



準備安裝適用於 **Microsoft SQL Server** 的**SnapCenter**插件 SnapCenter software

NetApp
November 06, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/snapcenter-61/protect-scsql/task_install_snapcenter_plug_in_for_microsoft_sql_server_database.html on November 06, 2025. Always check docs.netapp.com for the latest.

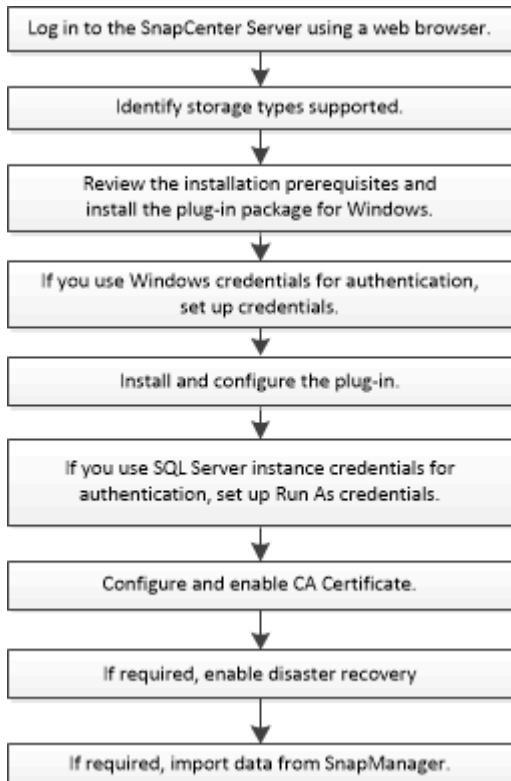
目錄

準備安裝適用於 Microsoft SQL Server 的SnapCenter插件	1
SnapCenter Plug-in for Microsoft SQL Server 的安裝工作流程	1
新增主機並安裝適用於 Microsoft SQL Server 的SnapCenter外掛程式的先決條件	1
安裝適用於 Windows 的SnapCenter插件包的主機需求	2
為 Windows 的SnapCenter插件包設定憑證	3
為單一 SQL Server 資源配置憑證	4
步驟 1：新增並設定憑證	5
步驟 2：設定實例	5
在 Windows Server 2016 或更高版本上設定 gMSA	6
為 Microsoft SQL Server 安裝SnapCenter插件	7
新增主機並安裝適用於 Windows 的SnapCenter插件包	7
使用 cmdlet 在多個遠端主機上安裝適用於 Microsoft SQL Server 的SnapCenter插件	10
從命令列靜默安裝適用於 Microsoft SQL Server 的SnapCenter插件	11
監控 SQL Server 插件的安裝狀態	12
設定 CA 憑證	13
產生CA憑證CSR文件	13
匯入 CA 憑證	13
取得 CA 憑證指紋	14
使用 Windows 主機插件服務設定 CA 憑證	14
為插件啟用 CA 憑證	15
配置災難復原	16
SnapCenter插件 for SQL Server 的災難復原	16
SnapCenter Plug-in for SQL Server 的儲存災難復原 (DR)	16
從適用於 SQL Server 二級儲存的SnapCenter插件故障還原到主存儲	17

準備安裝適用於 Microsoft SQL Server 的 SnapCenter 插件

SnapCenter Plug-in for Microsoft SQL Server 的安裝工作流程

如果您想要保護 SQL Server 資料庫，則應該安裝並設定適用於 Microsoft SQL Server 的 SnapCenter 外掛程式。



新增主機並安裝適用於 Microsoft SQL Server 的 SnapCenter 外掛程式的先決條件

在新增主機和安裝插件包之前，您必須完成所有要求。

- 如果您正在使用 iSCSI，則 iSCSI 服務必須正在執行。
- 您必須擁有具有本機管理員權限的用戶，且該用戶在遠端主機上具有本機登入權限。
- 如果您在 SnapCenter 中管理叢集節點，則必須擁有對叢集中所有節點具有管理權限的使用者。
- 您必須擁有在 SQL Server 上具有 sysadmin 權限的使用者。

適用於 Microsoft SQL Server 的 SnapCenter 外掛程式使用 Microsoft VDI 框架，該框架需要系統管理員存取權。

["Microsoft 支援文章 2926557：SQL Server VDI 備份與還原作業需要 Sysadmin 權限"](#)

- 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。
- 如果安裝了 SnapManager for Microsoft SQL Server，則必須停止或停用該服務和計畫。

如果您打算將備份或複製作業匯入 SnapCenter，請不要解除安裝 SnapManager for Microsoft SQL Server。

- 主機必須能夠解析為伺服器的完全限定網域名稱 (FQDN)。

如果修改了 hosts 檔案以使其可解析，並且在 hosts 檔案中指定了短名稱和 FQDN，則在 SnapCenter hosts 檔案中建立一個項目，格式如下：<ip_address> <host_fqdn> <host_name>

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。

物品	要求
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 • Java 11 Oracle Java 與 OpenJDK Java 11 Oracle Java 和 OpenJDK 僅適用於 SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp支援的插件以及可安裝在 Windows 主機上的其他自訂應用程式。 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。"

為 Windows 的SnapCenter插件包設定憑證

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。

開始之前

- 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。
- Windows 主機上的 SQL 驗證

安裝插件後，您必須設定 SQL 憑證。

如果您正在為 Microsoft SQL Server 部署SnapCenter插件，則必須在安裝插件後設定 SQL 憑證。為具有 SQL Server sysadmin 權限的使用者設定憑證。

SQL 驗證方法針對 SQL Server 執行個體進行驗證。這意味著必須在SnapCenter中發現 SQL Server 執行個體。因此，在新增SQL憑證前，必須先新增主機、安裝外掛程式包、刷新資源。您需要 SQL Server 驗證才能執行諸如調度或發現資源之類的操作。

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/密碼	輸入用於身份驗證的使用者名稱和密碼。 • 網域管理員 指定要安裝SnapCenter插件的系統上的網域管理員。用戶名字段的有效格式為： ◦ NetBIOS\UserName ◦ Domain FQDN\UserName • 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。用戶名字段的有效格式為： UserName 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， lessthan<!10 、 lessthan10<! 、 backtick`12 。
認證模式	選擇您想要使用的身份驗證模式。如果選擇SQL驗證模式，也必須指定SQL伺服器執行個體以及SQL實例所在的主機。

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。

為單一 SQL Server 資源配置憑證

您可以設定憑證來為每個使用者在單獨的 SQL Server 資源上執行資料保護作業。雖然您可以全域設定憑證，但您可能只想針對特定資源執行此操作。

關於此任務

- 如果您使用 Windows 憑證進行驗證，則必須在安裝外掛程式之前設定您的憑證。

但是，如果您使用 SQL Server 執行個體進行驗證，則必須在安裝外掛程式後新增憑證。

- 如果您在設定憑證時啟用了 SQL 驗證，則發現的執行個體或資料庫將顯示紅色掛鎖圖示。

如果出現掛鎖圖標，則必須指定實例或資料庫憑證才能成功將實例或資料庫新增至資源組。

- 當滿足下列條件時，您必須將憑證指派給沒有 sysadmin 存取權限的基於角色的存取控制 (RBAC) 使用者：
 - 憑證已指派給 SQL 實例。
 - SQL 實例或主機被指派給 RBAC 使用者。

使用者必須同時擁有資源群組和備份權限。

步驟 1：新增並設定憑證

1. 在左側導覽窗格中，選擇「設定」。
2. 在設定頁面中，選擇*憑證*。
 - a. 若要新增憑證，請選擇「新建」。
 - b. 在憑證頁面中，設定憑證：

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 SQL Server 驗證的使用者名稱。 • 網域管理員或管理員群組的任何成員 指定要安裝SnapCenter外掛程式的系統上的網域管理員或管理員群組的任何成員。「使用者名稱」欄位的有效格式為： ◦ <i>NetBIOS</i>\使用者名稱 ◦ 域 <i>FQDN</i>\用戶名 • 本機管理員（僅限工作群組）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。使用者名稱 欄位的有效格式為： <i>UserName</i>
密碼	輸入用於身份驗證的密碼。
認證方式	選擇 SQL Server 驗證模式。如果 Windows 使用者在 SQL 伺服器上具有 sysadmin 權限，您也可以選擇 Windows 驗證。
主持人	選擇主機。
SQL Server 執行個體	選擇 SQL Server 執行個體。

- c. 選擇“確定”新增憑證。

步驟 2：設定實例

1. 在左側導覽窗格中，選擇「資源」。

2. 在資源頁面中，從*檢視*清單中選擇*實例*。
 - a. 選擇 image:.../media/filter_icon.png[過濾器圖示]，然後選擇主機名稱來過濾實例。
 - b. 選擇 image:.../media/filter_icon.png[filter icon] 以關閉過濾器窗格。
3. 在實例保護頁面中，保護實例，如果需要，選擇*配置憑證*。

如果登入 SnapCenter 伺服器的使用者無法存取 Microsoft SQL Server 的 SnapCenter 插件，則使用者必須設定憑證。



憑證選項不適用於資料庫和可用性群組。

4. 選擇*刷新資源*。

在 Windows Server 2016 或更高版本上設定 gMSA

Windows Server 2016 或更高版本可讓您建立群組託管服務帳戶 (gMSA)，該帳戶會從託管網域帳戶提供自動服務帳戶密碼管理。

開始之前

- 您應該擁有 Windows Server 2016 或更高版本的網域控制站。
- 您應該擁有一個 Windows Server 2016 或更高版本的主機，它是網域的成員。

步驟

1. 建立 KDS 根金鑰來為 gMSA 中的每個物件產生唯一的密碼。
2. 對於每個網域，從 Windows 網域控制站執行以下命令：Add-KDSRootKey -EffectiveImmediately
3. 建立並配置 gMSA：
 - a. 建立用戶群組帳號，格式如下：

```
domainName\accountName$  
.. 將電腦物件新增至群組。  
.. 使用您剛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,...>  
.. 跑步 `Get-ADServiceAccount` 命令來驗證服務帳戶。
```

4. 在您的主機上設定 gMSA：
 - a. 在要使用 gMSA 帳號的主機上啟用 Windows PowerShell 的 Active Directory 模組。

為此，請從 PowerShell 執行以下命令：

```
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. 透過從 PowerShell 命令提示字元執行以下命令在主機上安裝 gMSA：Install-AdServiceAccount <gMSA>
 - c. 透過執行以下命令驗證你的 gMSA 帳戶：Test-AdServiceAccount <gMSA>
5. 將管理權限指派給主機上配置的 gMSA。
 6. 透過在 SnapCenter 伺服器中指定配置的 gMSA 帳戶來新增 Windows 主機。

SnapCenter Server 將在主機上安裝選定的插件，並且指定的 gMSA 將在插件安裝期間用作服務登入帳戶。

為 Microsoft SQL Server 安裝 SnapCenter 插件

新增主機並安裝適用於 Windows 的 SnapCenter 插件包

您必須使用 SnapCenter *新增主機* 頁面來新增主機並安裝插件包。插件會自動安裝在遠端主機上。

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 主機上安裝外掛程式時，如果指定非內建的憑證，則應在主機上停用 UAC。

- 您應該確保訊息佇列服務處於運行狀態。
- 如果您使用群組託管服務帳戶 (gMSA)，則應使用管理權限設定 gMSA。

["在 Windows Server 2016 或更高版本上為 SQL 設定組託管服務帳戶"](#)

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。

您可以新增主機並為單一主機或叢集安裝插件包。如果您在叢集或 Windows Server 故障轉移叢集 (WSFC) 上安裝插件，則插件將安裝在叢集的所有節點上。

有關管理主機的信息，請參閱["管理主機"](#)。

步驟

1. 在左側導覽窗格中，選擇*主機*。
2. 驗證頂部的「託管主機」標籤是否已選取。
3. 選擇“新增”。
4. 在「主機」頁面中執行以下操作：

對於這個領域...	這樣做...
主機類型	選擇 Windows 作為主機類型。SnapCenter伺服器會新增主機，然後安裝適用於 Windows 的插件（如果主機上尚未安裝該插件）。 如果您在「外掛程式」頁面上選擇「Microsoft SQL Server」選項，SnapCenter伺服器將安裝 SQL Server 外掛程式。
主機名稱	輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。只有當 IP 位址解析為 FQDN 時，不受信任的網域主機才支援該 IP 位址。 SnapCenter依賴 DNS 的正確配置。因此，最佳做法是輸入 FQDN。 您可以輸入以下之一的 IP 位址或 FQDN： • 獨立主機 • WSFC 如果您使用SnapCenter新增主機且該主機是子網域的一部分，則必須提供 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。 您可以將遊標置於指定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。

6. 選擇*更多選項*。

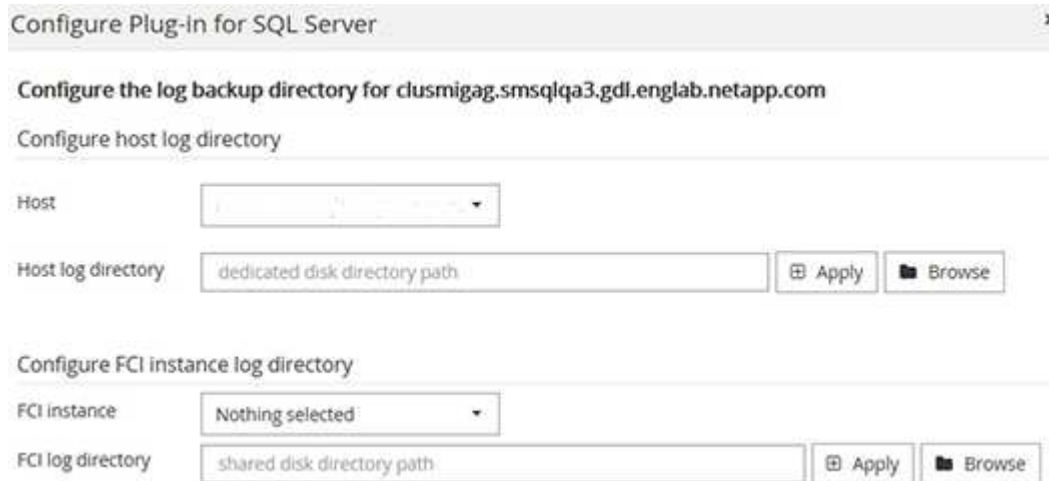
對於這個領域...	這樣做...
港口	保留預設連接埠號碼或指定連接埠號碼。預設連接埠號碼為 8145。如果SnapCenter伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。
安裝路徑	預設路徑為 C:\Program Files\ NetApp\ SnapCenter。您可以選擇自訂路徑。
新增叢集中的所有主機	選取此核取方塊可新增 WSFC 或 SQL 可用性群組中的所有叢集節點。如果您想要管理和識別叢集內的多個可用的 SQL 可用性群組，則應該透過選擇 GUI 中的對應叢集複選框來新增所有叢集節點。
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。
使用群組託管服務帳戶 (gMSA) 執行外掛程式服務	如果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。 以以下格式提供 gMSA 名稱 ：domainName\accountName\$。  如果主機新增了 gMSA，且 gMSA 具有登入和系統管理員權限，則 gMSA 將用於連線到 SQL 實例。

7. 選擇*提交*。

8. 對於SQL插件，選擇主機來設定日誌目錄。

a. 選擇*設定日誌目錄*，在設定主機日誌目錄頁面中選擇*瀏覽*並完成下列步驟：

僅列出NetApp LUN（驅動器）可供選擇。 SnapCenter在備份作業過程中備份並複製主機日誌目錄。



i. 選擇主機上將儲存主機日誌的磁碟機號碼或掛載點。

ii. 如果需要，請選擇一個子目錄。

iii. 選擇*儲存*。

9. 選擇*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。

10. 監控安裝進度。

使用 **cmdlet** 在多個遠端主機上安裝適用於 **Microsoft SQL Server** 的**SnapCenter**插件

您可以使用 Install-SmHostPackage PowerShell cmdlet 同時在多個主機上安裝適用於 Microsoft SQL Server 的SnapCenter外掛程式。

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 和所需參數在多個遠端主機上安裝適用於 Microsoft SQL Server

的SnapCenter外掛程式。

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時，可以使用 `-skipprecheck` 選項。

4. 輸入您的遠端安裝憑證。

從命令列靜默安裝適用於 Microsoft SQL Server 的SnapCenter插件

您應該從SnapCenter使用者介面安裝適用於 Microsoft SQL Server 的SnapCenter外掛程式。但是，如果您因為某些原因無法這樣做，您可以從 Windows 命令列以靜默模式無人值守執行 SQL Server 外掛程式安裝程式。

開始之前

- 在安裝之前，您必須刪除適用於 Microsoft SQL Server 的早期版本的SnapCenter外掛程式。

有關更多信息，請參閱 ["如何從插件主機手動直接安裝SnapCenter插件"](#)。

步驟

- 驗證插件主機上是否存在 `C:\temp` 資料夾以及登入使用者是否對該資料夾具有完全存取權限。
- 從 `C:\ProgramData\NetApp\SnapCenter\Package Repository` 下載 SQL Server 軟體插件。

可以從安裝SnapCenter伺服器的主機存取此路徑。

- 將安裝檔案複製到要安裝插件的主機上。
- 從本機上的 Windows 命令提示符，導覽至儲存插件安裝檔案的目錄。
- 安裝 SQL Server 軟體插件：

```
"snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"  
/log"Log_Path" BI_SNAPCENTER_PORT=Num  
SUITE_INSTALLDIR="Install_Directory_Path"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW,SCSQL
```

用您的資料替換佔位符值

- Debug_Log_Path 是套件安裝程式日誌檔案的名稱和位置。
- Log_Path 是插件元件（SCW、SCSQL 和 SMCore）的安裝日誌的位置。
- Num 是SnapCenter與 SMCore 通訊的端口
- Install_Directory_Path是主機插件包安裝目錄。
- domain\administrator 是 Microsoft Windows Web 服務帳戶的SnapCenter外掛程式。
- password 是 Microsoft Windows Web 服務帳戶的SnapCenter外掛程式的密碼。+
"snapcenter_windows_host_plugin.exe"/silent
/debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\ " BI_SNAPCENTER_PORT=8145

```
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW,SCSQL
```



安裝 SQL Server 外掛程式期間傳遞的所有參數都區分大小寫。

6. 監視 Windows 工作排程器、主安裝記錄檔 C:\Installdebug.log 以及 C:\Temp 中的附加安裝檔。
7. 監控 %temp% 目錄以驗證 msix.exe 安裝程式是否正在無錯誤地安裝軟體。



SQL Server 插件的安裝在主機上註冊該插件，而不是在 SnapCenter 伺服器上註冊。您可以透過使用 SnapCenter GUI 或 PowerShell cmdlet 新增主機在 SnapCenter 伺服器上註冊插件。新增主機後，會自動發現插件。

監控 SQL Server 插件的安裝狀態

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 and 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：

- 雙擊該證書。
- 在「證書」對話方塊中，按一下「詳細資料」標籤。
- 捲動瀏覽欄位清單並按一下「指紋」。
- 從框複製十六進位字元。
- 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：“a909502dd82ae41433e68383883”。

2. 從 PowerShell 執行以下操作：

- 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
```

- 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。

配置災難復原

SnapCenter 插件 for SQL Server 的災難復原

當 SQL Server 的 SnapCenter 外掛程式關閉時，請使用下列步驟切換到其他 SQL 主機並還原資料。

開始之前

- 輔助主機應具有與主主機相同的作業系統、應用程式和主機名稱。
- 使用「新增主機」或「修改主機」頁面將 SQL Server 的 SnapCenter 外掛程式推送到備用主機。看["管理主機"](#)了解更多。

步驟

1. 從「主機」頁面中選擇主機來修改並安裝 SQL Server 的 SnapCenter 插件。
2. (可選) 將 SQL Server 設定檔的 SnapCenter 插件從災難復原 (DR) 備份取代到新電腦。
3. 從 DR 備份中的 SQL Server 資料夾的 SnapCenter 插件匯入 Windows 和 SQL 計畫。

相關資訊

查看["災難復原 API"](#)影片。

SnapCenter Plug-in for SQL Server 的儲存災難復原 (DR)

您可以透過在「全域設定」頁面中啟用儲存的 DR 模式來還原用於 SQL Server 儲存的 SnapCenter 插件。

開始之前

- 確保插件處於維護模式。
- 中斷 SnapMirror/ SnapVault 關係。["中斷 SnapMirror 關係"](#)
- 將從屬磁碟的 LUN 連接到具有相同磁碟機號碼的主機。
- 確保所有磁碟都使用 DR 之前使用的相同磁碟機號碼進行連接。
- 重新啟動 MSSQL 伺服器服務。
- 確保 SQL 資源重新連線。

關於此任務

VMDK 和 RDM 配置不支援災難復原 (DR)。

步驟

1. 在「設定」頁面中，導覽至「設定」>「全域設定」>「災難復原」。
2. 選擇“啟用災難復原”。
3. 按一下“應用”。
4. 按一下「監控」>「作業」來驗證 DR 作業是否已啟用。

完成後

- 如果故障轉移後建立了新的資料庫，則資料庫將處於非 DR 模式。

新的資料庫將像故障轉移之前一樣繼續運作。

- 在 DR 模式下建立的新備份將在拓樸頁面中的SnapMirror或SnapVault（輔助）下列出。

新備份旁邊會顯示一個「i」圖標，表示這些備份是在 DR 模式期間建立的。

- 您可以使用 UI 或以下 cmdlet 刪除故障轉移期間建立的 SQL Server 備份的SnapCenter插件：Remove-SmBackup
- 故障轉移後，如果您希望某些資源處於非 DR 模式，請使用下列 cmdlet：Remove-SmResourceDRMode

更多資訊請參閱 "[SnapCenter軟體 Cmdlet 參考指南](#)"。

- SnapCenter Server 將管理處於 DR 或非 DR 模式的單一儲存資源（SQL 資料庫），但不管理處於 DR 模式或非 DR 模式的儲存資源的資源群組。

從適用於 **SQL Server** 二級儲存的**SnapCenter**插件故障還原到主儲存

在 SQL Server 主儲存的SnapCenter外掛程式還原連線後，您應該故障還原到主儲存。

開始之前

- 從託管主機頁面將 SQL Server 的SnapCenter插件置於*維護*模式。
- 中斷輔助儲存與主機的連線並從主儲存進行連線。
- 若要故障恢復到主儲存，請透過執行反向重新同步操作確保關係方向與故障轉移之前保持相同。

為了在反向重新同步操作後保留主儲存和輔助儲存的角色，請再次執行反向重新同步操作。

更多資訊請參見"[反向重新同步鏡像關係](#)"

- 重新啟動 MSSQL 伺服器服務。
- 確保 SQL 資源重新連線。



在插件故障轉移或故障回復期間，插件整體狀態不會立即刷新。主機和插件的整體狀態在後續的主機刷新操作中更新。

步驟

1. 在「設定」頁面中，導覽至「設定」>「全域設定」>「災難復原」。
2. 取消選擇“啟用災難復原”。
3. 按一下“應用”。
4. 按一下「監控」>「作業」來驗證 DR 作業是否已啟用。

完成後

您可以使用 UI 或以下 cmdlet 刪除故障轉移期間建立的 SQL Server 備份的SnapCenter插件：Remove-SmDRFailoverBackups

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。