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

SnapCenter Software 4.7

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/snapcenter-47/protect-scsql/task_install_snapcenter_plug_in_for_microsoft_sql_server_database.html on September 26, 2025. Always check docs.netapp.com for the latest.

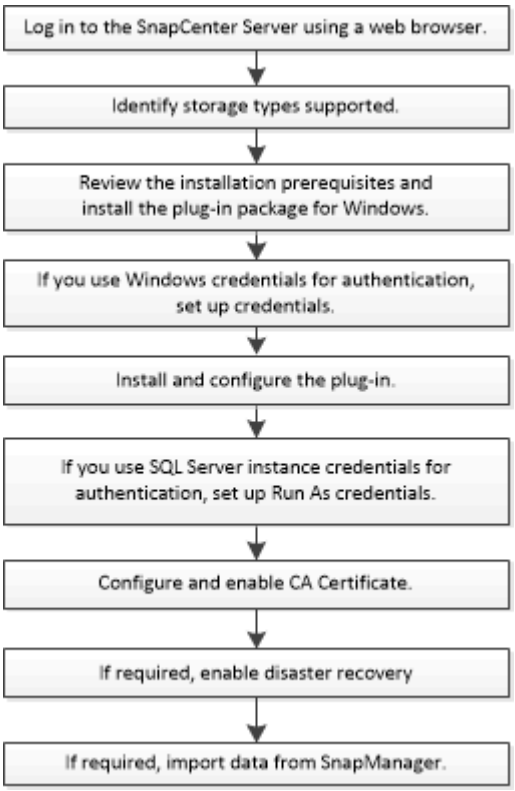
目录

准备安装适用于 Microsoft SQL Server 的 SnapCenter 插件 1
适用于 Microsoft SQL Server 的 SnapCenter 插件的安装工作流 1
添加主机和安装适用于 Microsoft SQL Server 的 SnapCenter 插件的前提条件 1
安装适用于 Windows 的 SnapCenter 插件软件包的主机要求 2
设置适用于 Windows 的 SnapCenter 插件软件包的凭据 2
配置单个 SQL Server 资源的凭据 4
在 Windows Server 2012 或更高版本上配置 GMSA 6
安装适用于 Microsoft SQL Server 的 SnapCenter 插件 7
添加主机并安装适用于 Windows 的 SnapCenter 插件软件包 7
使用 cmdlet 在多个远程主机上安装适用于 Microsoft SQL Server 的 SnapCenter 插件 10
通过命令行以静默方式安装适用于 Microsoft SQL Server 的 SnapCenter 插件 11
监控适用于 SQL Server 的插件的安装状态 12
配置 CA 证书 12
生成 CA 证书 CSR 文件 13
导入 CA 证书 13
获取 CA 证书指纹 14
使用 Windows 主机插件服务配置 CA 证书 14
为插件启用 CA 证书 15
配置灾难恢复 15
适用于 SQL Server 的 SnapCenter 插件的灾难恢复 15
适用于 SQL Server 的 SnapCenter 插件的存储灾难恢复（ DR ） 16
从适用于 SQL Server 的 SnapCenter 插件二级存储故障恢复到主存储 17

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

适用于 Microsoft SQL Server 的 SnapCenter 插件的安装工作流

如果要保护 SQL Server 数据库，应安装和设置适用于 Microsoft SQL Server 的 SnapCenter 插件。



添加主机和安装适用于 Microsoft SQL Server 的 SnapCenter 插件的前提条件

在添加主机并安装插件软件包之前，您必须满足所有要求。

- 如果使用的是 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，并在远程主机上拥有本地登录权限。
- 如果您在 SnapCenter 中管理集群节点，则必须具有对集群中所有节点具有管理权限的用户。
- 您必须具有对 SQL Server 具有 sysadmin 权限的用户。

  适用于 Microsoft SQL Server 的 SnapCenter 插件使用 Microsoft VDI Framework ，这需要 sysadmin 访问权限。

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

- 在 Windows 主机上安装插件时，如果您指定的凭据不是内置的，或者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 ，则必须已停止或禁用此服务和计划。
- 主机必须可从服务器解析为完全限定域名（ FQDN ）。

  如果修改了 hosts 文件以使其可解析，并且在 hosts 文件中同时指定了短名称和 FQDN ，请在 SnapCenter hosts 文件中按以下格式创建一个条目： <IP_address> <host_FQDN> <host_name>

安装适用于 Windows 的 SnapCenter 插件软件包的主机要求

在安装适用于 Windows 的 SnapCenter 插件软件包之前，您应熟悉一些基本的主机系统空间要求和规模估算要求。

项目	要求
操作系统	Microsoft Windows 有关受支持版本的最新信息，请参见 "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 您应分配足够的磁盘空间并通过 logs 文件夹监控存储消耗。所需的日志空间因要保护的实体数量和数据保护操作的频率而异。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。
所需的软件包	• Microsoft .NET Framework 4.7.2或更高版本 • Windows Management Framework （ WMF ） 4.0 或更高版本 • PowerShell 4.0 或更高版本 有关受支持版本的最新信息，请参见 "NetApp 互操作性表工具"。 有关.NET疑难解答的信息、请参阅 "对于没有Internet连接的原有系统、SnapCenter 升级或安装失败"。

设置适用于 Windows 的 SnapCenter 插件软件包的凭据

SnapCenter 使用凭据对 SnapCenter 操作的用户进行身份验证。您应创建用于安装 SnapCenter 插件的凭据以及用于对数据库或 Windows 文件系统执行数据保护操作的其他

凭据。

- 您需要的内容 *
- 在安装插件之前，您必须设置 Windows 凭据。
- 您必须使用管理员权限设置凭据，包括对远程主机的管理员权限。
- Windows 主机上的 SQL 身份验证

  您必须在安装插件后设置 SQL 凭据。

  如果要部署适用于 Microsoft SQL Server 的 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，在添加 SQL 凭据之前，您必须添加主机，安装插件软件包并刷新资源。要执行计划或发现资源等操作，您需要进行 SQL Server 身份验证。

- 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：

对于此字段 ...	执行此操作 ...
凭据名称	输入凭据的名称。

对于此字段 ...	执行此操作 ...
用户名 / 密码	输入要用于身份验证的用户名和密码。 • 域管理员 在要安装 SnapCenter 插件的系统上指定域管理员。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，请指定要安装 SnapCenter 插件的系统上的内置本地管理员。如果用户帐户具有提升的权限或在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(")或反勾号(`)。不应使用小于(<)和感叹号(！) 密码中的符号。例如、小于<！10、小于10<！、回退键`12。
身份验证模式	选择要使用的身份验证模式。如果选择 SQL 身份验证模式，则还必须指定 SQL Server 实例和 SQL 实例所在的主机。

5. 单击 * 确定 * 。

完成凭据设置后，您可能需要在 " 用户和访问 " 页面中为用户或用户组分配凭据维护。

配置单个 SQL Server 资源的凭据

您可以配置凭据，以便对每个用户的单个 SQL Server 资源执行数据保护作业。虽然您可以全局配置凭据，但可能只想对特定资源执行此操作。

- 关于此任务 *
- 如果使用 Windows 凭据进行身份验证，则必须在安装插件之前设置凭据。

  但是，如果使用 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一个红色挂锁图标。

  如果显示挂锁图标，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。

- 满足以下条件时，必须将凭据分配给不具有 sysadmin 访问权限的基于角色的访问控制（ Role-Based Access Control ， RBAC ）用户：

- 此凭据将分配给 SQL 实例。
- SQL 实例或主机已分配给 RBAC 用户。

  用户必须同时具有资源组和备份权限

- 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. 要添加新凭据，请单击 * 新建 * 。
4. 在凭据页面中，配置凭据：

对于此字段 ...	执行此操作 ...
• 凭据名称 *	输入凭据的名称。
• 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\username* ◦ 域 FQDN\username_ • 本地管理员（仅适用于工作组）对于属于工作组的系统，请指定要安装 SnapCenter 插件的系统上的内置本地管理员。如果用户帐户具有提升的权限或在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。
• 身份验证模式 *	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，您也可以选择 Windows 身份验证。
• 主机 *	选择主机。
• SQL Server 实例 *	选择 SQL Server 实例。

5. 单击 * 确定 * 以添加凭据。
6. 在左侧导航窗格中，单击 * 资源 * 。
7. 在资源页面中，从 * 视图 * 列表中选择 * 实例 * 。

a. 单击，然后选择要筛选实例的主机名。

b. 单击 以关闭筛选器窗格。

8. 在实例保护页面中，保护实例，如果需要，请单击 * 配置凭据 * 。

   如果登录到 SnapCenter 服务器的用户无法访问适用于 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。

1. 单击 * 刷新资源 * 。

在 Windows Server 2012 或更高版本上配置 GMSA

通过 Windows Server 2012 或更高版本，您可以创建组托管服务帐户（ GMSA ），以便从受管域帐户自动管理服务帐户密码。

- 您需要的内容 *
- 您应具有 Windows Server 2012 或更高版本的域控制器。
- 您应该拥有一个 Windows Server 2012 或更高版本的主机，该主机是域的成员。
- 步骤 *

1. 创建一个 KDS 根密钥，以便为 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. 创建和配置 GMSA ：

   a. 按以下格式创建用户组帐户：

   ```
    domainName\accountName$
   .. 向组中添加计算机对象。
   .. 使用刚刚创建的用户组创建 GMSA 。
   ```

   例如：

   ```
    New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
   <fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
   -ServicePrincipalNames <SPN1,SPN2,…>
   .. 运行 `Get-ADServiceAccount` 用于验证服务帐户的命令。
   ```

4. 在主机上配置 GMSA ：

   a. 在要使用 GMSA 帐户的主机上为 Windows PowerShell 启用 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. 在PowerShell命令提示符处运行以下命令、在主机上安装GMSA： `Install-AdServiceAccount <gMSA>`

c. 运行以下命令、验证您的GMSA帐户： `Test-AdServiceAccount <gMSA>`

1. 为主机上配置的 GMSA 分配管理权限。
2. 通过在 SnapCenter 服务器中指定已配置的 GMSA 帐户来添加 Windows 主机。

   SnapCenter 服务器将在主机上安装选定插件，并且在安装此插件期间，指定的 GMSA 将用作服务登录帐户。

安装适用于 Microsoft SQL Server 的 SnapCenter 插件

添加主机并安装适用于 Windows 的 SnapCenter 插件软件包

您必须使用 SnapCenter * 添加主机 * 页面添加主机并安装插件软件包。这些插件会自动安装在远程主机上。

- 您需要的内容 *
- 您必须是分配给具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，如果指定的凭据不是内置的，则应在主机上禁用 UAC 。
- 您应确保消息队列服务处于运行状态。
- 如果您使用的是组托管服务帐户（ GMSA ），则应使用管理权限配置 GMSA 。

  "在 Windows Server 2012 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。

您可以为单个主机或集群添加主机并安装插件软件包。如果要在集群或 Windows Server 故障转移集群（ WSFC ）上安装插件，则这些插件将安装在集群的所有节点上。

有关管理主机的信息，请参见 "管理主机"。

- 步骤 *

1. 在左侧导航窗格中，单击 * 主机 * 。
2. 验证顶部是否已选中 * 受管主机 * 选项卡。
3. 单击 * 添加 * 。
4. 在主机页面中，执行以下操作：

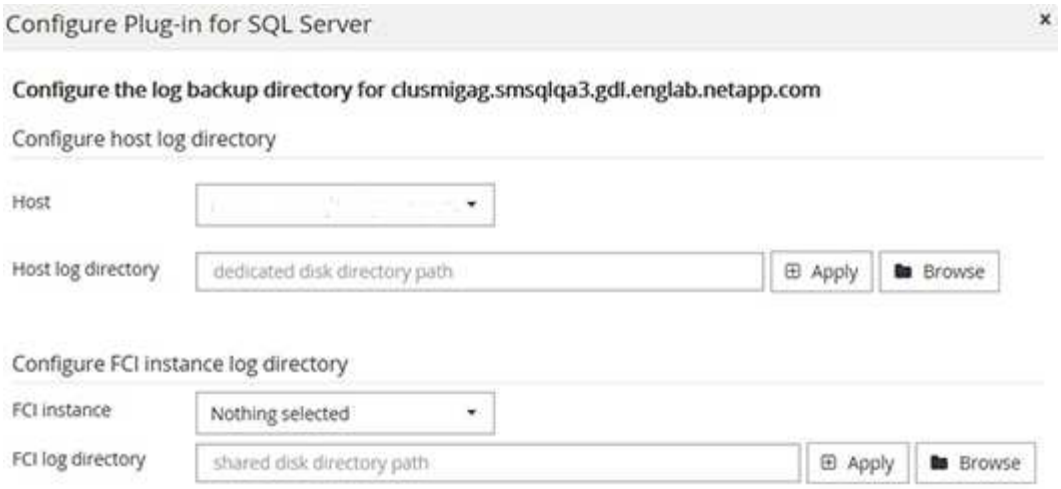
对于此字段 ...	执行此操作 ...
主机类型	选择 Windows 作为主机类型。SnapCenter 服务器会添加此主机，如果此主机上尚未安装适用于 Windows 的插件，则会安装此插件。 如果在插件页面上选择 Microsoft SQL Server 选项，则 SnapCenter 服务器将安装适用于 SQL Server 的插件。
主机名	输入主机的完全限定域名（ FQDN ）或 IP 地址。只有在将 IP 地址解析为 FQDN 时，不受信任的域主机才支持此 IP 地址。 SnapCenter 取决于 DNS 的正确配置。因此，最佳做法是输入 FQDN 。 您可以输入以下项之一的 IP 地址或 FQDN ： • 独立主机 • WSFC 如果要使用 SnapCenter 添加主机，并且此主机属于子域，则必须提供 FQDN 。
凭据	选择您创建的凭据名称或创建新凭据。凭据必须对远程主机具有管理权限。有关详细信息，请参见有关创建凭据的信息。 您可以通过将光标置于指定的凭据名称上方来查看有关凭据的详细信息。 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. 单击 * 更多选项 * 。

对于此字段 ...	执行此操作 ...
Port	保留默认端口号或指定端口号。默认端口号为 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，操作将失败。
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。如果要管理和标识集群中的多个可用 SQL 可用性组，应通过在图形用户界面中选中相应的集群复选框来添加所有集群节点。
跳过安装前检查	如果您已手动安装插件，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 ）运行插件服务，请选中此复选框。 按以下格式提供 GMSA 名称： domainname\accountName$ 。 如果使用 GMSA 添加主机，并且 GMSA 具有登录和系统管理员权限，则将使用 GMSA 连接到 SQL 实例。

7. 单击 * 提交 * 。
8. 对于 SQL 插件，选择要配置日志目录的主机。
   a. 单击 * 配置日志目录 * ，然后在配置主机日志目录页面中，单击 * 浏览 * 并完成以下步骤：

      仅列出 NetApp LUN （驱动器）以供选择。在备份操作中， SnapCenter 会备份和复制主机日志目录。



i. 选择要存储主机日志的主机上的驱动器号或挂载点。

ii. 如果需要，请选择子目录。

iii. 单击 * 保存 * 。

9. 单击 * 提交 * 。

   如果未选中 * 跳过预检 * 复选框，则主机将通过验证以验证它是否符合安装插件的要求。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）均已根据最低要求进行验证。如果不满足最低要求，则会显示相应的错误或警告消息。

   如果此错误与磁盘空间或 RAM 相关，您可以更新位于 C： \Program Files\NetApp\SnapCenter WebApp 的 web.config 文件以修改默认值。如果此错误与其他参数相关，则必须修复问题描述。

   在 HA 设置中，如果要更新 web.config 文件，则必须同时更新两个节点上的文件。

1. 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 在多个主机上同时安装适用于 Microsoft SQL Server 的 SnapCenter 插件。

- 您需要的内容 *

您必须已在要安装此插件软件包的每个主机上以具有本地管理员权限的域用户身份登录到 SnapCenter 。

- 步骤 *

1. 启动 PowerShell 。
2. 在 SnapCenter 服务器主机上，使用 Open-SmConnection cmdlet 建立会话，然后输入凭据。
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。

   有关可与 cmdlet 结合使用的参数及其说明的信息，可通过运行 *get-help command_name* 来获取。或者，您也可以参考 "《 SnapCenter 软件 cmdlet 参考指南》"。

如果您已手动安装了插件，并且不想验证主机是否满足安装插件的要求，则可以使用 -skipprecheck 选项。

1. 输入远程安装的凭据。

通过命令行以静默方式安装适用于 **Microsoft SQL Server** 的 **SnapCenter** 插件

您应从 SnapCenter 用户界面中安装适用于 Microsoft SQL Server 的 SnapCenter 插件。但是，如果由于某种原因而无法运行此插件，则可以通过 Windows 命令行在无人参与的情况下以静默模式运行适用于 SQL Server 的插件安装程序。

- 您需要的内容 *
- 在安装之前，必须删除适用于 Microsoft SQL Server 的早期版本的 SnapCenter 插件。

  有关详细信息，请参见 "如何手动或直接从插件主机安装 SnapCenter 插件"。

- 步骤 *

1. 验证插件主机上是否存在 C： \temp 文件夹，并且已登录用户是否具有对该文件夹的完全访问权限。
2. 从 C： \ProgramData\NetApp\SnapCenter\Package Repository 下载适用于 SQL Server 的插件软件。

   可以从安装了 SnapCenter 服务器的主机访问此路径。

3. 将安装文件复制到要安装此插件的主机。
4. 在本地主机上的 Windows 命令提示符处，导航到保存插件安装文件的目录。
5. 安装适用于 SQL Server 的插件软件：

   ```
   "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
   ```

   将占位值替换为数据

   - 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 ）安装日志的位置。
   - num 是 SnapCenter 与 SMCore 通信所使用的端口
   - install_Directory_Path 是主机插件软件包安装目录。
   - domain\administrator 是适用于 Microsoft Windows 的 SnapCenter 插件 Web 服务帐户。
   - password 是适用于 Microsoft Windows 的 SnapCenter 插件 Web 服务帐户的密码。+
     ```
     "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
     ```

在安装适用于 SQL Server 的插件期间传递的所有参数都区分大小写。

1. 监控 Windows 任务计划程序，主安装日志文件 C： \Installdebug.log 以及 C： \Temp 中的其他安装文件。
2. 监控 %temp% 目录，以验证 msiexe.exe 安装程序是否正在安装此软件，而不会出现错误。

适用于 SQL Server 的插件的安装会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 图形用户界面或 PowerShell cmdlet 添加主机来在 SnapCenter 服务器上注册此插件。添加主机后，系统将自动发现此插件。

监控适用于 **SQL Server** 的插件的安装状态

您可以使用作业页面监控 SnapCenter 插件软件包的安装进度。您可能需要检查安装进度以确定安装完成的时间或是否存在问题描述。

- 关于此任务 *

以下图标将显示在作业页面上，并指示操作的状态：

- 正在进行中
- 已成功完成
- 失败
- 已完成，但出现警告或由于出现警告而无法启动
- 已排队
- 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. 在作业页面中，要筛选列表以便仅列出插件安装操作，请执行以下操作：
     a. 单击 * 筛选器 * 。
     b. 可选：指定开始和结束日期。
     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. 在作业详细信息页面中，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。此证书将具有一个关联的专用密钥。

CSR 是一个编码文本块，提供给授权证书供应商以采购签名的 CA 证书。

有关生成 CSR 的信息，请参见 "如何生成 CA 证书 CSR 文件"。

如果您拥有域（ * .domain.company.com ）或系统（ machine1.domain.company.com ）的 CA 证书，则可以跳过生成 CA 证书 CSR 文件。您可以使用 SnapCenter 部署现有 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 ）以及相应的主机名。在获取证书之前，可以通过填写使用者替代名称（ SAN ）字段来更新此证书。对于通配符证书（ * .domain.company.com ），此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 证书导入到 SnapCenter 服务器和 Windows 主机插件中。

- 步骤 *
  1. 转到 Microsoft 管理控制台（ MMC ），然后单击 * 文件 * > * 添加 / 删除 Snapin * 。
  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 * > * 可信根证书颁发机构 * > * 证书 * 。
  5. 右键单击文件夹 " 可信根证书颁发机构 " ，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 * 是 * 选项，导入私钥，然后单击 * 下一步 * 。
导入文件格式	不进行任何更改；单击 * 下一步 * 。
安全性	指定要用于导出的证书的新密码，然后单击 * 下一步 * 。
正在完成证书导入向导	查看摘要，然后单击 * 完成 * 开始导入。

导入证书应与私钥捆绑在一起(支持的格式为：。**pfx**、。p12和*。p7b)。

  7. 对 "Personal" 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得出的。

- 步骤 *

1. 在 GUI 上执行以下操作：
   a. 双击证书。
   b. 在证书对话框中，单击 * 详细信息 * 选项卡。
   c. 滚动字段列表，然后单击 * 缩略图 * 。
   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" ，则在删除空格后，指纹将为 "a909502dd82ae41433e6f83886b00d4277a32a7b" 。

2. 从 PowerShell 执行以下操作：
   a. 运行以下命令以列出已安装证书的指纹，并按主题名称标识最近安装的证书。

      Get-子 项 -Path Cert ： *\LOCALLMACHINE\My*

   b. 复制指纹。

使用 **Windows** 主机插件服务配置 **CA** 证书

您应使用 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 服务器以及已部署 CA 证书的所有插件主机上执行以下步骤。

- 步骤 *

1. 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
   ```

   . 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”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

为插件启用 CA 证书

您应在 SnapCenter 服务器和相应插件主机中配置 CA 证书并部署 CA 证书。您应为插件启用 CA 证书验证。

- 您需要的内容 *
- 您可以使用 run *set-SmCertificateSettings* cmdlet 启用或禁用 CA 证书。
- 您可以使用 *Get-SmCertificateSettings* 显示插件的证书状态。

有关可与 cmdlet 结合使用的参数及其说明的信息，可通过运行 *get-help command_name* 来获取。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 * 受管主机 * 。
  3. 选择一个或多个插件主机。
  4. 单击 * 更多选项 * 。
  5. 选择 * 启用证书验证 * 。
- 完成后 *

受管主机选项卡主机会显示一个挂锁，挂锁的颜色表示 SnapCenter 服务器与插件主机之间的连接状态。

- ** 表示CA证书未启用、也未分配给插件主机。
- ** 表示CA证书已成功验证。
- ** 表示无法验证CA证书。
- ** 表示无法检索到连接信息。

如果状态为黄色或绿色，则表示数据保护操作已成功完成。

配置灾难恢复

适用于 SQL Server 的 SnapCenter 插件的灾难恢复

当适用于 SQL Server 的 SnapCenter 插件关闭时，切换到另一个 SQL 主机，并通过执行

几个步骤来恢复数据。

- 您需要的内容 *
- 二级主机应与主主机具有相同的操作系统，应用程序和主机名。
- 使用 * 添加主机 * 或 * 修改主机 * 页面将适用于 SQL Server 的 SnapCenter 插件推送到备用主机。

  "管理主机"

- 步骤 *
  1. 从 * 主机 * 页面中选择主机，以修改和安装适用于 SQL Server 的 SnapCenter 插件。
  2. （可选）将适用于 SQL Server 的 SnapCenter 插件配置文件从灾难恢复（ DR ）备份更换到新计算机。
  3. 从灾难恢复备份中的适用于 SQL Server 的 SnapCenter 插件文件夹导入 Windows 和 SQL 计划。

有关详细信息、请参见 "灾难恢复 API"视频。

适用于 **SQL Server** 的 **SnapCenter** 插件的存储灾难恢复（ **DR** ）

您可以通过在全局设置页面中启用存储的 DR 模式来恢复适用于 SQL Server 的 SnapCenter 插件存储。

- 您需要的内容 *
- 确保插件处于维护模式。
- 中断 SnapMirror/SnapVault 关系。"中断 SnapMirror 关系"
- 使用相同的驱动器盘符将 LUN 从二级系统连接到主机。
- 确保使用 DR 之前使用的相同驱动器盘符连接所有磁盘。
- 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，导航到 * 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 * 以验证是否已启用灾难恢复作业。
- 完成后 *
- 如果在故障转移后创建了新数据库，则这些数据库将处于非 DR 模式。

  新数据库将继续像故障转移前一样运行。

- 在灾难恢复模式下创建的新备份将在拓扑页面的 SnapMirror 或 SnapVault （二级）下列出。

新备份旁边会显示一个 "i" 图标，表示这些备份是在灾难恢复模式下创建的。

- 您可以使用UI或以下cmdlet删除在故障转移期间创建的适用于SQL Server的SnapCenter 插件备份：`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`

  有关详细信息，请参阅 "《 SnapCenter 软件 cmdlet 参考指南》"。

- SnapCenter 服务器将管理处于灾难恢复或非灾难恢复模式的各个存储资源（ SQL 数据库），但不管理存储资源处于灾难恢复模式或非灾难恢复模式的资源组。

从适用于 **SQL Server** 的 **SnapCenter** 插件二级存储故障恢复到主存储

在适用于 SQL Server 的 SnapCenter 插件主存储恢复联机后，您应故障恢复到主存储。

- 您需要的内容 *
- 从 " 受管主机 " 页面将适用于 SQL Server 的 SnapCenter 插件置于 * 维护 * 模式。
- 断开二级存储与主机的连接，并与主存储进行连接。
- 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前的关系方向保持一致。

  要在执行反向重新同步操作后保留主存储和二级存储的角色，请再次执行反向重新同步操作。

  有关详细信息，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。

> 在该插件的故障转移或故障恢复期间、不会立即刷新该插件的整体状态。主机和插件的整体状态将在后续主机刷新操作期间更新。

- 步骤 *
  1. 在设置页面中，导航到 * 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 * 以验证是否已启用灾难恢复作业。
- 完成后 *
- 您可以使用UI或以下cmdlet删除在故障转移期间创建的适用于SQL Server的SnapCenter 插件备份：`Remove-SmDRFailoverBackups`

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。