准备安装适用于 PostgreSQL 的 SnapCenter插件

SnapCenter software

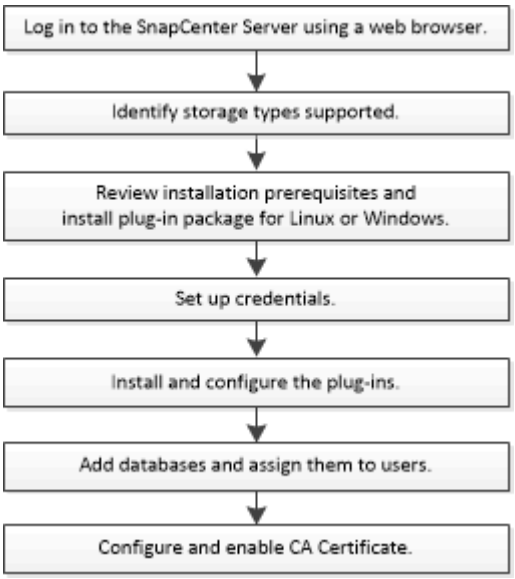
NetApp
November 06, 2025

目录

准备安装适用于 PostgreSQL 的SnapCenter插件

SnapCenter Plug-in for PostgreSQL 的安装工作流程

如果您想保护 PostgreSQL 集群，则应该安装并设置适用于 PostgreSQL 的SnapCenter插件。



添加主机并安装 PostgreSQL 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。 SnapCenter Plug-in for PostgreSQL 可在 Windows 和 Linux 环境中使用。

- 您必须在主机上安装 Java 11。

  IBM Java 在 Windows 和 Linux 主机上不受支持。

- 对于 Windows，插件创建服务应该使用“LocalSystem”Windows 用户运行，这是以域管理员身份安装 PostgreSQL 插件时的默认行为。
- 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。适用于 Microsoft Windows 的SnapCenter插件将默认与 Windows 主机上的 PostgreSQL 插件一起部署。
- SnapCenter服务器应该可以访问 PostgreSQL 主机插件的 8145 或自定义端口。

Windows 主机

- 您必须拥有具有本地管理员权限的域用户，并在远程主机上拥有本地登录权限。
- 在 Windows 主机上安装适用于 PostgreSQL 的插件时，适用于 Microsoft Windows 的SnapCenter插件会自动安装。
- 您必须为 root 用户或非 root 用户启用基于密码的 SSH 连接。

- 您必须在 Windows 主机上安装 Java 11。

  "下载适用于所有操作系统的 JAVA"

  "NetApp 互操作性表工具"

Linux 主机

- 您必须为 root 用户或非 root 用户启用基于密码的 SSH 连接。
- 您必须在 Linux 主机上安装 Java 11。

  "下载适用于所有操作系统的 JAVA"

  "NetApp 互操作性表工具"

- 对于在 Linux 主机上运行的 PostgreSQL 集群，在安装 PostgreSQL 插件时，会自动安装 UNIX 的SnapCenter插件。
- 您应该将 **bash** 作为插件安装的默认 shell。

补充命令

要在 PostgreSQL 的SnapCenter插件上运行补充命令，必须将其包含在 *allowed_commands.config* 文件中。

- Windows 主机上的默认位置：*C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Linux 主机上的默认位置：*/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

要允许插件主机上的补充命令，请在编辑器中打开_allowed_commands.config_文件。每个命令在单独的行上输入，并且命令不区分大小写。确保指定完全限定的路径名，并且如果路径名包含空格，则将其括在引号 (") 中。

例如：

命令：mount 命令：umount 命令：“C:\Program Files\ NetApp\SnapCreator commands\sdcli.exe” 命令：myscript.bat

如果不存在 *allowed_commands.config* 文件，命令或脚本执行将被阻止，并且工作流将失败并出现以下错误：

不允许执行“[/mnt/mount -a]。通过在插件主机上的文件 %s 中添加命令来授权。”

如果命令或脚本不在_allowed_commands.config_中，则命令或脚本的执行将被阻止，并且工作流将失败并出现以下错误：

不允许执行“[/mnt/mount -a]。通过在插件主机上的文件 %s 中添加命令来授权。”

您不应使用通配符 (*) 来允许所有命令。

为 Linux 主机的非 root 用户配置 sudo 权限

SnapCenter允许非 root 用户安装适用于 Linux 的SnapCenter插件包并启动插件进程。插件进程将以有效的非

root 用户身份运行。您应该为非 root 用户配置 sudo 权限以提供对多个路径的访问。

您需要什么

- Sudo 版本 1.8.7 或更高版本。
- 如果 umask 为 0027，请确保 java 文件夹及其内部的所有文件的权限为 555。否则插件安装可能会失败。
- 对于非root用户，请确保非root用户的名称和用户所在组的名称相同。
- 编辑_/etc/ssh/sshd_config_文件，配置消息认证码算法：MACs hmac-sha2-256、MACs hmac-sha2-512。

  更新配置文件后重新启动sshd服务。

  示例：

  ```
  #Port 22
  #AddressFamily any
  #ListenAddress 0.0.0.0
  #ListenAddress ::
  #Legacy changes
  #KexAlgorithms diffie-hellman-group1-sha1
  #Ciphers aes128-cbc
  #The default requires explicit activation of protocol
  Protocol 2
  HostKey/etc/ssh/ssh_host_rsa_key
  MACs hmac-sha2-256
  ```

关于此任务

您应该为非 root 用户配置 sudo 权限以提供对以下路径的访问权限：

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/安装/插件/卸载
- /custom_location/ NetApp/snapcenter/spl/bin/spl

步骤

1. 登录到要安装适用于 Linux 的SnapCenter插件包的 Linux 主机。
2. 使用 visudo Linux 实用程序将以下行添加到 /etc/sudoers 文件。

```
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 env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
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 **sc_unix_plugins_checksum.txt** 文件中获取 *checksum_value*，该文件位于：

- _C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _ 如果SnapCenter Server 安装在 Windows 主机上。
- _/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ 如果SnapCenter Server 安装在 Linux 主机上。

该示例仅应作为创建您自己的数据的参考。

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

物品	要求
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。
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 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。"

安装适用于 Linux 的SnapCenter插件包的主机要求

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

物品	要求
操作系统	• Red Hat Enterprise Linux • SUSE Linux 企业服务器 (SLES) 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	2 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。所需的日志空间有所不同，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	Java 11 Oracle Java 和 OpenJDK 如果您已将 JAVA 升级到最新版本，则必须确保位于 /var/opt/snapcenter/spl/etc/spl.properties 的 JAVA_HOME 选项设置为正确的 JAVA 版本和正确的路径。 有关受支持版本的最新信息，请参阅 "NetApp 互操作性表工具"。

为 PostgreSQL 的SnapCenter插件设置凭据

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集群或 Windows 文件系统上执行数据保护操作的其他凭据。

关于此任务

- 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进程。

  *最佳实践：*虽然您可以在部署主机和安装插件后为 Linux 创建凭据，但最佳实践是在添加 SVM 之后、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。

如果您为单个资源组设置凭据，并且用户名没有完全管理权限，则必须至少为该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：

对于这个领域...	操作
凭证名称	输入凭证的名称。

对于这个领域...	操作
用户名	输入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*\用户名 ◦ 域 *FQDN*\用户名 • 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。
密码	输入用于身份验证的密码。
认证模式	选择您想要使用的身份验证模式。
使用 sudo 权限	如果您要为非 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。

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。

安装适用于 PostgreSQL 的SnapCenter插件

添加主机并在远程主机上安装插件包

您必须使用SnapCenter添加主机页面来添加主机，然后安装插件包。插件会自动安装在远程主机上。您可以添加主机并为单个主机安装插件包。

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，或者用户属于本地工作组用户，则必须在主机上禁用 UAC。
- 您应该确保消息队列服务正在运行。
- 管理文档包含有关管理主机的信息。
- 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 PostgreSQL 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。

步骤

1. 在左侧导航窗格中，单击“主机”。
2. 验证顶部的“托管主机”选项卡是否被选中。
3. 单击“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	选择主机类型： • Windows • Linux PostgreSQL 插件安装在 PostgreSQL 客户端主机上，该主机可以是 Windows 系统，也可以是 Linux 系统。
主机名	输入通信主机名。输入主机的完全限定域名 (FQDN) 或 IP 地址。 SnapCenter依赖于 DNS 的正确配置。因此，最佳做法是输入 FQDN。
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。 您可以将光标放在您提供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。

   使用 REST API 安装 PostgreSQL 插件时，必须传递版本为 3.0。例如，PostgreSQL:3.0

6. （可选）单击“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。

对于这个领域...	操作
安装路径	PostgreSQL 插件安装在 PostgreSQL 客户端主机上，该主机可以是 Windows 系统，也可以是 Linux 系统。 • 对于适用于 Windows 的SnapCenter插件包，默认路径为 C:\Program Files\ NetApp\ SnapCenter。您也可以选择自定义路径。 • 对于适用于 Linux 的SnapCenter插件包，默认路径为 /opt/ NetApp/snapcenter。您也可以选择自定义路径。
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。
添加集群中的所有主机	选中此复选框可添加所有集群节点。
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) 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$。 gMSA 将仅用作 Windows 服务的SnapCenter插件的登录服务帐户。

7. 单击“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。

8. 如果主机类型为Linux，请验证指纹，然后单击*确认并提交*。

   在集群设置中，您应该验证集群中每个节点的指纹。

   即使之前已将同一主机添加到SnapCenter并且已确认指纹，也必须进行指纹验证。

9. 监控安装进度。
   - 对于 Windows 插件，安装和升级日志位于：*C:\Windows\ SnapCenter plugin\Install*<JOBID>_
   - 对于 Linux 插件，安装日志位于：*/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-*

in_Install<JOBID>.log_，升级日志位于：*/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

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

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

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 和所需参数在多个主机上安装插件。

   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。

使用命令行界面在 **Linux** 主机上安装适用于 **PostgreSQL** 的**SnapCenter**插件

您应该使用SnapCenter用户界面 (UI) 安装适用于 PostgreSQL 集群的SnapCenter插件。如果您的环境不允许从SnapCenter UI 远程安装插件，您可以使用命令行界面 (CLI) 以控制台模式或静默模式安装适用于 PostgreSQL 集群的插件。

开始之前

- 您应该在 PostgreSQL 客户端所在的每个 Linux 主机上安装 PostgreSQL 集群插件。
- 要安装SnapCenter Plug-in for PostgreSQL 集群的 Linux 主机必须满足相关软件、集群和操作系统要求。

  互操作性矩阵工具 (IMT) 包含有关受支持配置的最新信息。

  "NetApp 互操作性表工具"

- 适用于 PostgreSQL 集群的SnapCenter插件是适用于 Linux 的SnapCenter插件包的一部分。在安装适用于 Linux 的SnapCenter插件包之前，您应该已经在 Windows 主机上安装了SnapCenter 。

步骤

1. 将 Linux 安装文件 (snapcenter_linux_host_plugin.bin) 的SnapCenter插件包从 C:\ProgramData\ NetApp\ SnapCenter\Package Repository 复制到要安装 PostgreSQL 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. 从命令提示符处，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 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 Linux 版SnapCenter插件包的目录。
- 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. 编辑 /<安装目录> NetApp文件，然后添加 PLUGINS_ENABLED = PostgreSQL:3.0 参数。
5. 使用 Add-Smhost cmdlet 和所需参数将主机添加到SnapCenter服务器。

   可以通过运行_Get-Help command_name_来获取有关可与命令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"。

监控 **PostgreSQL** 插件安装状态

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*。

在此向导窗口中...	执行以下操作...
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 **Linux** 主机上的**SnapCenter PostgreSQL** 插件服务配置 **CA** 证书

您应该管理插件密钥库及其证书的密码，配置 CA 证书，将根证书或中间证书配置到插件信任库，并使用SnapCenter插件服务将 CA 签名密钥对配置到插件信任库以激活已安装的数字证书。

插件使用位于 */opt/ NetApp/snapcenter/scc/etc* 的文件"keystore.jks"作为其信任库和密钥库。

管理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. 您可以从插件代理属性文件中检索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
```
. 将密钥库中所有私钥条目别名的密码更改为与密钥库相同的密码：

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

对 *agent.properties* 文件中的密钥 KEYSTORE_PASS 进行相同的更新。

3. 修改密码后重启服务。

插件密钥库的密码和私钥的所有相关别名的密码应该相同。

配置根证书或中间证书以插入信任库

您应该配置没有私钥的根证书或中间证书来插入信任库。

步骤

1. 导航到包含插件密钥库的文件夹：/opt/ NetApp/snapcenter/scc/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 -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. 配置根证书或中间证书以插入信任库后重新启动服务。
```

您应该添加根 CA 证书，然后添加中间 CA 证书。

配置 **CA** 签名密钥对以插入信任库

您应该将 CA 签名的密钥对配置到插件信任库。

步骤

1. 导航到包含插件密钥库 /opt/ NetApp/snapcenter/scc/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. 添加具有私钥和公钥的 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添加到密钥库的新 CA 证书相对应的别名。
7. 将添加的CA证书私钥密码更改为keystore密码。

默认插件密钥库密码是 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，且包含空格或特殊字符（"*"，"，
"），请将别名修改为简单名称：

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
```

. 在 agent.properties 文件中配置来自 CA 证书的别名。

根据键 SCC_CERTIFICATE_ALIAS 更新此值。

8. 配置 CA 签名密钥对以插入信任库后重新启动服务。

为插件配置证书吊销列表 **(CRL)**

关于此任务

- SnapCenter插件将在预配置的目录中搜索 CRL 文件。
- SnapCenter插件的 CRL 文件的默认目录是"opt/ NetApp/snapcenter/scc/etc/crl"。

步骤

1. 您可以根据键 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。将根据每个 CRL 验证传入的证书。

为 **Windows** 主机上的**SnapCenter PostgreSQL** 插件服务配置 **CA** 证书

您应该管理插件密钥库及其证书的密码，配置 CA 证书，将根证书或中间证书配置到插件信任库，并使用SnapCenter插件服务将 CA 签名密钥对配置到插件信任库以激活已安装的数字证书。

插件使用位于 *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* 的文件 *keystore.jks* 作为其信任库和密钥库。

管理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. 您可以从插件代理属性文件中检索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 密钥库*.jks*

如果 Windows 命令提示符无法识别“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. 将密钥库中所有私钥条目别名的密码更改为与密钥库相同的密码：

   *keytool -keypasswd -alias“*别名在证书中*”-keystore keystore.jks*

   对 *agent.properties* 文件中的密钥 KEYSTORE_PASS 进行相同的更新。

4. 修改密码后重启服务。

插件密钥库的密码和私钥的所有相关别名的密码应该相同。

配置根证书或中间证书以插入信任库

您应该配置没有私钥的根证书或中间证书来插入信任库。

步骤

1. 导航到包含插件密钥库的文件夹 *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\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 -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. 配置根证书或中间证书以插入信任库后重新启动服务。

您应该添加根 CA 证书，然后添加中间 CA 证书。

配置 **CA** 签名密钥对以插入信任库

您应该将 CA 签名的密钥对配置到插件信任库。

步骤

1. 导航到包含插件密钥库的文件夹 *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\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. 添加具有私钥和公钥的 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添加到密钥库的新 CA 证书相对应的别名。
7. 将添加的CA证书私钥密码更改为keystore密码。

   默认插件密钥库密码是 agent.properties 文件中密钥 KEYSTORE_PASS 的值。

   *keytool -keypasswd -alias“*别名在*CA*证书中的名称*”-keystore keystore.jks*

8. 在_agent.properties_文件中配置来自CA证书的别名。

   根据键 SCC_CERTIFICATE_ALIAS 更新此值。

9. 配置 CA 签名密钥对以插入信任库后重新启动服务。

为**SnapCenter**插件配置证书吊销列表 **(CRL)**

关于此任务

- 要下载相关 CA 证书的最新 CRL 文件，请参阅 "如何更新SnapCenter CA 证书中的证书吊销列表文件"。
- SnapCenter插件将在预配置的目录中搜索 CRL 文件。
- SnapCenter插件的 CRL 文件的默认目录是 *'C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*。

步骤

1. 您可以根据键 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。

   将根据每个 CRL 验证传入的证书。

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。