準備安裝SnapCenter 適用於Microsoft SQL Server的支援功能

SnapCenter software

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/snapcenter/protect-scsql/task_install_snapcenter_plug_in_for_microsoft_sql_server_database.html on January 09, 2026. Always check docs.netapp.com for the latest.

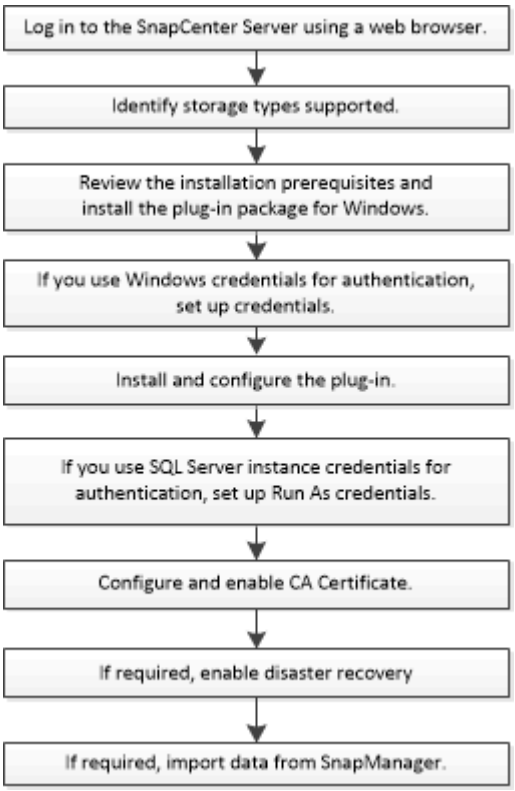
目錄

準備安裝SnapCenter 適用於Microsoft SQL Server的支援功能 1
適用於Microsoft SQL Server的安裝工作流程SnapCenter 1
新增主機和安裝SnapCenter Microsoft SQL Server的支援功能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 2
設定SnapCenter 適用於Windows的效能不整套件認證 3
設定個別SQL Server資源的認證資料 4
步驟 1 ：新增及設定認證 5
步驟 2 ：設定執行個體 5
在Windows Server 2016或更新版本上設定GMSA 6
安裝SnapCenter 適用於Microsoft SQL Server的功能性外掛程式 7
新增主機並安裝SnapCenter 適用於Windows的Sfor Plug-ins套件 7
使用Cmdlet在SnapCenter 多個遠端主機上安裝適用於Microsoft SQL Server的支援功能外掛程式 10
從命令列以無訊息方式安裝SnapCenter 適用於Microsoft SQL Server的功能 11
監控安裝SQL Server外掛程式的狀態 12
設定CA憑證 13
產生CA認證CSR檔案 13
匯入CA憑證 13
取得CA憑證指紋 14
使用Windows主機外掛程式服務設定CA憑證 14
啟用外掛程式的CA憑證 15
設定災難恢復 16
SQL Server適用的支援功能SnapCenter 16
適用於SQL Server的儲存災難恢復（DR）SnapCenter 16
從SnapCenter SQL Server二線儲存設備的支援程式容錯回復到一線儲存設備 17

準備安裝SnapCenter 適用於Microsoft SQL Server的支援功能

適用於Microsoft SQL Server的安裝工作流程SnapCenter

若要SnapCenter 保護SQL Server資料庫、您應該安裝並設定Microsoft SQL Server的支援功能。



新增主機和安裝SnapCenter Microsoft SQL Server的支援功能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。

- 如果您使用iSCSI、則必須執行iSCSI服務。
- 您必須擁有具有本機系統管理員權限的使用者、且該使用者具有遠端主機的本機登入權限。
- 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。
- 您的使用者必須具有SQL Server上的Sysadmin權限。

  適用於Microsoft SQL Server的VMware vCenter外掛程式使用Microsoft VDI架構、需要系統管理員存取權。SnapCenter

  "Microsoft支援文件編號2926557：SQL Server VDI備份與還原作業需要Sysadmin權限"

- 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.
- 如果安裝了適用於Microsoft SQL Server的功能、您必須停止或停用服務和排程。SnapManager

  如果您打算將備份或複製工作匯入SnapCenter 到支援區、請勿解除安裝SnapManager Microsoft SQL Server的功能。

- 主機必須可解析為伺服器的完整網域名稱（FQDN）。

  如果已修改hosts檔案以使其可解析、且在hosts檔案中同時指定了簡短名稱和FQDN、請在SnapCenter 下列格式的lsethosts檔案中建立項目：<ip_address><host_fqd><host_name>

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 有關受支援版本的最新信息，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 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	• ASP.NET Core Runtime 8.0.12 （以及所有後續 8.0.x 修補程式）代管產品組合 • PowerShell Core 7.4.2 • Java 11 Oracle Java 和 OpenJDK 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"

設定SnapCenter 適用於Windows的效能不整套件認證

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

- 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。
- Windows主機上的SQL驗證

  安裝外掛程式之後、您必須設定SQL認證。

  如果您要部署SnapCenter 適用於Microsoft SQL Server的支援功能、則必須在安裝外掛程式之後設定SQL認證。為具有SQL Server Sysadmin權限的使用者設定認證。

  SQL驗證方法會針對SQL Server執行個體進行驗證。這表示SQL Server執行個體必須在SnapCenter 支援中發現。因此、在新增SQL認證之前、您必須先新增主機、安裝外掛程式套件、以及重新整理資源。您需要SQL Server驗證、才能執行排程或探索資源等作業。

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。

針對此欄位...	執行此動作...
使用者名稱/密碼	輸入用於驗證的使用者名稱和密碼。 • 網域管理員 在您要安裝SnapCenter 此插件的系統上指定網域管理員。「使用者名稱」欄位的有效格式為： ◦ 「netbios\使用者名稱」 ◦ 「主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」（使用者名稱） 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、lessthan<!10、lessthan10<!、backtick'12。
驗證模式	選取您要使用的驗證模式。如果您選取SQL驗證模式、也必須指定SQL Server執行個體和SQL執行個體所在的主機。

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」頁面中指派認證維護給使用者或使用者群組。

設定個別SQL Server資源的認證資料

您可以設定認證資料、以便在每個使用者的個別SQL Server資源上執行資料保護工作。雖然您可以全域設定認證、但您可能只想針對特定資源進行設定。

關於這項工作

- 如果您使用Windows認證來進行驗證、則必須先設定認證、才能安裝外掛程式。

  不過、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之後新增認證。

- 如果您在設定認證資料時啟用SQL驗證、探索到的執行個體或資料庫會顯示紅色掛鎖圖示。

  如果出現掛鎖圖示、您必須指定執行個體或資料庫認證、才能將執行個體或資料庫成功新增至資源群組。

- 當符合下列條件時、您必須將認證指派給不具備Sysadmin存取權限的角色型存取控制（RBAC）使用者：
  - 認證資料會指派給SQL執行個體。
  - SQL執行個體或主機會指派給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 ：新增及設定認證

1. 在左導覽窗格中、選取 * 設定 * 。
2. 在「設定」頁面中、選取 * 認證 * 。
   a. 若要新增認證、請選取 * 新增 * 。
   b. 在「認證」頁面中、設定認證資料：

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SQL Server驗證的使用者名稱。 • 網域管理員或系統管理員群組的任何成員、都會在您要安裝SnapCenter 此插件的系統上、指定網域管理員或系統管理員群組的任何成員。*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_ • 本機系統管理員（僅適用於工作群組）若為屬於某工作群組的系統、請在安裝SnapCenter 此程式的系統上指定內建本機系統管理員。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*
密碼	輸入用於驗證的密碼。
驗證模式	選取SQL Server驗證模式。如果Windows使用者在SQL Server上具有Sysadmin權限、您也可以選擇Windows驗證。
主機	選取主機。
SQL Server 執行個體	選取SQL Server執行個體。

   c. 選取 * 確定 * 以新增認證。

步驟 2 ：設定執行個體

1. 在左導覽窗格中、選取 * 資源 * 。

2. 在「資源」頁面中、從*檢視*清單中選取*執行個體*。
   a. 選取 [篩選圖示] ，然後選取要篩選執行個體的主機名稱。
   b. 選取映像： ../media/filter 圖示 .png [filter icon] 以關閉篩選窗格。
3. 在 Instance Protect （執行個體保護）頁面中、保護執行個體、必要時選取 * Configure Credentials* （設定認證 * ）。

   如果登入SnapCenter 到此伺服器的使用者無法存取SnapCenter 適用於Microsoft SQL Server的支援功能、則使用者必須設定認證資料。

   認證選項不適用於資料庫和可用度群組。

4. 選擇*重新整理資源*。

在Windows Server 2016或更新版本上設定GMSA

Windows Server 2016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 2016或更新版本的網域控制器。
- 您應該擁有Windows Server 2016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 適用於Microsoft SQL Server的功能性外掛程式

新增主機並安裝SnapCenter 適用於Windows的Sfor Plug-ins套件

您必須使用SnapCenter 「功能不全*新增主機*」頁面來新增主機並安裝外掛程式套件。外掛程式會自動安裝在遠端主機上。

開始之前

- 如果 SnapCenter 伺服器主機的作業系統為 Windows 2019 、而外掛主機的作業系統為 Windows 2022 、則應執行下列步驟：
  - 升級至 Windows Server 2019 （ OS Build 17763.5936 ）或更新版本
  - 升級至 Windows Server 2022 （ OS Build 20348.2402 ）或更新版本

- 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、就應該停用主機上的UAC。
- 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。

  "在Windows Server 2016或更新版本上為SQL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。

您可以為個別主機或叢集新增主機並安裝外掛程式套件。如果您要在叢集或Windows Server容錯移轉叢集（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。

如需管理主機的相關資訊、請參閱 "管理主機"。

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」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Windows作為主機類型。如果主機上尚未安裝外掛程式、則會新增該主機、然後安裝Windows外掛程式。SnapCenter 如果您在外掛程式頁面上選取Microsoft SQL Server選項、SnapCenter 則會安裝適用於SQL Server的外掛程式。
主機名稱	輸入主機的完整網域名稱（FQDN）或IP位址。僅當不受信任的網域主機解析為FQDN時、才支援IP位址。 取決於DNS的正確組態。SnapCenter因此、最佳做法是輸入FQDN。 您可以輸入下列其中一項的IP位址或FQDN： • 獨立式主機 • WSFC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。

針對此欄位...	執行此動作...
認證資料	選取您所建立的認證名稱、或建立新認證資料。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。

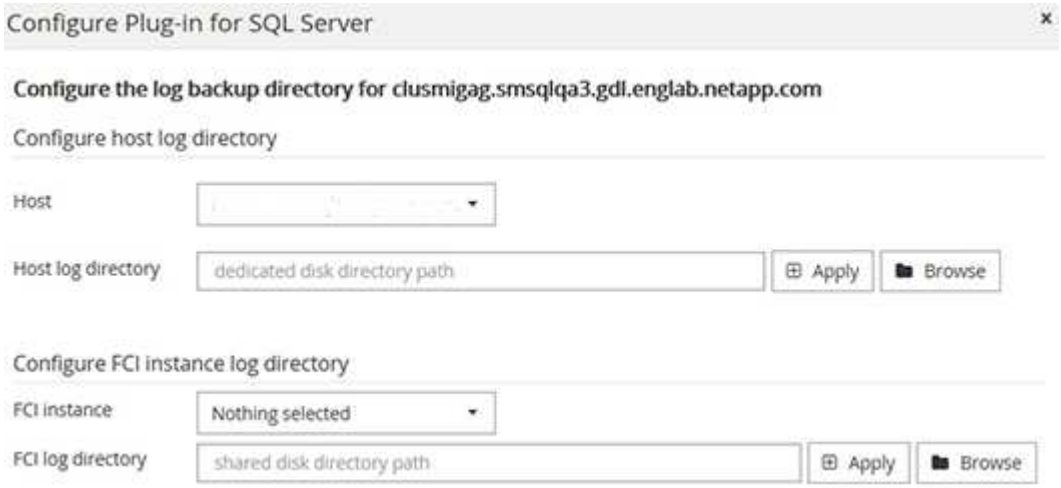
5. 在*選取要安裝的外掛程式*區段中、選取要安裝的外掛程式。
6. 選擇*更多選項*。

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。
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。
新增叢集中的所有主機	選取此核取方塊可新增WSFC或SQL可用度群組中的所有叢集節點。如果您想要管理及識別叢集內的多個可用SQL可用度群組、請在GUI中選取適當的叢集核取方塊、以新增所有叢集節點。
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$。 如果使用GMSA新增主機、且GMSA具有登入和系統管理權限、則會使用GMSA連線至SQL執行個體。

7. 選擇*提交*。

8. 對於SQL外掛程式、請選取要設定記錄目錄的主機。
   a. 選取 * 設定記錄目錄 * 、然後在「設定主機記錄目錄」頁面中選取 * 瀏覽 * 、然後完成下列步驟：

      僅列出NetApp LUN（磁碟機）供選擇。作爲備份作業的一部分、支援並複寫主機記錄目錄。SnapCenter



      i. 選取要儲存主機記錄的主機上的磁碟機代號或掛載點。
      ii. 如有需要、請選擇子目錄。
      iii. 選擇*保存*。
9. 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。

10. 監控安裝進度。

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

您SnapCenter 可以使用Install-SmHostPackage PowerShell Cmdlet、在多個主機上同時安裝適用於Microsoft SQL Server的VMware®更新外掛程式。

開始之前

您必須以SnapCenter 網域使用者的身分登入到支援安裝外掛程式套件的每個主機、並具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SnapCenter 多個遠端主機上安裝適用於Microsoft SQL Server的VMware vCenter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"。

   當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時、可以使用-skipprecheck選項。

4. 輸入遠端安裝的認證資料。

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

您應該SnapCenter 從SnapCenter 支援功能的使用者介面中安裝適用於Microsoft SQL Server的支援功能。不過、如果您因為某些原因無法執行、您可以從Windows命令列以無訊息模式執行SQL Server外掛程式安裝程式。

開始之前

- 安裝之前、您必須先刪除SnapCenter 舊版的Microsoft SQL Server適用的支援功能。

  如需詳細資訊、請參閱 "如何SnapCenter 手動直接從外掛主機安裝功能不全的外掛程式"。

步驟

1. 驗證外掛程式主機上是否存在C：\Temp資料夾、且登入的使用者是否擁有該資料夾的完整存取權。
2. 從C：\ProgramData \NetApp\SnapCenter\Package儲存庫下載SQL Server外掛程式軟體。

   此路徑可從SnapCenter 安裝了此伺服器的主機存取。

3. 將安裝檔案複製到您要安裝外掛程式的主機。
4. 從本機主機上的Windows命令提示字元、瀏覽至您儲存外掛程式安裝檔案的目錄。
5. 安裝適用於SQL Server軟體的外掛程式：

   「snapcenter_windows_host_plugin.exe」/無聲/debuglog"debug_Log_Path"/log"Log_Path" BI_SNAPCENTE_port=Numsit_Install_Directory路徑" BI_ServiceAccount=domain\Administrator BI_SERVERICEPW=password ISfeatureInstall=SCW,SCSQL

   將預留位置值取代為您的資料

   - debug_Log_Path是套件安裝程式記錄檔的名稱和位置。
   - Log_Path是外掛程式元件（SCW、SCSQL和SMCore）安裝記錄的位置。
   - 區號是SnapCenter 指與SMCore進行通訊的連接埠
   - 安裝目錄路徑是主機外掛程式套件安裝目錄。
   - 網域\系統管理員是SnapCenter 適用於Microsoft Windows Web服務帳戶的功能不全外掛程式。
   - 密碼是SnapCenter Microsoft Windows Web服務帳戶的密碼。+"snapcenter_windows_host_plugin.exe"/silent /debuglog" C：\HPPW_SCSQL_Install.log"/log" C

：" BI_SNAPCENTE_port=8145套件_INSTALLDIR="C：\Program Files\NetApp\Center" BI_ServiceAccount=domain\Administrator BI_SCW=SnapSCW=SQL安裝

安裝適用於SQL Server的外掛程式時所傳遞的所有參數都區分大小寫。

6. 監控Windows工作排程器、主要安裝記錄檔C：\Installdebug.log、以及C：\Temp中的其他安裝檔案。
7. 監控%temp%目錄、確認msiexe.exe安裝程式安裝軟體時沒有錯誤。

SQL Server外掛程式的安裝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。

監控安裝**SQL Server**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 金鑰長度必須至少為 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*」。

在此精靈視窗中...	請執行下列動作...
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"
```

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。

設定災難恢復

SQL Server適用的支援功能SnapCenter

SnapCenter Plug-in for SQL Server 當機時、請使用下列步驟切換至不同的 SQL 主機並恢復資料。

開始之前

- 次要主機的作業系統、應用程式和主機名稱應與主要主機相同。
- 使用「新增主機」或「修改主機」頁面、將SnapCenter 適用於SQL Server的「功能不全」外掛程式推送到替代主機。請參閱 "管理主機" 以取得更多資訊。

步驟

1. 從「主機」頁面選取主機、以修改及安裝SnapCenter 適用於SQL Server的「支援SQL Server的支援程式」。
2. （選用）將SnapCenter SQL Server組態檔案的支援範本從災難恢復（DR）備份取代為新機器。
3. 從SnapCenter DR備份的「SQL Server適用的支援程式」資料夾匯入Windows和SQL排程。

相關資訊

觀看 "災難恢復API" 影片。

適用於SQL Server的儲存災難恢復（DR）SnapCenter

您可以SnapCenter 在「Global Settings（全域設定）」頁面中啟用「DR Mode for Storage（儲存的DR模式）」、以還原適用於SQL Server儲存設備的「支援功能」外掛程式。

開始之前

- 確認外掛程式處於維護模式。
- 打破SnapMirror/SnapVault關係。"打破SnapMirror關係"
- 使用相同的磁碟機代號將LUN從次要連接到主機機器。
- 確保所有磁碟均使用DR之前使用的相同磁碟機代號進行連接。
- 重新啟動MSSQL伺服器服務。
- 確保SQL資源重新連線。

關於這項工作

VMDK和RDM組態不支援災難恢復（DR）。

步驟

1. 在「設定」頁面中、瀏覽至*設定*>*全域設定*>*災難恢復*。
2. 選取*「啟用災難恢復」*。
3. 按一下「*套用*」。
4. 按一下「監控>*工作*」來確認DR工作是否已啟用。

完成後

- 如果在容錯移轉之後建立新資料庫、資料庫將處於非DR模式。

  新資料庫的運作方式將如同容錯移轉之前一樣。

- 以DR模式建立的新備份會列SnapVault 在「拓撲」頁面的SnapMirror或還原（次要）下方。

  新備份旁邊會顯示「I」圖示、表示這些備份是在DR模式期間建立。

- 您可以使用SnapCenter UI或下列Cmdlet刪除在容錯移轉期間建立的SQL Server備份的現象：「移除SmBackup」
- 容錯移轉之後、如果您想讓部分資源處於非DR模式、請使用下列Cmdlet：「移除-短資源DRMode」

  如需詳細資訊、請參閱 "《軟件指令程式參考指南》SnapCenter"。

- 使用DR模式或非DR模式的個別儲存資源（SQL資料庫）、而非資源群組、將以DR模式或非DR模式的儲存資源來管理。SnapCenter

從SnapCenter SQL Server二線儲存設備的支援程式容錯回復到一線儲存設備

當SQL Server主要儲存設備的「支援還原」外掛程式重新連線後SnapCenter 、您應該容錯回復至主要儲存設備。

開始之前

- 從SnapCenter 「託管主機」頁面、將適用於SQL Server的「支援」外掛程式置於*維護*模式。
- 從主機拔下二線儲存設備、然後從一線儲存設備連線。
- 若要容錯回復至主要儲存設備、請執行反向重新同步作業、確保關係方向與容錯移轉之前的方向相同。

  若要在反向重新同步作業之後保留主要和次要儲存設備的角色、請再次執行反轉重新同步作業。

  如需詳細資訊、請參閱 "反轉重新同步鏡射關係"

- 重新啟動MSSQL伺服器服務。
- 確保SQL資源重新連線。

> 在外掛程式的容錯移轉或容錯回復期間、外掛程式的整體狀態不會立即重新整理。主機和外掛程式的整體狀態會在後續的主機重新整理作業期間更新。

步驟

1. 在「設定」頁面中、瀏覽至*設定*>*全域設定*>*災難恢復*。

2. 取消選擇*啟用災難恢復*。
3. 按一下「 * 套用 * 」。
4. 按一下「監控>*工作*」來確認DR工作是否已啟用。

完成後

您可以使用SnapCenter UI或下列Cmdlet刪除在容錯移轉期間建立的SQL Server備份的現象：「移除-短型RFailoverBackups」

版權資訊

Copyright © 2026 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。