准备安装 SnapCenter 自定义插件

SnapCenter Software 4.9

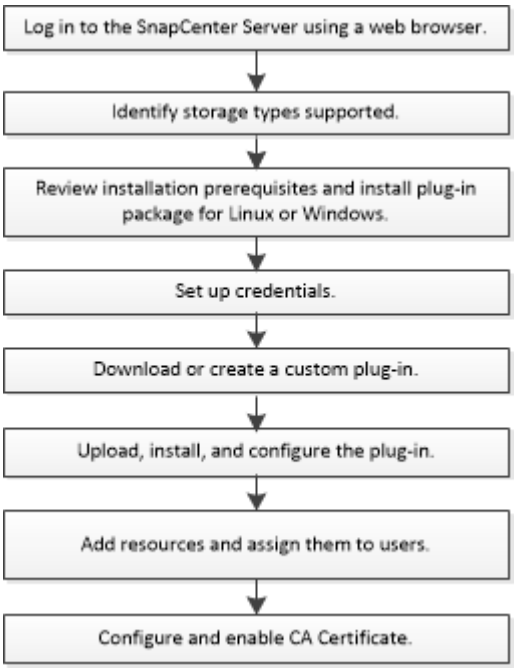
NetApp
March 20, 2024

目录

准备安装 SnapCenter 自定义插件

SnapCenter 自定义插件的安装工作流

如果要保护自定义插件资源，应安装和设置 SnapCenter 自定义插件。



"为您的应用程序开发一个插件"

添加主机和安装 SnapCenter 自定义插件的前提条件

在添加主机并安装插件软件包之前，您必须满足所有要求。自定义插件既可以在 Windows 环境中使用，也可以在 Linux 环境中使用。

- 您必须已创建自定义插件。有关详细信息，请参见开发人员信息。

  "为您的应用程序开发一个插件"

- 如果要管理 MySQL 或 DB2 应用程序，必须已下载 NetApp 提供的 MySQL 和 DB2 自定义插件。
- 您必须已在Linux或Windows主机上安装Java 1.8或Java 11 (64位)。
- 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 。
- 自定义插件必须在执行添加主机操作的客户端主机上可用。

常规

如果使用的是iSCSI、则iSCSI服务应正在运行。

SHA512哈希

- 对于NetApp提供的自定义插件、您应确保已将自定义插件文件的SHA512哈希添加到_custom_plugin_checksum_list_文件中。
  - 对于Linux主机、SHA512哈希位于：_/var/opt/snapcenter/SCC/custom_plugin_checksum_list.txt
  - 对于Windows主机、SHA512哈希位于 *C：\Program Files\NetApp\SnapCenter Plug-in Creper\ETC\custom_plugin_*校 验和*_list.TXT*

    对于自定义安装路径、SHA512哈希位于_<custom path>\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\custom_plugin_checksum_list.txt

  custom_plugin_checksum_list是SnapCenter 在主机上安装的自定义插件的一部分。

- 对于为应用程序创建的自定义插件、您应已执行以下步骤：

  a. 已生成插件zip文件的SHA512哈希。

     您可以使用等联机工具 "SHA512哈希"。

  b. 已将生成的SHA512哈希添加到custom_plugin_checksum_list文件中的新行。

     注释以#符号开头、用于标识哈希所属的插件。

     以下是校验和文件中SHA512哈希条目的示例：

```
#ORASCPM
03721f567a1e4a1cb5569066b9a58af619ee12b1f8713108f81b696cfbdb81c25232fa63
d6e6777a2b2a1ec068bb0a93a59a8ade71587182f8bccbe81f7e0ba6
```

Windows 主机

- 您必须具有具有本地管理员权限的域用户，并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，则必须具有对集群中所有节点具有管理权限的用户。

Linux 主机

- 您必须已为 root 用户或非 root 用户启用基于密码的 SSH 连接。
- 您必须已在Linux主机上安装Java 1.8或Java 11 (64位)。

  如果要对SnapCenter 服务器主机使用Windows Server 2019或Windows Server 2016、则必须安装Java 1.8或Java 11 (64位)。互操作性表工具（ IMT ）包含有关要求的最新信息。

  "适用于所有操作系统的 Java 下载"

  "NetApp 互操作性表工具"

- 您必须为非 root 用户配置 sudo 权限，才能提供对多个路径的访问权限。使用 visudo Linux 实用程序将以下

行添加到 /etc/sudoers 文件中。

确保使用的是sudo 1.8.7或更高版本。

```
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_Prechecks.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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

_linux_user_是 您创建的非root用户的名称。

您可以从* ORACLE_checksum.txt *文件中获取_checksum_value_、该文件位于_C：\ProgramData\NetApp\SnapCenter\Package Repository _。

此示例只能用作创建自己数据的参考。

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

项目	要求
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专用的故障排除信息、请参见 "对于没有Internet连接的原有系统、SnapCenter 升级或安装失败。"

安装适用于 Linux 的 SnapCenter 插件软件包的主机要求

在安装适用于 Linux 的 SnapCenter 插件软件包之前，应确保主机满足要求。

项目	要求
操作系统	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server （ SLES ）
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	2 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。

项目	要求
所需的软件包	Java 1.8 （64 位） Oracle Java 或 OpenJDK 版本 如果已将 Java 升级到最新版本，则必须确保 /var/opt/snapcenter/spl/etc/spl.properties 上的 java_home 选项设置为正确的 Java 版本和路径。

有关受支持版本的最新信息，请参见 "NetApp 互操作性表工具"

设置 SnapCenter 自定义插件的凭据

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。

开始之前

- Linux 主机

  您必须设置在 Linux 主机上安装插件的凭据。

  您必须为 root 用户或具有 sudo 权限的非 root 用户设置凭据，才能安装和启动插件过程。

  * 最佳实践： * 虽然在部署主机和安装插件后，您可以为 Linux 创建凭据，但最佳实践是在添加 SVM 之后，在部署主机和安装插件之前创建凭据。

- Windows 主机

  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。

- 自定义插件应用程序

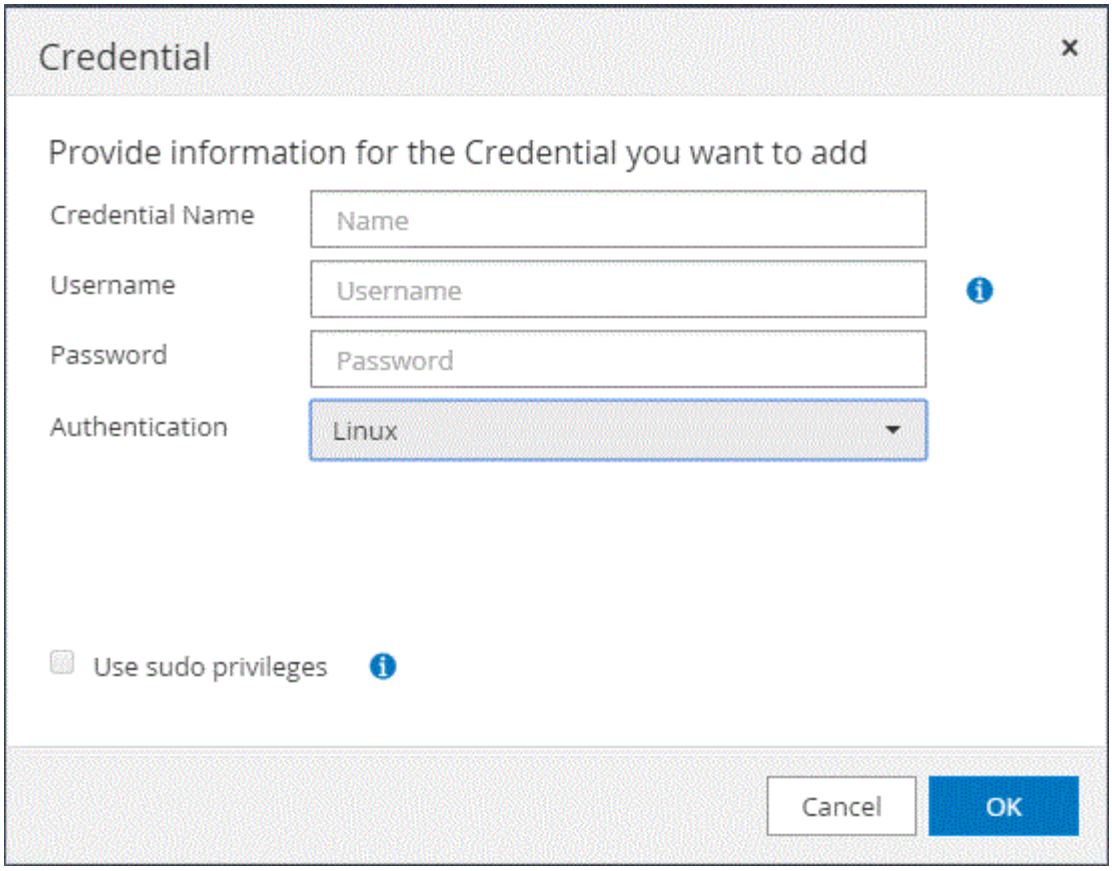
  此插件使用在添加资源时选择或创建的凭据。如果在数据保护操作期间资源不需要凭据，则可以将凭据设置为 * 无 * 。

关于此任务

如果您为各个资源组设置了凭据，并且用户名不具有完全管理员权限，则必须至少为此用户名分配资源组和备份权限。

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. 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。
用户名	输入要用于身份验证的用户名和密码。 • 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*

对于此字段 ...	执行此操作 ...
Password	输入用于身份验证的密码。
身份验证模式	选择要使用的身份验证模式。
使用 sudo 权限	如果要为非 root 用户创建凭据，请选中 * 使用 sudo 权限 * 复选框。 仅适用于 Linux 用户。

5. 单击 * 确定 * 。

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

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。

开始之前

- 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>`

5. 为主机上配置的 GMSA 分配管理权限。

6. 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 SnapCenter 自定义插件

添加主机并在远程主机上安装插件软件包

您必须使用 SnapCenterAdd Host 页面添加主机，然后安装插件软件包。这些插件会自动安装在远程主机上。您可以为单个主机或集群添加主机并安装插件软件包。

开始之前

- 您应该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。
- 您应确保消息队列服务正在运行。
- 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 或更高版本上为自定义应用程序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。

如果在集群（ WSFC ）上安装插件，则这些插件将安装在集群的所有节点上。

步骤

1. 在左侧导航窗格中，选择 * 主机 * 。
2. 验证顶部是否已选中 * 受管主机 * 选项卡。
3. 选择 * 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	选择主机类型： • Windows • Linux 自定义插件可在 Windows 和 Linux 环境中使用。
主机名	输入主机的完全限定域名（ FQDN ）或 IP 地址。 SnapCenter 取决于 DNS 的正确配置。因此，最佳做法是输入 FQDN 。 对于 Windows 环境，只有在将 IP 地址解析为 FQDN 时，不可信域主机才支持此 IP 地址。 您可以输入独立主机的 IP 地址或 FQDN 。 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。 这些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. (可选)选择*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。

对于此字段 ...	执行此操作 ...
安装路径	自定义插件可以安装在 Windows 系统或 Linux 系统上。 • 对于适用于 Windows 的 SnapCenter 插件软件包，默认路径为 C： \Program Files\NetApp\SnapCenter 。 您也可以自定义路径。 • 对于适用于Linux的SnapCenter插件软件包、默认路径为 `/opt/NetApp/snapcenter`。 您也可以自定义路径。 • 对于 SnapCenter 自定义插件： i. 在“Custom Plug-ins”(自定义插件)部分，选择*Browse*(浏览*)，然后选择压缩的自定义插件文件夹。 压缩文件夹包含自定义插件代码和描述符 .xml 文件。 对于存储插件、导航到 *`C:\ProgramData\NetApp\SnapCenter\Package Repository`* 并选择 `Storage.zip` 文件夹。 ii. 选择*上传*。 上传软件包之前，会验证压缩后的自定义插件文件夹中的描述符 .xml 文件。 此时将列出上传到 SnapCenter 服务器的自定义插件。 如果要管理 MySQL 或 DB2 应用程序，可以使用 NetApp 提供的 MySQL 和 DB2 自定义插件。MySQL 和 DB2 自定义插件可从获取 "NetApp 自动化商店"
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。

对于此字段 ...	执行此操作 ...
使用组托管服务帐户（ GMSA ）运行插件服务	对于 Windows 主机，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$ 。 GMSA 仅用作适用于 Windows 的 SnapCenter 插件服务的登录服务帐户。

7. 选择 * 提交 * 。

   如果未选中 * 跳过预检查 * 复选框，则主机将通过验证以验证主机是否满足安装插件的要求。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。

8. 如果主机类型为Linux，请验证指纹，然后选择*确认并提交*。

   即使先前已将同一主机添加到 SnapCenter 并确认了指纹，也必须进行指纹验证。

9. 监控安装进度。

   安装专用的日志文件位于 `/custom_location/snapcenter/` 日志。

使用 **cmdlet** 在多个远程主机上安装适用于 **Linux** 或 **Windows** 的 **SnapCenter** 插件软件包

您可以使用 Install-SmHostPackage PowerShell cmdlet 在多个主机上同时安装适用于 Linux 或 Windows 的 SnapCenter 插件软件包。

开始之前

添加主机的用户应具有该主机的管理权限。

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 和所需参数在多个主机上安装此插件。

   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。

4. 输入远程安装的凭据。

使用命令行界面在 **Linux** 主机上安装 **SnapCenter** 自定义插件

您应使用 SnapCenter 用户界面（ UI ）安装 SnapCenter 自定义插件。如果您的环境不允许从 SnapCenter UI 远程安装此插件，则可以使用命令行界面（ CLI ）在控制台模式或静默模式下安装此自定义插件。

步骤

1. 将适用于 Linux 的 SnapCenter 插件软件包安装文件（ snapcenter_linux_host_plugin.bin ）从 C：\ProgramData\NetApp\SnapCenter\Package Repository 复制到要安装自定义插件的主机。

   您可以从安装了 SnapCenter 服务器的主机访问此路径。

2. 在命令提示符处，导航到复制安装文件的目录。
3. 安装插件： `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 用于指定 SMCore HTTPS 通信端口。
   - -dserver_ip 指定 SnapCenter 服务器 IP 地址。
   - -dserver_HTTPS_port 指定 SnapCenter 服务器 HTTPS 端口。
   - -duser_install_DIR 指定要安装适用于 Linux 的 SnapCenter 插件软件包的目录。
   - DINSTALL_LOG_name 指定日志文件的名称。

   ```
   /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. 使用 Add-Smhost cmdlet 和所需参数将主机添加到 SnapCenter 服务器。

   有关可与命令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》"。

5. 登录到 SnapCenter ，然后从 UI 或使用 PowerShell cmdlet 上传自定义插件。

   您可以参考从 UI 上传自定义插件 "添加主机并在远程主机上安装插件软件包" 部分。

   SnapCenter cmdlet 帮助和 cmdlet 参考信息包含有关 PowerShell cmdlet 的详细信息。

   "《 SnapCenter 软件 cmdlet 参考指南》"。

监控安装自定义插件的状态

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*Jobs*页中，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 * 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。

CA证书RSA密钥长度应至少为3072位。

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。 可以通过在获取证书之前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"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

在 **Linux** 主机上为 **SnapCenter** 自定义插件服务配置 **CA** 证书

您应管理自定义插件密钥库及其证书的密码、配置CA证书、为自定义插件信任存储库配置根或中间证书、并使用SnapCenter自定义插件服务将CA签名密钥对配置为自定义插件信任存储库、以激活已安装的数字证书。

自定义插件使用文件 "keystore.jks" ，该文件位于 */opt/netapp/snapcenter/scc/ etc* ，同时用作其信任存储和密钥存储。

管理自定义插件密钥库的密码以及正在使用的 **CA** 签名密钥对的别名

步骤

1. 您可以从自定义插件代理属性文件中检索自定义插件密钥库默认密码。

   它是与密钥 "keystore_pass" 对应的值。

2. 更改密钥库密码：

   ```
    keytool -storepasswd -keystore keystore.jks
   ```
   . 将密钥库中私钥条目的所有别名的密码更改为密钥库使用的相同密码：

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

   为 *agent.properties* 文件中的 keystore_pass 密钥更新相同的。

3. 更改密码后重新启动服务。

自定义插件密钥库的密码和专用密钥的所有关联别名密码应相同。

将根证书或中间证书配置为自定义插件信任存储

您应将不带私钥的根证书或中间证书配置为自定义插件信任存储。

步骤

1. 导航到包含自定义插件密钥库的文件夹：/opt/NetApp/ssnapcCenter/SCC/等
2. 找到文件 "keystore.jks" 。
3. 列出密钥库中添加的证书：

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

4. 添加根证书或中间证书：

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. 将根证书或中间证书配置为自定义插件信任存储后重新启动服务。
```

您应先添加根 CA 证书，然后再添加中间 CA 证书。

将 **CA** 签名密钥对配置为自定义插件信任存储

您应将 CA 签名密钥对配置为自定义插件信任存储。

步骤

1. 导航到包含自定义插件密钥库 /opt/netapp/snapcenter/scc/ 等的文件夹
2. 找到文件 "keystore.jks" 。
3. 列出密钥库中添加的证书：

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

4. 添加同时具有私钥和公有密钥的 CA 证书。

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

5. 列出密钥库中添加的证书。

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

6. 验证密钥库是否包含与已添加到密钥库中的新 CA 证书对应的别名。
7. 将为 CA 证书添加的私钥密码更改为密钥库密码。

   默认自定义插件密钥库密码是 agent.properties 文件中密钥 keystore_pass 的值。

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . 如果 CA 证书中的别名较长，并且包含空格或特殊字符（ "*" ， " ， "
   ），请将别名更改为简单名称：
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . 从 agent.properties 文件中的 CA 证书配置别名。
   ```

   根据密钥 SCC_certificate_alias 更新此值。

8. 将 CA 签名密钥对配置为自定义插件信任存储后重新启动服务。

为 **SnapCenter** 自定义插件配置证书撤消列表（ **Certificate Revocation List ， CRL** ）

关于此任务

- SnapCenter 自定义插件将在预配置的目录中搜索 CRL 文件。
- SnapCenter 自定义插件的 CRL 文件的默认目录为 " opt/netapp/snapcenter/SCC/etc/CRL" 。

步骤

1. 您可以使用密钥 CRL_PATH 修改和更新 agent.properties 文件中的默认目录。

   您可以在此目录中放置多个 CRL 文件。系统将根据每个 CRL 验证传入的证书。

在 **Windows** 主机上为 **SnapCenter** 自定义插件服务配置 **CA** 证书

您应管理自定义插件密钥库及其证书的密码、配置CA证书、为自定义插件信任存储库配置根或中间证书、并使用SnapCenter自定义插件服务将CA签名密钥对配置为自定义插件信任存储库、以激活已安装的数字证书。

自定义插件使用文件 *keystore.jks* ，该文件位于 *C* ： *\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc* ，同时用作其信任存储和密钥存储。

管理自定义插件密钥库的密码以及正在使用的 **CA** 签名密钥对的别名

步骤

1. 您可以从自定义插件代理属性文件中检索自定义插件密钥库默认密码。

   该值与 key_keystore_pass_ 键对应。

2. 更改密钥库密码：

   keytool -storepasswd -keystore keystore.jks

   > 如果在 Windows 命令提示符处无法识别 "keytool" 命令，请将 keytool 命令替换为其完整路径。

   C ： *\Program Files\java\<JDK_version>\bin\keytool.exe " -storepasswd -keystore keystore.jks*

3. 将密钥库中私钥条目的所有别名的密码更改为密钥库使用的相同密码：

   keytool -keypasswd -alias "alias_name_in_ct" -keystore keystore.jks

   为 *agent.properties* 文件中的 keystore_pass 密钥更新相同的。

4. 更改密码后重新启动服务。

   > 自定义插件密钥库的密码和专用密钥的所有关联别名密码应相同。

将根证书或中间证书配置为自定义插件信任存储

您应将不带私钥的根证书或中间证书配置为自定义插件信任存储。

步骤

1. 导航到包含自定义插件密钥库的文件夹_C：\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creper\ETC_
2. 找到文件 "keystore.jks" 。
3. 列出密钥库中添加的证书：

   keytool -list -v -keystore keystore.jks

4. 添加根证书或中间证书：

   keytool -import -trustcacerks -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. 将根证书或中间证书配置为自定义插件信任存储后重新启动服务。

   您应先添加根 CA 证书，然后再添加中间 CA 证书。

将 **CA** 签名密钥对配置为自定义插件信任存储

您应将 CA 签名密钥对配置为自定义插件信任存储。

步骤

1. 导航到包含自定义插件密钥库 *C： \Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc* 的文件夹
2. 找到文件 *keystore.jks* 。
3. 列出密钥库中添加的证书：

   keytool -list -v -keystore keystore.jks

4. 添加同时具有私钥和公有密钥的 CA 证书。

   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype PKCS12 -destkeystore keystore.jks -deststoretype JKS

5. 列出密钥库中添加的证书。

   keytool -list -v -keystore keystore.jks

6. 验证密钥库是否包含与已添加到密钥库中的新 CA 证书对应的别名。
7. 将为 CA 证书添加的私钥密码更改为密钥库密码。

   默认自定义插件密钥库密码是 agent.properties 文件中密钥 keystore_pass 的值。

   keytool -keypasswd -alias "alias_name_in_CA_ct" -keystore keystore.jks

8. 从 *agent.properties* 文件中的 CA 证书配置别名。

根据密钥 SCC_certificate_alias 更新此值。

9. 将 CA 签名密钥对配置为自定义插件信任存储后重新启动服务。

为 **SnapCenter** 自定义插件配置证书撤消列表（ **Certificate Revocation List** ， **CRL** ）

关于此任务

- 要下载相关 CA 证书的最新 CRL 文件，请参见 "如何更新 SnapCenter CA 证书中的证书撤消列表文件"。
- SnapCenter 自定义插件将在预配置的目录中搜索 CRL 文件。
- SnapCenter 自定义插件的 CRL 文件的默认目录为： *C* ： *\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\ etc\CRL'* 。

步骤

1. 您可以使用密钥 CRL_PATH 修改和更新 *agent.properties* 文件中的默认目录。
2. 您可以在此目录中放置多个 CRL 文件。

   系统将根据每个 CRL 验证传入的证书。

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。

开始之前

- 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 证书既未启用，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。