准备安装适用于 Microsoft SQL Server 的SnapCenter插件

SnapCenter software

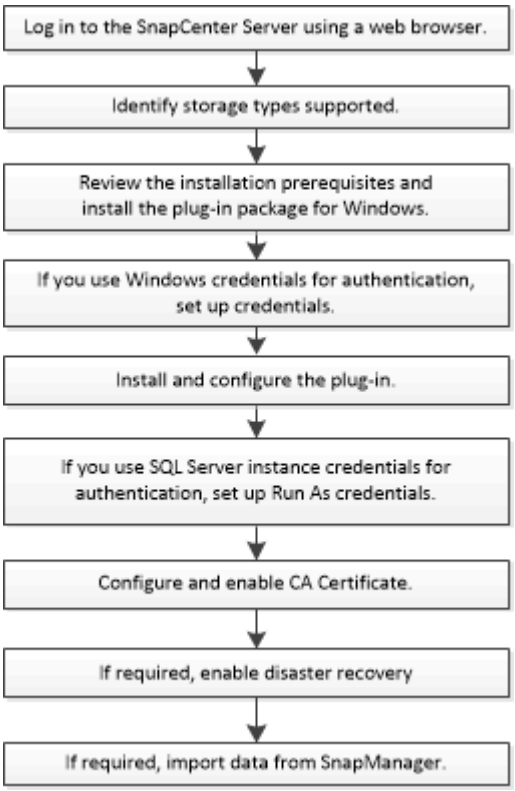
NetApp
November 06, 2025

目录

准备安装适用于 Microsoft SQL Server 的SnapCenter插件

SnapCenter Plug-in for Microsoft SQL Server 的安装工作流程

如果您想保护 SQL Server 数据库，则应该安装并设置适用于 Microsoft SQL Server 的SnapCenter插件。



添加主机并安装适用于 Microsoft SQL Server 的SnapCenter插件的先决条件

在添加主机和安装插件包之前，您必须完成所有要求。

- 如果您正在使用 iSCSI，则 iSCSI 服务必须正在运行。
- 您必须拥有具有本地管理员权限的用户，并且该用户在远程主机上具有本地登录权限。
- 如果您在SnapCenter中管理集群节点，则必须拥有对集群中所有节点具有管理权限的用户。
- 您必须拥有在 SQL Server 上具有 sysadmin 权限的用户。

  适用于 Microsoft SQL Server 的SnapCenter插件使用 Microsoft VDI 框架，该框架需要系统管理员访问权限。

  "Microsoft 支持文章 2926557：SQL Server VDI 备份和还原操作需要 Sysadmin 权限"

- 在 Windows 主机上安装插件时，如果指定非内置的凭据或用户属于本地工作组用户，则必须在主机上禁用 UAC。
- 如果安装了SnapManager for Microsoft SQL Server，则必须停止或禁用该服务和计划。

  如果您计划将备份或克隆作业导入SnapCenter，请不要卸载SnapManager for Microsoft SQL Server。

- 主机必须能够解析为服务器的完全限定域名 (FQDN)。

  如果修改了 hosts 文件以使其可解析，并且在 hosts 文件中指定了短名称和 FQDN，则在SnapCenter hosts 文件中创建一个条目，格式如下：<ip_address> <host_fqdn> <host_name>

安装适用于 **Windows** 的**SnapCenter**插件包的主机要求

在安装适用于 Windows 的SnapCenter插件包之前，您应该熟悉一些基本的主机系统空间要求和大小要求。

物品	要求
操作系统	Microsoft Windows 有关受支持版本的最新信息，请参阅 "NetApp 互操作性表工具"。
主机上SnapCenter插件的最小 RAM	1 GB
主机上SnapCenter插件的最小安装和日志空间	5 GB 您应该分配足够的磁盘空间并监控日志文件夹的存储消耗。所需的日志空间取决于要保护的实体的数量和数据保护操作的频率。如果没有足够的磁盘空间，则不会为最近运行的操作创建日志。

物品	要求
所需的软件包	• ASP.NET Core Runtime 8.0.12（以及所有后续 8.0.x 补丁）托管包 • PowerShell 核心 7.4.2 • Java 11 Oracle Java 和 OpenJDK Java 11 Oracle Java 和 OpenJDK 仅适用于 SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp支持的插件以及可安装在 Windows 主机上的其他自定义应用程序。 有关受支持版本的最新信息，请参阅 "NetApp 互操作性表工具"。 有关 .NET 特定的故障排除信息，请参阅 "对于没有互联网连接的传统系统， SnapCenter升级或安装将失败。"

为 Windows 的SnapCenter插件包设置凭据

SnapCenter使用凭据对SnapCenter操作的用户进行身份验证。您应该创建用于安装SnapCenter插件的凭据以及用于在数据库或 Windows 文件系统上执行数据保护操作的附加凭据。

开始之前

- 在安装插件之前，您必须设置 Windows 凭据。
- 您必须设置具有管理员权限的凭据，包括远程主机上的管理员权限。
- Windows 主机上的 SQL 身份验证

  安装插件后，您必须设置 SQL 凭据。

  如果您正在为 Microsoft SQL Server 部署SnapCenter插件，则必须在安装插件后设置 SQL 凭据。为具有 SQL Server sysadmin 权限的用户设置凭据。

  SQL 身份验证方法针对 SQL Server 实例进行身份验证。这意味着必须在SnapCenter中发现 SQL Server 实例。因此，添加SQL凭证前，必须先添加主机、安装插件包、刷新资源。您需要 SQL Server 身份验证才能执行诸如调度或发现资源之类的操作。

步骤

1. 在左侧导航窗格中，单击“设置”。
2. 在“设置”页面中，单击“凭据”。
3. 单击“新建”。
4. 在“凭据”页面中，指定配置凭据所需的信息：

对于这个领域...	操作
凭证名称	输入凭证的名称。
用户名/密码	输入用于身份验证的用户名和密码。 • 域管理员 指定要安装SnapCenter插件的系统上的域管理员。用户名字段的有效格式为： ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • 本地管理员（仅适用于工作组） 对于属于工作组的系统，请在要安装SnapCenter插件的系统上指定内置的本地管理员。如果用户帐户具有提升的权限或主机系统上禁用了用户访问控制功能，则可以指定属于本地管理员组的本地用户帐户。用户名字段的有效格式为：`UserName` 请勿在密码中使用双引号（“）或反引号（`）。密码中不应同时使用小于号 (<) 和感叹号 (!) 符号。例如，lessthan<!10、lessthan10<!、backtick`12。
认证模式	选择您想要使用的身份验证模式。如果选择SQL身份验证模式，还必须指定SQL服务器实例以及SQL实例所在的主机。

5. 单击“确定”。

完成凭证设置后，您可能希望在“用户和访问”页面中将凭证维护分配给用户或用户组。

为单个 SQL Server 资源配置凭据

您可以配置凭据来为每个用户在单独的 SQL Server 资源上执行数据保护作业。虽然您可以全局配置凭据，但您可能只想针对特定资源执行此操作。

关于此任务

- 如果您使用 Windows 凭据进行身份验证，则必须在安装插件之前设置您的凭据。

  但是，如果您使用 SQL Server 实例进行身份验证，则必须在安装插件后添加凭据。

- 如果您在设置凭据时启用了 SQL 身份验证，则发现的实例或数据库将显示红色挂锁图标。

  如果出现挂锁图标，则必须指定实例或数据库凭据才能成功将实例或数据库添加到资源组。

- 当满足以下条件时，您必须将凭据分配给没有 sysadmin 访问权限的基于角色的访问控制 (RBAC) 用户：
  - 凭据已分配给 SQL 实例。
  - SQL 实例或主机被分配给 RBAC 用户。

    用户必须同时拥有资源组和备份权限。

步骤 1：添加并配置凭据

1. 在左侧导航窗格中，选择“设置”。
2. 在设置页面中，选择*凭证*。
   a. 要添加新凭证，请选择“新建”。
   b. 在凭证页面中，配置凭证：

对于这个领域...	操作
凭证名称	输入凭证的名称。
用户名	输入用于 SQL Server 身份验证的用户名。 • 域管理员或管理员组的任何成员 指定要安装SnapCenter插件的系统上的域管理员或管理员组的任何成员。“用户名”字段的有效格式为： ◦ *NetBIOS*\用户名 ◦ 域 *FQDN*\用户名 • 本地管理员（仅限工作组）对于属于工作组的系统，请在要安装SnapCenter插件的系统上指定内置的本地管理员。如果用户帐户具有提升的权限或主机系统上禁用了用户访问控制功能，则可以指定属于本地管理员组的本地用户帐户。 用户名 字段的有效格式为：*UserName*
密码	输入用于身份验证的密码。
认证方式	选择 SQL Server 身份验证模式。如果 Windows 用户在 SQL 服务器上具有 sysadmin 权限，您还可以选择 Windows 身份验证。
主机	选择主机。
SQL Server 实例	选择 SQL Server 实例。

   c. 选择“确定”添加凭证。

步骤 2：配置实例

1. 在左侧导航窗格中，选择“资源”。
2. 在资源页面中，从*查看*列表中选择*实例*。

a. 选择 image::../media/filter_icon.png[过滤器图标]，然后选择主机名来过滤实例。

b. 选择 image::../media/filter_icon.png[filter icon] 以关闭过滤器窗格。

3. 在实例保护页面中，保护实例，如果需要，选择*配置凭证*。

   如果登录到SnapCenter服务器的用户无权访问 Microsoft SQL Server 的SnapCenter插件，则用户必须配置凭据。

   凭据选项不适用于数据库和可用性组。

4. 选择*刷新资源*。

在 Windows Server 2016 或更高版本上配置 gMSA

Windows Server 2016 或更高版本允许您创建组托管服务帐户 (gMSA)，该帐户从托管域帐户提供自动服务帐户密码管理。

开始之前

- 您应该拥有 Windows Server 2016 或更高版本的域控制器。
- 您应该拥有一个 Windows Server 2016 或更高版本的主机，它是域的成员。

步骤

1. 创建 KDS 根密钥来为 gMSA 中的每个对象生成唯一的密码。
2. 对于每个域，从 Windows 域控制器运行以下命令：Add-KDSRootKey -EffectiveImmediately
3. 创建并配置 gMSA：

   a. 创建用户组账号，格式如下：

   ```
    domainName\accountName$
   .. 将计算机对象添加到组中。
   .. 使用您刚刚创建的用户组来创建 gMSA。
   ```

   例如，

   ```
    New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
   -PrincipalsAllowedToRetrieveManagedPassword <group>
   -ServicePrincipalNames <SPN1,SPN2,…>
   .. 跑步 `Get-ADServiceAccount`命令来验证服务帐户。
   ```

4. 在您的主机上配置 gMSA：

   a. 在要使用 gMSA 帐户的主机上启用 Windows PowerShell 的 Active Directory 模块。

      为此，请从 PowerShell 运行以下命令：

```
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. 重新启动主机。

b. 通过从 PowerShell 命令提示符运行以下命令在主机上安装 gMSA： `Install-AdServiceAccount <gMSA>`

c. 通过运行以下命令验证你的 gMSA 帐户： `Test-AdServiceAccount <gMSA>`

5. 将管理权限分配给主机上配置的 gMSA。
6. 通过在SnapCenter服务器中指定配置的 gMSA 帐户来添加 Windows 主机。

SnapCenter Server 将在主机上安装选定的插件，并且指定的 gMSA 将在插件安装期间用作服务登录帐户。

为 Microsoft SQL Server 安装SnapCenter插件

添加主机并安装适用于 Windows 的SnapCenter插件包

您必须使用SnapCenter *添加主机*页面来添加主机并安装插件包。插件会自动安装在远程主机上。

开始之前

- 如果SnapCenter Server 主机的操作系统是 Windows 2019，而插件主机的操作系统是 Windows 2022，则应执行以下操作：
  - 升级到 Windows Server 2019（操作系统内部版本 17763.5936）或更高版本
  - 升级到 Windows Server 2022（操作系统内部版本 20348.2402）或更高版本
- 您必须是分配有插件安装和卸载权限的角色的用户，例如SnapCenter管理员角色。
- 在 Windows 主机上安装插件时，如果指定非内置的凭据，则应在主机上禁用 UAC。
- 您应该确保消息队列服务处于运行状态。

- 如果您使用组托管服务帐户 (gMSA)，则应使用管理权限配置 gMSA。

  "在 Windows Server 2016 或更高版本上为 SQL 配置组托管服务帐户"

关于此任务

您不能将SnapCenter服务器作为插件主机添加到另一个SnapCenter服务器。

您可以添加主机并为单个主机或集群安装插件包。如果您在群集或 Windows Server 故障转移群集 (WSFC) 上安装插件，则插件将安装在群集的所有节点上。

有关管理主机的信息，请参阅"管理主机"。

步骤

1. 在左侧导航窗格中，选择*主机*。
2. 验证顶部的“托管主机”选项卡是否被选中。
3. 选择“添加”。
4. 在“主机”页面中执行以下操作：

对于这个领域...	操作
主机类型	选择 Windows 作为主机类型。 SnapCenter服务器添加主机，然后安装适用于 Windows 的插件（如果主机上尚未安装该插件）。 如果您在“插件”页面上选择“Microsoft SQL Server”选项， SnapCenter服务器将安装 SQL Server 插件。
主机名	输入主机的完全限定域名 (FQDN) 或 IP 地址。仅当 IP 地址解析为 FQDN 时，不受信任的域主机才支持该 IP 地址。 SnapCenter依赖于 DNS 的正确配置。因此，最佳做法是输入 FQDN。 您可以输入以下之一的 IP 地址或 FQDN： • 独立主机 • WSFC 如果您使用SnapCenter添加主机并且该主机是子域的一部分，则必须提供 FQDN。

对于这个领域...	操作
凭据	选择您创建的凭证名称或创建新的凭证。该凭证必须具有远程主机的管理权限。有关详细信息，请参阅有关创建凭证的信息。 您可以将光标置于指定的凭证名称上来查看有关凭证的详细信息。 凭据身份验证模式由您在添加主机向导中指定的主机类型决定。

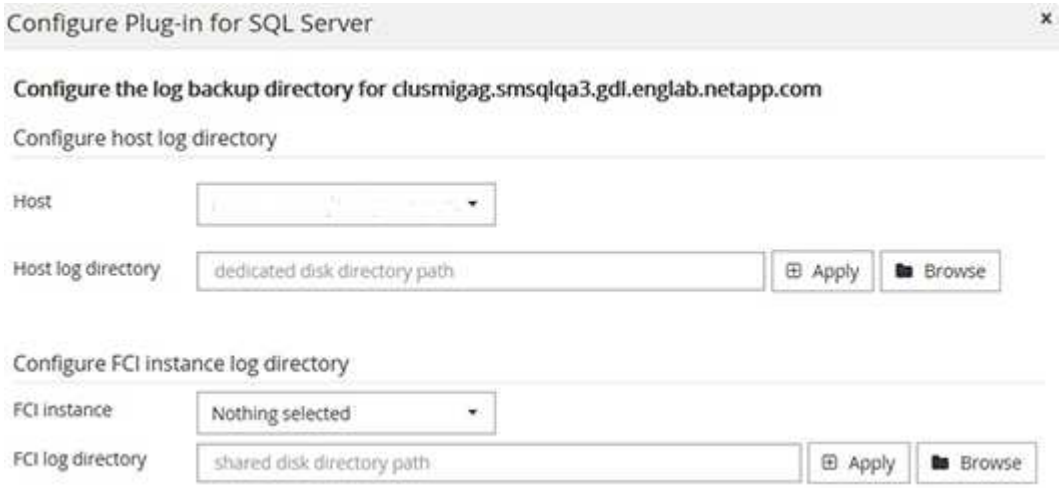
5. 在*选择要安装的插件*部分中，选择要安装的插件。
6. 选择*更多选项*。

对于这个领域...	操作
端口	保留默认端口号或指定端口号。默认端口号是 8145 如果SnapCenter服务器安装在自定义端口上，则该端口号将显示为默认端口。 如果您手动安装了插件并指定了自定义端口，则必须指定相同的端口。否则，操作失败。
安装路径	默认路径为 C:\Program Files\ NetApp\ SnapCenter。您可以选择自定义路径。
添加集群中的所有主机	选中此复选框可添加 WSFC 或 SQL 可用性组中的所有集群节点。如果您想管理和识别集群内的多个可用的 SQL 可用性组，则应该通过选择 GUI 中的相应集群复选框来添加所有集群节点。
跳过预安装检查	如果您已经手动安装了插件并且不想验证主机是否满足安装插件的要求，请选中此复选框。
使用组托管服务帐户 (gMSA) 运行插件服务	如果要使用组托管服务帐户 (gMSA) 来运行插件服务，请选中此复选框。 以以下格式提供 gMSA 名称：domainName\accountName$。 如果主机添加了 gMSA，并且 gMSA 具有登录和系统管理员权限，则 gMSA 将用于连接到 SQL 实例。

7. 选择*提交*。

8. 对于SQL插件，选择主机来配置日志目录。
   a. 选择*配置日志目录*，在配置主机日志目录页面中选择*浏览*并完成以下步骤：

      仅列出NetApp LUN（驱动器）以供选择。 SnapCenter在备份操作过程中备份并复制主机日志目录。



      i. 选择主机上将存储主机日志的驱动器号或挂载点。
      ii. 如果需要，选择一个子目录。
      iii. 选择*保存*。
9. 选择*提交*。

   如果您未选中“跳过预检查”复选框，则会验证主机是否满足安装插件的要求。系统会根据最低要求验证磁盘空间、RAM、PowerShell 版本、.NET 版本、位置（对于 Windows 插件）和 Java 版本（对于 Linux 插件）。如果不满足最低要求，则会显示相应的错误或警告消息。

   如果错误与磁盘空间或 RAM 有关，您可以更新位于 C:\Program Files\ NetApp\ SnapCenter WebApp 的 web.config 文件以修改默认值。如果错误与其他参数有关，则必须修复该问题。

   在 HA 设置中，如果您要更新 web.config 文件，则必须在两个节点上更新该文件。
10. 监控安装进度。

使用 **cmdlet** 在多个远程主机上安装适用于 **Microsoft SQL Server** 的**SnapCenter**插件

您可以使用 Install-SmHostPackage PowerShell cmdlet 同时在多个主机上安装适用于 Microsoft SQL Server 的SnapCenter插件。

开始之前

您必须以域用户身份登录到SnapCenter ，并在要安装插件包的每个主机上拥有本地管理员权限。

步骤

1. 启动 PowerShell。
2. 在SnapCenter Server 主机上，使用 Open-SmConnection cmdlet 建立会话，然后输入您的凭据。
3. 使用 Install-SmHostPackage cmdlet 和所需参数在多个远程主机上安装适用于 Microsoft SQL Server

的SnapCenter插件。

可以通过运行_Get-Help command_name_来获取有关可与 cmdlet 一起使用的参数及其描述的信息。或者，您也可以参考 "SnapCenter软件 Cmdlet 参考指南"。

当您已经手动安装了插件并且不想验证主机是否满足安装插件的要求时，可以使用 -skipprecheck 选项。

4. 输入您的远程安装凭据。

从命令行静默安装适用于 **Microsoft SQL Server** 的**SnapCenter**插件

您应该从SnapCenter用户界面中安装适用于 Microsoft SQL Server 的SnapCenter插件。但是，如果由于某种原因您无法这样做，您可以从 Windows 命令行以静默模式无人值守运行 SQL Server 插件安装程序。

开始之前

- 安装之前，您必须删除适用于 Microsoft SQL Server 的早期版本的SnapCenter插件。

  有关更多信息，请参阅 "如何从插件主机手动直接安装SnapCenter插件" 。

步骤

1. 验证插件主机上是否存在 C:\temp 文件夹以及登录用户是否对该文件夹具有完全访问权限。
2. 从 C:\ProgramData\ NetApp\ SnapCenter\Package Repository 下载 SQL Server 软件插件。

   可以从安装SnapCenter服务器的主机访问此路径。

3. 将安装文件复制到要安装插件的主机上。
4. 从本地主机上的 Windows 命令提示符，导航到保存插件安装文件的目录。
5. 安装 SQL Server 软件插件：

   ```
   "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
   ```

   用您的数据替换占位符值

   - Debug_Log_Path 是套件安装程序日志文件的名称和位置。
   - Log_Path 是插件组件（SCW、SCSQL 和 SMCore）的安装日志的位置。
   - Num 是SnapCenter与 SMCore 通信的端口
   - Install_Directory_Path是主机插件包安装目录。
   - domain\administrator 是适用于 Microsoft Windows Web 服务帐户的SnapCenter插件。
   - password 是 Microsoft Windows Web 服务帐户的SnapCenter插件的密码。+
     ```
     "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
```

安装 SQL Server 插件期间传递的所有参数都区分大小写。

6. 监视 Windows 任务计划程序、主安装日志文件 C:\Installdebug.log 以及 C:\Temp 中的附加安装文件。
7. 监视 %temp% 目录以验证 msiexe.exe 安装程序是否正在无错误地安装软件。

SQL Server 插件的安装在主机上注册该插件，而不是在SnapCenter服务器上注册。您可以通过使用SnapCenter GUI 或 PowerShell cmdlet 添加主机在SnapCenter服务器上注册插件。添加主机后，会自动发现插件。

监控 SQL Server 插件的安装状态

您可以使用“作业”页面监控SnapCenter插件包的安装进度。您可能需要检查安装进度以确定安装何时完成或是否存在问题。

关于此任务

以下图标出现在“作业”页面上并指示操作的状态：

- 进行中
- 成功完成
- 失败的
- 已完成但有警告，或由于警告而无法启动
- 排队

步骤

1. 在左侧导航窗格中，单击“监控”。
2. 在“监控”页面中，单击“作业”。
3. 在 **Jobs** 页面中，要过滤列表以便仅列出插件安装操作，请执行以下操作：
   a. 单击“过滤器”。
   b. 可选：指定开始日期和结束日期。
   c. 从类型下拉菜单中，选择*插件安装*。
   d. 从状态下拉菜单中，选择安装状态。
   e. 单击“应用”。
4. 选择安装作业并单击*详细信息*以查看作业详细信息。
5. 在“作业详情”页面中，单击“查看日志”。

配置 CA 证书

生成CA证书CSR文件

您可以生成证书签名请求 (CSR) 并导入可使用生成的 CSR 从证书颁发机构 (CA) 获取的证书。该证书将有一个与之关联的私钥。

CSR 是一段编码文本，提供给授权证书供应商以获取签名的 CA 证书。

CA 证书 RSA 密钥长度必须至少为 3072 位。

有关生成 CSR 的信息，请参阅 "如何生成CA证书CSR文件"。

如果您拥有您的域（*.domain.company.com）或您的系统（machine1.domain.company.com）的 CA 证书，您可以跳过生成 CA 证书 CSR 文件。您可以使用SnapCenter部署现有的 CA 证书。

对于集群配置，CA 证书中应提及集群名称（虚拟集群 FQDN）和相应的主机名。在获取证书之前，可以通过填写主题备用名称 (SAN) 字段来更新证书。对于通配符证书（*.domain.company.com），该证书将隐式包含域的所有主机名。

导入 CA 证书

您必须使用 Microsoft 管理控制台 (MMC) 将 CA 证书导入SnapCenter服务器和 Windows 主机插件。

步骤

1. 转到 Microsoft 管理控制台 (MMC)，然后单击 文件 > 添加/删除管理单元。
2. 在“添加或删除管理单元”窗口中，选择“证书”，然后单击“添加”。
3. 在证书管理单元窗口中，选择“计算机帐户”选项，然后单击“完成”。
4. 单击 控制台根 > 证书 - 本地计算机 > 受信任的根证书颁发机构 > 证书。
5. 右键单击文件夹“受信任的根证书颁发机构”，然后选择*所有任务*>*导入*以启动导入向导。
6. 完成向导，如下所示：

在此向导窗口中...	执行以下操作...
导入私钥	选择选项*是*，导入私钥，然后单击*下一步*。
导入文件格式	不做任何更改；单击“下一步”。
安全性	指定导出证书要使用的新密码，然后单击“下一步”。
完成证书导入向导	查看摘要，然后单击“完成”开始导入。

导入证书时需携带私钥（支持格式为：**.pfx**、.p12、*.p7b）。

7. 对“个人”文件夹重复步骤 5。

获取 **CA** 证书指纹

证书指纹是用于标识证书的十六进制字符串。指纹是使用指纹算法根据证书内容计算出来的。

步骤

1. 在 GUI 上执行以下操作：
   a. 双击该证书。
   b. 在证书对话框中，单击“详细信息”选项卡。
   c. 滚动浏览字段列表并单击“指纹”。
   d. 从框中复制十六进制字符。
   e. 删除十六进制数之间的空格。

      例如，如果指纹为：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，删除空格后，将为：“a909502dd82ae41433e6f83886b00d4277a32a7b”。

2. 从 PowerShell 执行以下操作：
   a. 运行以下命令列出已安装证书的指纹并通过主题名称识别最近安装的证书。

      Get-ChildItem -Path 证书*:\LocalMachine\My*

   b. 复制指纹。

使用 **Windows** 主机插件服务配置 **CA** 证书

您应该使用 Windows 主机插件服务配置 CA 证书以激活已安装的数字证书。

在SnapCenter服务器和所有已部署 CA 证书的插件主机上执行以下步骤。

步骤

1. 通过运行以下命令删除与 SMCore 默认端口 8145 的现有证书绑定：

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

   例如：

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

. 通过运行以下命令将新安装的证书与 Windows 主机插件服务绑定：

```
> $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"
```

为插件启用 CA 证书

您应该配置 CA 证书并在SnapCenter服务器和相应的插件主机中部署 CA 证书。您应该为插件启用 CA 证书验证。

开始之前

- 您可以使用运行_Set-SmCertificateSettings_ cmdlet 来启用或禁用 CA 证书。
- 您可以使用_Get-SmCertificateSettings_显示插件的证书状态。

可以通过运行_Get-Help command_name_来获取有关可与 cmdlet 一起使用的参数及其描述的信息。或者，您也可以参考 "SnapCenter软件 Cmdlet 参考指南"。

步骤

1. 在左侧导航窗格中，单击“主机”。
2. 在“主机”页面中，单击“托管主机”。
3. 选择单个或多个插件主机。
4. 单击“更多选项”。
5. 选择*启用证书验证*。

完成后

托管主机选项卡主机显示一个挂锁，挂锁的颜色表示SnapCenter服务器和插件主机之间的连接状态。

- * * 表示 CA 证书未启用或未分配给插件主机。
- * * 表示 CA 证书验证成功。
- * * 表示无法验证 CA 证书。
- * * 表示无法检索连接信息。

当状态为黄色或绿色时，表示数据保护操作成功完成。

配置灾难恢复

SnapCenter插件 for SQL Server 的灾难恢复

当 SQL Server 的SnapCenter插件关闭时，请使用以下步骤切换到其他 SQL 主机并恢复数据。

开始之前

- 辅助主机应具有与主主机相同的操作系统、应用程序和主机名。
- 使用“添加主机”或“修改主机”页面将 SQL Server 的SnapCenter插件推送到备用主机。看"管理主机"了解更多信息。

步骤

1. 从“主机”页面中选择主机来修改并安装 SQL Server 的SnapCenter插件。
2. （可选）将 SQL Server 配置文件的SnapCenter插件从灾难恢复 (DR) 备份替换到新计算机。
3. 从 DR 备份中的 SQL Server 文件夹的SnapCenter插件导入 Windows 和 SQL 计划。

相关信息

查看"灾难恢复 API"视频。

SnapCenter Plug-in for SQL Server 的存储灾难恢复 (DR)

您可以通过在“全局设置”页面中启用存储的 DR 模式来恢复用于 SQL Server 存储的SnapCenter插件。

开始之前

- 确保插件处于维护模式。
- 中断SnapMirror/ SnapVault关系。"中断SnapMirror关系"
- 将从属磁盘的 LUN 连接到具有相同驱动器号的主机。
- 确保所有磁盘都使用 DR 之前使用的相同驱动器号进行连接。
- 重新启动 MSSQL 服务器服务。
- 确保 SQL 资源重新联机。

关于此任务

VMDK 和 RDM 配置不支持灾难恢复 (DR)。

步骤

1. 在“设置”页面中，导航至“设置”>“全局设置”>“灾难恢复”。
2. 选择“启用灾难恢复”。
3. 单击“应用”。
4. 单击“监控”>“作业”来验证 DR 作业是否已启用。

完成后

- 如果故障转移后创建了新的数据库，则数据库将处于非 DR 模式。

  新的数据库将像故障转移之前一样继续运行。

- 在 DR 模式下创建的新备份将在拓扑页面中的SnapMirror或SnapVault （辅助）下列出。

  新备份旁边会显示一个“i”图标，表示这些备份是在 DR 模式期间创建的。

- 您可以使用 UI 或以下 cmdlet 删除故障转移期间创建的 SQL Server 备份的SnapCenter插件： `Remove-SmBackup`
- 故障转移后，如果您希望某些资源处于非 DR 模式，请使用以下 cmdlet： `Remove-SmResourceDRMode`

  更多信息请参阅 "SnapCenter软件 Cmdlet 参考指南"。

- SnapCenter Server 将管理处于 DR 或非 DR 模式的单个存储资源（SQL 数据库），但不管理处于 DR 模式或非 DR 模式的存储资源的资源组。

从 SQL Server 二级存储的SnapCenter插件故障恢复到主存储

在 SQL Server 主存储的SnapCenter插件恢复联机后，您应该故障恢复到主存储。

开始之前

- 从托管主机页面将 SQL Server 的SnapCenter插件置于*维护*模式。
- 断开辅助存储与主机的连接并从主存储进行连接。
- 要故障恢复到主存储，请通过执行反向重新同步操作确保关系方向与故障转移之前保持相同。

  为了在反向重新同步操作后保留主存储和辅助存储的角色，请再次执行反向重新同步操作。

  更多信息请参见"反向重新同步镜像关系"

- 重新启动 MSSQL 服务器服务。
- 确保 SQL 资源重新联机。

> 在插件故障转移或故障回复期间，插件整体状态不会立即刷新。主机和插件的整体状态在后续的主机刷新操作中更新。

步骤

1. 在“设置”页面中，导航至“设置”>“全局设置”>“灾难恢复”。
2. 取消选择“启用灾难恢复”。
3. 单击“应用”。
4. 单击“监控”>“作业”来验证 DR 作业是否已启用。

完成后

您可以使用 UI 或以下 cmdlet 删除故障转移期间创建的 SQL Server 备份的SnapCenter插件： `Remove-SmDRFailoverBackups`