掛程式代理程式內容檔擷取自訂外掛程式Keystore預設密碼。

   它是對應於key_keystore _pass的值。

2. 變更Keystore密碼：

   keytool-storepasswd -keystore keystor.jks

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

   C：\Program Files\Java\<JDK_VERY>\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。

   自訂外掛程式Keystore的密碼、以及私密金鑰的所有相關別名密碼均應相同。

將根或中繼憑證設定為自訂外掛程式信任存放區

您應該設定根或中繼憑證、而不使用私密金鑰、以自訂外掛程式信任存放區。

步驟

1. 瀏覽至包含自訂外掛程式Keystore _C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\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 keyKeystore .jks

4. 新增根或中繼憑證：

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

5. 將根或中繼憑證設定為自訂外掛程式信任存放區之後、請重新啟動服務。

   您應該先新增根CA憑證、然後再新增中繼CA憑證。

將**CA**簽署金鑰配對設定為自訂外掛程式信任存放區

您應該將CA簽署金鑰配對設定為自訂外掛程式信任存放區。

步驟

1. 瀏覽至包含自訂外掛程式Keystore _C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc_ 的資料夾
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。

   預設的自訂外掛程式Keystore密碼是agent.properties檔案中KeyKeyKeystore _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. 將CA簽署金鑰配對設定為自訂外掛程式信任存放區之後、請重新啟動服務。

針對**SnapCenter** 「不一樣的自訂外掛程式」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"。
- 「自訂外掛程式」會在預先設定的目錄中搜尋CRL檔案。SnapCenter
- 適用於「不適用自訂外掛程式」的CRL檔案預設目錄SnapCenter 為：*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 伺服器和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 © 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。