为 Unix 文件系统安装SnapCenter插件

SnapCenter software

NetApp
November 06, 2025

目录

为 Unix 文件系统安装SnapCenter插件

添加主机并安装 Linux 插件包的先决条件

在添加主机并安装 Linux 的插件包之前，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。
- 您可以对 root 用户或非 root 用户使用基于密码的身份验证，也可以使用基于 SSH 密钥的身份验证。

  非 root 用户可以安装适用于 Unix 文件系统的SnapCenter插件。但是，您应该为非 root 用户配置 sudo 权限来安装和启动插件进程。安装插件后，进程将作为有效的非 root 用户运行。

- 为安装用户创建以 Linux 为身份验证模式的凭据。
- 您必须在 Linux 主机上安装 Java 11。

  确保您在 Linux 主机上仅安装了 JAVA 11 的认证版本。

  有关下载 JAVA 的信息，请参阅： "适用于所有操作系统的 Java 下载"

- 您应该将 **bash** 作为插件安装的默认 shell。

Linux 主机要求

在安装适用于 Linux 的SnapCenter插件包之前，您应该确保主机满足要求。

物品	要求
操作系统	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux 企业服务器 (SLES)
主机上SnapCenter插件的最小 RAM	2 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 确保您在 Linux 主机上仅安装了 JAVA 11 的认证版本。 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"。

使用 GUI 添加主机并安装 Linux 插件包

您可以使用“添加主机”页面添加主机，然后安装适用于 Linux 的SnapCenter插件包。插件会自动安装在远程主机上。

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 **Linux** 作为主机类型。
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。 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*Unix 文件系统*。
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。
安装路径	默认路径为 */opt/ NetApp/snapcenter*。 您可以选择自定义路径。如果您使用自定义路径，请确保 sudoers 的默认内容使用自定义路径进行更新。
跳过可选的预安装检查	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。

7. 单击“提交”。

如果您没有选中“跳过预检查”复选框，则会对主机进行验证，以验证主机是否满足安装插件的要求。

如果防火墙拒绝规则中指定了插件端口防火墙状态，则预检查脚本不会验证该状态。

如果未满足最低要求，则会显示适当的错误或警告消息。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，则应修复该问题。

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. 验证指纹，然后单击*确认并提交*。

   SnapCenter不支持 ECDSA 算法。

   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。

   特定于安装的日志文件位于 */custom_location/snapcenter/logs*。

结果

主机上挂载的所有文件系统都会自动发现并显示在资源页面下。如果没有显示任何内容，请单击“刷新资源”。

监控安装状态

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SnapCenter插件Loader服务

SnapCenter插件加载Loader服务加载 Linux 的插件包以便与SnapCenter服务器交互。安装适用于 Linux 的SnapCenter插件包时，也会安装SnapCenter插件加载Loader服务。

关于此任务

安装适用于 Linux 的SnapCenter插件包后， SnapCenter插件Loader服务将自动启动。如果SnapCenter插件Loader服务无法自动启动，您应该：

- 确保插件运行的目录没有被删除
- 增加分配给 Java 虚拟机的内存空间

spl.properties 文件位于 */custom_location/ NetApp/snapcenter/spl/etc/*，包含以下参数。这些参数被分配了默认值。

参数名称	描述
日志级别	显示支持的日志级别。 可能的值是 TRACE、DEBUG、INFO、WARN、ERROR 和 FATAL。
SPL_协议	显示SnapCenter插件Loader程序支持的协议。 仅支持HTTPS协议。如果缺少默认值，您可以添加该值。
SNAPCENTER_SERVER_协议	显示SnapCenter Server 支持的协议。 仅支持HTTPS协议。如果缺少默认值，您可以添加该值。
跳过JAVAHOME更新	默认情况下，SPL 服务会检测 java 路径并更新 JAVA_HOME 参数。 因此默认值设置为 FALSE。如果您想禁用默认行为并手动修复 java 路径，可以将其设置为 TRUE。
SPL_KEYSTORE_PASS	显示密钥库文件的密码。 仅当您更改密码或创建新的密钥库文件时才可以更改此值。

参数名称	描述
SPL_端口	显示SnapCenter插件Loader服务正在运行的端口号。 如果缺少默认值，您可以添加该值。 安装插件后您不应更改该值。
SNAPCENTER_SERVER_HOST	显示SnapCenter服务器的 IP 地址或主机名。
SPL_KEYSTORE_PATH	显示密钥库文件的绝对路径。
SNAPCENTER_SERVER_PORT	显示SnapCenter服务器正在运行的端口号。
日志最大数量	显示保留在 */custom_location/snapcenter/spl/logs* 文件夹中的SnapCenter插件Loader日志文件的数量。 默认值设置为 5000。如果计数超过指定值，则保留最后 5000 个修改的文件。从SnapCenter插件Loader服务启动时起，每 24 小时自动检查一次文件数量。 如果手动删除 spl.properties 文件，则要保留的文件数将设置为 9999。
JAVA_HOME	显示用于启动 SPL 服务的 JAVA_HOME 的绝对目录路径。 此路径是在安装期间和启动 SPL 的过程中确定的。
日志最大大小	显示作业日志文件的最大大小。 一旦达到最大大小，日志文件就会被压缩，并且日志会被写入该作业的新文件中。
保留最近几天的日志	显示日志最多保留的天数。
启用证书验证	当主机启用 CA 证书验证时显示 true。 您可以通过编辑 spl.properties 或使用SnapCenter GUI 或 cmdlet 来启用或禁用此参数。

如果这些参数中的任何一个没有分配默认值或者您想要分配或更改值，那么您可以修改 spl.properties 文件。您还可以验证 spl.properties 文件并编辑该文件以解决与分配给参数的值相关的任何问题。修改 spl.properties 文件后，您应该重新启动SnapCenter插件Loader服务。

步骤

1. 根据需要执行以下操作之一：
   - 启动SnapCenter插件Loader服务：
     - 以 root 用户身份运行： `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - 以非 root 用户身份运行： `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - 停止SnapCenter插件Loader服务：
     - 以 root 用户身份运行： `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - 以非 root 用户身份运行： `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

       您可以将 -force 选项与 stop 命令结合使用来强制停止SnapCenter插件Loader服务。但是，在执行此操作之前应谨慎，因为它也会终止现有操作。
   - 重新启动SnapCenter插件Loader服务：
     - 以 root 用户身份运行： `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - 以非 root 用户身份运行： `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
   - 查找SnapCenter插件Loader服务的状态：
     - 以 root 用户身份运行： `/custom_location/NetApp/snapcenter/spl/bin/spl status`
     - 以非 root 用户身份运行： `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
   - 查找SnapCenter插件Loader服务中的更改：
     - 以 root 用户身份运行： `/custom_location/NetApp/snapcenter/spl/bin/spl change`
     - 以非 root 用户身份运行： `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

在 Linux 主机上使用SnapCenter插件Loader(SPL) 服务配置 CA 证书

您应该管理 SPL 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 SPL 信任库，并使用SnapCenter插件Loader服务将 CA 签名密钥对配置到 SPL 信任库以激活已安装的数字证书。

SPL 使用位于“/var/opt/snapcenter/spl/etc”的文件“keystore.jks”作为其信任库和密钥库。

管理 SPL 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 SPL 属性文件中检索 SPL 密钥库默认密码。

它是与键“SPL_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>" -keystore keystore.jks
```

对 spl.properties 文件中的密钥 SPL_KEYSTORE_PASS 进行相同的更新。

3. 修改密码后重启服务。

SPL 密钥库的密码和私钥的所有相关别名的密码应该相同。

将根证书或中间证书配置到 SPL 信任库

您应该将没有私钥的根证书或中间证书配置到 SPL 信任库。

步骤

1. 导航到包含 SPL 密钥库的文件夹：*/var/opt/snapcenter/spl/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
. 添加根证书或中间证书：
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. 将根证书或中间证书配置到 SPL 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。

将 CA 签名密钥对配置到 SPL 信任库

您应该将 CA 签名的密钥对配置到 SPL 信任库。

步骤

1. 导航到包含 SPL 密钥库 /var/opt/snapcenter/spl/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
```

. 添加具有私钥和公钥的 CA 证书。

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

. 列出密钥库中添加的证书。

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

. 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。
. 将添加的CA证书私钥密码更改为keystore密码。

默认 SPL 密钥库密码是 spl.properties 文件中密钥 SPL_KEYSTORE_PASS 的值。

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -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 "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
```

. 从位于 spl.properties 文件中的密钥库配置别名。

根据键 SPL_CERTIFICATE_ALIAS 更新此值。

4. 将 CA 签名密钥对配置到 SPL 信任库后重新启动服务。

为 SPL 配置证书吊销列表 (CRL)

您应该为 SPL 配置 CRL

关于此任务

- SPL 将在预配置的目录中查找 CRL 文件。
- SPL 的 CRL 文件的默认目录是 */var/opt/snapcenter/spl/etc/crl*。

步骤

1. 您可以根据键 SPL_CRL_PATH 修改和更新 spl.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。