



準備安裝適用於 **MySQL** 的**SnapCenter**插件 SnapCenter software

NetApp
November 06, 2025

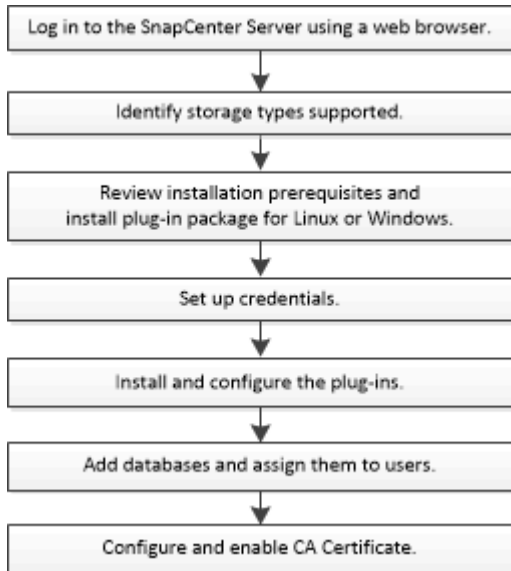
目錄

準備安裝適用於 MySQL 的SnapCenter插件	1
SnapCenter Plug-in for MySQL 的安裝工作流程	1
新增主機並安裝 MySQL 的SnapCenter插件的先決條件	1
Windows 主機	1
Linux 主機	2
補充命令	2
為 Linux 主機的非 root 使用者配置 sudo 權限	3
安裝適用於 Windows 的SnapCenter插件包的主機需求	4
安裝適用於 Linux 的SnapCenter插件包的主機需求	5
為 MySQL 的SnapCenter插件設定憑證	6
安裝適用於 MySQL 的SnapCenter插件	8
新增主機並在遠端主機上安裝插件包	8
使用 cmdlet 在多個遠端主機上安裝適用於 Linux 或 Windows 的SnapCenter插件包	10
使用命令列介面在 Linux 主機上安裝適用於 MySQL 的SnapCenter插件	10
監控 MySQL 外掛程式安裝狀態	11
設定 CA 憑證	12
產生CA憑證CSR文件	12
匯入 CA 憑證	13
取得 CA 憑證指紋	13
使用 Windows 主機插件服務設定 CA 憑證	14
為 Linux 主機上的SnapCenter MySQL 插件服務設定 CA 憑證	14
為 Windows 主機上的SnapCenter MySQL 插件服務設定 CA 證書	17
為插件啟用 CA 憑證	19

準備安裝適用於 MySQL 的 SnapCenter 插件

SnapCenter Plug-in for MySQL 的安裝工作流程

如果您想要保護 MySQL 資料庫，則應該安裝並設定適用於 MySQL 的 SnapCenter 插件。



新增主機並安裝 MySQL 的 SnapCenter 插件的先決條件

在新增主機和安裝插件包之前，您必須完成所有要求。 SnapCenter Plug-in for MySQL 可在 Windows 和 Linux 環境中使用。

- 您必須在主機上安裝 Java 11。



IBM Java 在 Windows 和 Linux 主機上不受支援。

- 對於 Windows，外掛程式建立服務應該使用「LocalSystem」Windows 使用者執行，這是以網域管理員身分安裝 MySQL 外掛程式時的預設行為。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。適用於 Microsoft Windows 的 SnapCenter 外掛程式將預設與 Windows 主機上的 MySQL 外掛程式一起部署。
- SnapCenter 伺服器應該可以存取 MySQL 主機插件的 8145 或自訂連接埠。
- 對於 MySQL 5.7，應該在 mysql 配置（my.cnf 或 mysql-server.cnf）檔案中指定 binlog。

Windows 主機

- 您必須擁有具有本機管理員權限的網域用戶，並在遠端主機上擁有本機登入權限。
- 在 Windows 主機上安裝適用於 MySQL 的外掛程式時，適用於 Microsoft Windows 的 SnapCenter 外掛程式會自動安裝。
- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。

- 您必須在 Windows 主機上安裝 Java 11。

"下載適用於所有作業系統的 JAVA"

"NetApp互通性表工具"

Linux 主機

- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。
- 您必須在 Linux 主機上安裝 Java 11。

"下載適用於所有作業系統的 JAVA"

"NetApp互通性表工具"

- 對於在 Linux 主機上執行的 MySQL 資料庫，安裝 MySQL 插件時，會自動安裝 UNIX 的 SnapCenter 插件。
- 您應該將 **bash** 作為插件安裝的預設 shell。

補充命令

要在 MySQL 的 SnapCenter 插件上執行補充命令，必須將其包含在 *allowed_commands.config* 檔案中。

- Windows 主機上的預設位置：*C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Linux 主機上的預設位置：*/opt/ NetApp/ snapcenter/ scc/ etc/ allowed_commands.config*

若要允許插件主機上的補充命令，請在編輯器中開啟 *_allowed_commands.config* 檔案。每個命令在單獨的行上輸入，並且命令不區分大小寫。確保指定完全限定的路徑名，並且如果路徑名包含空格，則將其括在引號 (") 中。

例如：

指令：mount 指令：umount 指令：「C:\Program Files\ NetApp\ SnapCreator commands\sdcli.exe」 指令：
：myscript.bat

如果不存在 *allowed_commands.config* 文件，命令或腳本執行將被阻止，並且工作流程將失敗並出現以下錯誤：

不允許執行「[/mnt/mount -a]。透過在插件主機上的檔案 %s 中新增命令來授權。」

如果命令或腳本不在 *_allowed_commands.config* 中，則命令或腳本的執行將被阻止，並且工作流程將失敗並出現以下錯誤：

不允許執行「[/mnt/mount -a]。透過在插件主機上的檔案 %s 中新增命令來授權。」



您不應使用通配符 (*) 來允許所有命令。

為 Linux 主機的非 root 使用者配置 sudo 權限

SnapCenter允許非 root 使用者安裝適用於 Linux 的SnapCenter插件包並啟動插件進程。插件進程將以有效的非 root 使用者身分運行。您應該為非 root 使用者配置 sudo 權限以提供對多個路徑的存取。

您需要什麼

- Sudo 版本 1.8.7 或更高版本。
- 如果 umask 為 0027，請確保 java 資料夾及其內部的所有檔案的權限為 555。否則插件安裝可能會失敗。
- 對於非root用戶，請確保非root用戶的名稱和用戶所在群組的名稱相同。
- 編輯 `/etc/ssh/sshd_config` 文件，設定訊息認證碼演算法：MACs hmac-sha2-256、MACs hmac-sha2-512。

更新設定檔後重新啟動sshd服務。

範例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

關於此任務

您應該為非 root 使用者配置 sudo 權限以提供對以下路徑的存取權限：

- `/home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/ NetApp/snapcenter/spl/安裝/插件/卸載`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

步驟

1. 登入要安裝適用於 Linux 的SnapCenter插件套件的 Linux 主機。
2. 使用 visudo Linux 實用程式將以下行新增至 `/etc/sudoers` 檔案。

```

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_Precchecks.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 SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



如果您有 RAC 設置，以及其他允許的命令，您應該將以下內容添加到 `/etc/sudoers` 檔案：
`:/<crs_home>/bin/olsnodes`

您可以從 `/etc/oracle/olr.loc` 檔中取得 `_crs_home` 的值。

`LINUX_USER` 是您建立的非 root 使用者的名稱。

您可以從 `sc_unix_plugins_checksum.txt` 檔案中取得 `checksum_value`，該檔案位於：

- `_C:\ProgramData\NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` _ 如果 SnapCenter Server 安裝在 Windows 主機上。
- `_/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` _ 如果 SnapCenter Server 安裝在 Linux 主機上。



此範例僅應作為建立您自己的資料的參考。

安裝適用於 Windows 的 SnapCenter 插件包的主機需求

在安裝適用於 Windows 的 SnapCenter 插件包之前，您應該熟悉一些基本的主機系統空間需求和大小需求。

物品	要求
作業系統	微軟 Windows 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	5GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 核心 7.4.2 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 有關 .NET 特定的故障排除信息，請參閱 "對於沒有網路連線的傳統系統，SnapCenter升級或安裝將會失敗。"

安裝適用於 Linux 的SnapCenter插件包的主機需求

在安裝適用於 Linux 的SnapCenter插件包之前，您應該熟悉一些基本的主機系統空間和大小需求。

物品	要求
作業系統	• 紅帽企業 Linux • SUSE Linux 企業伺服器 (SLES) 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。
主機上SnapCenter插件的最小 RAM	1GB

物品	要求
主機上SnapCenter插件的最小安裝和日誌空間	2GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間有所不同，取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	Java 11 Oracle Java 與 OpenJDK 如果您已將 JAVA 升級至最新版本，則必須確保位於 <code>/var/opt/snapcenter/spl/etc/spl.properties</code> 的 <code>JAVA_HOME</code> 選項設定為正確的 JAVA 版本和正確的路徑。 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。

為 MySQL 的SnapCenter插件設定憑證

SnapCenter使用憑證對SnapCenter操作的使用者進行身份驗證。您應該建立用於安裝SnapCenter插件的憑證以及用於在資料庫或 Windows 檔案系統上執行資料保護作業的附加憑證。

關於此任務

- Linux 主機

您必須設定在 Linux 主機上安裝插件的憑證。

您必須為 root 使用者或具有 sudo 權限的非 root 使用者設定憑證才能安裝和啟動插件進程。

最佳實務：雖然您可以在部署主機和安裝外掛程式後為 Linux 建立憑證，但最佳實務是在新增 SVM 之後、部署主機和安裝外掛程式之前建立憑證。

- Windows 主機

在安裝插件之前，您必須設定 Windows 憑證。

您必須設定具有管理員權限的憑證，包括遠端主機上的管理員權限。

如果您為單一資源群組設定憑證，且使用者名稱沒有完全管理權限，則必須至少為該使用者名稱指派資源群組和備份權限。

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「憑證」。
3. 點選“新建”。
4. 在「憑證」頁面中，指定配置憑證所需的資訊：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。
使用者名稱	輸入用於身份驗證的使用者名稱和密碼。 • 網域管理員或管理員群組的任何成員 指定要安裝SnapCenter插件的系統上的網域管理員或管理員群組的任何成員。用戶名字段的有效格式為： ◦ <i>NetBIOS</i>\使用者名稱 ◦ 域 <i>FQDN</i>\用戶名 • 本機管理員（僅適用於工作群組） 對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。使用者名字段的有效格式為：<i>UserName</i> 請勿在密碼中使用雙引號 (") 或反引號 (')。密碼中不應同時使用小於號 (<) 和驚嘆號 (!) 符號。例如，less<than<!10、less<than10<!、backtick`12。
密碼	輸入用於身份驗證的密碼。
認證模式	選擇您想要使用的身份驗證模式。
使用 sudo 權限	如果您要為非 root 使用者建立憑證，請勾選「使用 sudo 權限」複選框。  僅適用於 Linux 使用者。

5. 按一下“確定”。

完成憑證設定後，您可能想要在「使用者和造訪」頁面中將憑證維護指派給使用者或使用者群組。

安裝適用於 MySQL 的SnapCenter插件

新增主機並在遠端主機上安裝插件包

您必須使用SnapCenter新增主機頁面來新增主機，然後安裝插件包。插件會自動安裝在遠端主機上。您可以新增主機並為單一主機安裝插件包。

開始之前

- 如果SnapCenter Server 主機的作業系統是 Windows 2019，而插件主機的作業系統是 Windows 2022，則應執行下列操作：
 - 升級到 Windows Server 2019（作業系統內部版本 17763.5936）或更高版本
 - 升級到 Windows Server 2022（作業系統內部版本 20348.2402）或更高版本
- 您必須是分配有插件安裝和卸載權限的角色的用戶，例如SnapCenter管理員角色。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證，或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 您應該確保訊息佇列服務正在運行。
- 管理文件包含有關管理主機的資訊。

關於此任務

- 您不能將SnapCenter伺服器作為插件主機新增至另一個SnapCenter伺服器。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 驗證頂部的「託管主機」標籤是否已選取。
3. 按一下“新增”。
4. 在「主機」頁面中，執行下列操作：

對於這個領域...	這樣做...
主機類型	選擇主機類型： • 視窗 • Linux  必須在 MySQL 資料庫伺服器上安裝 MySQL 插件。
主機名稱	輸入通訊主機名稱。輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。SnapCenter依賴 DNS 的正確配置。因此，最佳做法是輸入 FQDN。

對於這個領域...	這樣做...
證書	選擇您建立的憑證名稱或建立新的憑證。該憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 您可以將遊標放在您提供的憑證名稱上來查看有關憑證的詳細資訊。  憑證驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在選擇要安裝的插件部分中，選擇要安裝的插件。

使用 REST API 安裝 MySQL 外掛程式時，必須傳遞版本為 3.0。例如，MySQL:3.0

6. （可選）按一下“更多選項”。

對於這個領域...	這樣做...
港口	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 伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。
安裝路徑	MySQL 插件安裝在 MySQL 客戶端主機上，該主機可以是 Windows 系統，也可以是 Linux 系統。 - 對於適用於 Windows 的 SnapCenter 插件包，預設路徑為 C:\Program Files\ NetApp\ SnapCenter。您也可以選擇自訂路徑。 - 對於適用於 Linux 的 SnapCenter 插件包，預設路徑為 /opt/ NetApp/snapcenter。您也可以選擇自訂路徑。
跳過預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。
新增叢集中的所有主機	不適用。
使用群組託管服務帳戶 (gMSA) 執行外掛程式服務	不適用。

7. 點選“提交”。

如果您未選取「跳過預先檢查」複選框，則會驗證主機是否符合安裝插件的要求。系統會根據最低要求驗證

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）。如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

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，則必須修復該問題。



在 HA 設定中，如果您要更新 `web.config` 文件，則必須在兩個節點上更新該文件。

8. 如果主機類型為Linux，請驗證指紋，然後按一下*確認並提交*。

在叢集設定中，您應該驗證叢集中每個節點的指紋。



即使之前已將同一台主機新增至SnapCenter並且已確認指紋，也必須進行指紋驗證。

9. 監控安裝進度。

- 對於 Windows 插件，安裝和升級日誌位於：`C:\Windows\ SnapCenter plugin\Install<JOBID>\_`
- 對於 Linux 插件，安裝日誌位於：`/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plugin_Install<JOBID>.log_`，升級日誌位於：`_var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-JOB_grade_f.`

完成後

如果要升級到SnapCenter 6.0 版本，則會從遠端插件伺服器中解除安裝現有的基於 PERL 的 MySQL 插件。

使用 **cmdlet** 在多個遠端主機上安裝適用於 **Linux** 或 **Windows** 的**SnapCenter**插件包

您可以使用 `Install-SmHostPackage PowerShell cmdlet` 同時在多個主機上安裝適用於 Linux 或 Windows 的SnapCenter插件套件。

開始之前

您必須以網域使用者身分登入SnapCenter，並在要安裝插件包的每個主機上擁有本機管理員權限。

步驟

1. 啟動 PowerShell。
2. 在SnapCenter Server 主機上，使用 `Open-SmConnection cmdlet` 建立會話，然後輸入您的憑證。
3. 使用 `Install-SmHostPackage cmdlet` 和所需參數在多個主機上安裝插件。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 `cmdlet` 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體 Cmdlet 參考指南](#)"。

當您手動安裝了插件並且不想驗證主機是否符合安裝插件的要求時，可以使用 `-skipcheck` 選項。

4. 輸入您的遠端安裝憑證。

使用命令列介面在 **Linux** 主機上安裝適用於 **MySQL** 的**SnapCenter**插件

您應該使用SnapCenter使用者介面 (UI) 安裝適用於 MySQL 資料庫的SnapCenter插件。如果您的環境不允許從SnapCenter UI 遠端安裝插件，您可以使用命令列介面 (CLI) 以控

制台模式或靜默模式安裝 MySQL 資料庫插件。

開始之前

- 您應該在每個必須保護 MySQL 執行個體的 Linux 主機上安裝 MySQL 資料庫外掛程式。
- 安裝 MySQL 資料庫的SnapCenter插件的 Linux 主機必須符合相關軟體、資料庫和作業系統要求。

互通性矩陣工具 (IMT) 包含受支援配置的最新資訊。

"NetApp互通性表工具"

- 適用於 MySQL 資料庫的SnapCenter插件是適用於 Linux 的SnapCenter插件包的一部分。在安裝適用於 Linux 的SnapCenter插件包之前，您應該已經在 Windows 主機上安裝了SnapCenter。

步驟

1. 將 Linux 安裝檔案 (snapcenter_linux_host_plugin.bin) 的SnapCenter插件包從 C:\ProgramData\ NetApp\ SnapCenter\Package Repository 複製到要安裝 MySQL 插件的主機。

您可以從安裝了SnapCenter伺服器的主機存取此路徑。

2. 從命令提示字元處，導覽至複製安裝檔案的目錄。
3. 安裝插件：`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 指定SnapCenter伺服器 IP 位址。
- -DSERVER_HTTPS_PORT 指定SnapCenter伺服器 HTTPS 連接埠。
- -DUSER_INSTALL_DIR 指定要安裝 Linux 版SnapCenter插件包的目錄。
- DINSTALL_LOG_NAME 指定日誌檔案的名稱。

```
/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. 編輯 /<安裝目錄> NetApp文件，然後新增 PLUGINS_ENABLED = MySQL:3.0 參數。
5. 使用 Add-Smhost cmdlet 和所需參數將主機新增至SnapCenter伺服器。

可以透過執行 `_Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體 Cmdlet 參考指南](#)"。

監控 MySQL 外掛程式安裝狀態

您可以使用「作業」頁面監控SnapCenter插件包的安裝進度。您可能需要檢查安裝進度以

確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
 - a. 按一下“過濾器”。
 - b. 可選：指定開始日期和結束日期。
 - c. 從類型下拉式選單中，選擇*插件安裝*。
 - d. 從狀態下拉式選單中，選擇安裝狀態。
 - e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

設定 CA 憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 ["如何產生CA憑證CSR文件"](#)。



如果您擁有您的網域 (*.domain.company.com) 或您的系統 (machine1.domain.company.com) 的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用SnapCenter部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過

填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證 (*.domain.company.com)，該憑證將隱式包含網域的所有主機名稱。

匯入 CA 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入 SnapCenter 伺服器 和 Windows 主機外掛程式。

步驟

- 1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
- 2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
- 3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
- 4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
- 5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
- 6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。



匯入憑證時需攜帶私鑰（支援格式為：.pfx、.p12、*.p7b）。

- 7. 對「個人」資料夾重複步驟 5。

取得 CA 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

- 1. 在 GUI 上執行以下操作：
 - a. 雙擊該證書。
 - b. 在「證書」對話方塊中，按一下「詳細資料」標籤。
 - c. 捲動瀏覽欄位清單並按一下「指紋」。
 - d. 從框複製十六進位字元。
 - e. 刪除十六進制數之間的空格。

例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e6f83886b00d4277a32a7b”。

2. 從 PowerShell 執行以下操作：

- a. 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。

```
Get-Childitem -Path 憑證:\LocalMachine\My
```

- b. 複製指紋。

使用 Windows 主機插件服務設定 CA 憑證

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

在SnapCenter伺服器 and 所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

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

例如：

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

- ． 透過執行下列命令將新安裝的憑證與 Windows 主機插件服務綁定：

```
> $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SnapCenter MySQL 插件服務設定 CA 憑證

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用SnapCenter插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

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。

它是與密鑰“KEYSTORE_PASS”對應的值。

2. 更改密鑰庫密碼：

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

． 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：

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

對 *agent.properties* 檔案中的金鑰 KEYSTORE_PASS 進行相同的更新。

3. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關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. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

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

4. 新增根證書或中間證書：

```
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。



您應該新增根 CA 證書，然後新增中間 CA 證書。

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。

步驟

1. 導航至包含插件金鑰庫 `/opt/ NetApp/snapcenter/scc/etc` 的資料夾。
2. 找到檔案“`keystore.jks`”。
3. 列出密鑰庫中新增的憑證：

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

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增的憑證。

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

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore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憑證中的別名較長，且包含空格或特殊字元（“*”、“\”，“”），請將別名修改為簡單名稱：

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

• 在 `agent.properties` 檔案中配置來自 CA 憑證的別名。

根據鍵 `SCC_CERTIFICATE_ALIAS` 更新此值。

8. 配置 CA 簽署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)

關於此任務

- 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. 您可以根據鍵 CRL_PATH 修改和更新 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。將根據每個 CRL 驗證傳入的憑證。

為 Windows 主機上的 SnapCenter MySQL 插件服務設定 CA 證書

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用 SnapCenter 插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

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。

它是與金鑰_KEYSTORE_PASS_對應的值。

2. 更改密鑰庫密碼：

`keytool -storepasswd -keystore 金鑰庫.jks`



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

`C:\Program Files\Java\<jdk_version>\bin\keytool.exe -storepasswd -keystore keystore.jks`

3. 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：

`keytool -keypasswd -alias 「別名在憑證中」 -keystore keystore.jks`

對 agent.properties 檔案中的金鑰 KEYSTORE_PASS 進行相同的更新。

4. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關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. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

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

4. 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.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。



您應該新增根 CA 證書，然後新增中間 CA 證書。

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。

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. 列出密鑰庫中新增的憑證：

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

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增的憑證。

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

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore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 「別名在CA憑證中的名稱」 -keystore keystore.jks
```

8. 在 `_agent.properties_` 檔案中配置來自CA憑證的別名。

根據鍵 `SCC_CERTIFICATE_ALIAS` 更新此值。

9. 配置 CA 簽署金鑰對以插入信任庫後重新啟動服務。

為SnapCenter插件配置憑證撤銷清單 (CRL)

關於此任務

- 若要下載相關 CA 憑證的最新 CRL 文件，請參閱 ["如何更新SnapCenter CA 憑證中的憑證撤銷清單文件"](#)。
- SnapCenter插件將在預先配置的目錄中搜尋 CRL 檔案。

- SnapCenterSnapCenter的 CRL 檔案的預設目錄是 'C:\Program Files\ NetApp \ SnapCenter \Snapcenter Plug-in Creator\ etc\crl' 。

步驟

1. 您可以根據鍵 CRL_PATH 修改和更新 *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。

將根據每個 CRL 驗證傳入的憑證。

為插件啟用 CA 憑證

您應該設定 CA 憑證並在SnapCenter伺服器 and 對應的插件主機中部署 CA 憑證。您應該為插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行 `_Set-SmCertificateSettings_ cmdlet` 來啟用或停用 CA 憑證。
- 您可以使用 `_Get-SmCertificateSettings_` 顯示插件的憑證狀態。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體 Cmdlet 參考指南](#)"。

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. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示SnapCenter伺服器和插件主機之間的連線狀態。

- *  * 表示 CA 憑證未啟用或未指派給插件主機。
- *  * 表示 CA 憑證驗證成功。
- *  * 表示無法驗證 CA 憑證。
- *  * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

版權資訊

Copyright © 2025 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。