Instalar el complemento SnapCenter para sistemas de archivos Unix

SnapCenter software

NetApp
November 06, 2025

Tabla de contenidos

Instalar el complemento SnapCenter para sistemas de archivos Unix

Requisitos previos para agregar hosts e instalar el paquete de complementos para Linux

Antes de agregar un host e instalar el paquete de complementos para Linux, debe completar todos los requisitos.

- Si está utilizando iSCSI, el servicio iSCSI debe estar ejecutándose.
- Puede utilizar la autenticación basada en contraseña para el usuario root o no root o la autenticación basada en clave SSH.

  El complemento SnapCenter para sistemas de archivos Unix puede ser instalado por un usuario que no sea root. Sin embargo, debe configurar los privilegios de sudo para que el usuario no root pueda instalar e iniciar el proceso del complemento. Después de instalar el complemento, los procesos se ejecutarán como un usuario no root efectivo.

- Cree credenciales con modo de autenticación como Linux para el usuario de instalación.
- Debes tener instalado Java 11 en tu host Linux.

  Asegúrese de haber instalado únicamente la edición certificada de JAVA 11 en el host Linux.

  Para obtener información sobre cómo descargar JAVA, consulte: "Descargas de Java para todos los sistemas operativos"

- Debe tener **bash** como el shell predeterminado para la instalación del complemento.

Requisitos del host Linux

Debe asegurarse de que el host cumpla con los requisitos antes de instalar el paquete de complementos de SnapCenter para Linux.

Artículo	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • Oracle Linux • Servidor empresarial SUSE Linux (SLES)
RAM mínima para el complemento SnapCenter en el host	2 GB

Artículo	Requisitos
Espacio mínimo de instalación y registro para el complemento SnapCenter en el host	2 GB Debe asignar suficiente espacio en disco y supervisar el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de entidades a proteger y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio en disco, no se crearán registros para las operaciones ejecutadas recientemente.
Paquetes de software necesarios	Java 11 Oracle Java y OpenJDK Asegúrese de haber instalado únicamente la edición certificada de JAVA 11 en el host Linux. Si ha actualizado JAVA a la última versión, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión de JAVA correcta y en la ruta correcta.

Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Agregar hosts e instalar el paquete de complementos para Linux mediante GUI

Puede utilizar la página Agregar host para agregar hosts y luego instalar el paquete de complementos de SnapCenter para Linux. Los complementos se instalan automáticamente en los hosts remotos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. Verifique que la pestaña **Hosts administrados** esté seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página Hosts, realice las siguientes acciones:

Para este campo…	Haz esto…
Tipo de host	Seleccione **Linux** como tipo de host.

Para este campo…	Haz esto…
Host name	Introduzca el nombre de dominio completo (FQDN) o la dirección IP del host. SnapCenter depende de la configuración adecuada del DNS. Por lo tanto, la mejor práctica es ingresar el FQDN. Si está agregando un host mediante SnapCenter y el host es parte de un subdominio, debe proporcionar el FQDN.
Cartas credenciales	Seleccione el nombre de la credencial que creó o cree nuevas credenciales. La credencial debe tener derechos administrativos en el host remoto. Para obtener más detalles, consulte la información sobre la creación de credenciales. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de la credencial que especificó. El modo de autenticación de credenciales está determinado por el tipo de host que especifique en el asistente Agregar host.

5. En la sección Seleccionar complementos para instalar, seleccione **Sistemas de archivos Unix**.
6. (Opcional) Haga clic en **Más opciones**.

Para este campo…	Haz esto…
Puerto	Mantenga el número de puerto predeterminado o especifique el número de puerto. El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado. Si instaló manualmente los complementos y especificó un puerto personalizado, debe especificar el mismo puerto. De lo contrario la operación falla.

Para este campo…	Haz esto…
Ruta de instalación	La ruta predeterminada es */opt/ NetApp/snapcenter*. Opcionalmente puedes personalizar la ruta. Si utiliza la ruta personalizada, asegúrese de que el contenido predeterminado de los sudoers se actualice con la ruta personalizada.
Omitir comprobaciones de preinstalación opcionales	Seleccione esta casilla de verificación si ya ha instalado los complementos manualmente y no desea validar si el host cumple con los requisitos para instalar el complemento.

7. Haga clic en **Enviar**.

   Si no ha seleccionado la casilla de verificación Omitir comprobaciones previas, se valida el host para verificar si cumple con los requisitos para instalar el complemento.

   > El script de verificación previa no valida el estado del firewall del puerto del complemento si está especificado en las reglas de rechazo del firewall.

   Se muestran mensajes de error o advertencia apropiados si no se cumplen los requisitos mínimos. Si el error está relacionado con el espacio en disco o la RAM, puede actualizar el archivo web.config ubicado en *C:\Program Files\ NetApp\ SnapCenter WebApp* para modificar los valores predeterminados. Si el error está relacionado con otros parámetros, debes solucionar el problema.

   > En una configuración de alta disponibilidad, si está actualizando el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Verifique la huella digital y luego haga clic en **Confirmar y enviar**.

   > SnapCenter no admite el algoritmo ECDSA.

   > La verificación de huellas dactilares es obligatoria incluso si el mismo host se agregó anteriormente a SnapCenter y se confirmó la huella dactilar.

9. Supervisar el progreso de la instalación.

   Los archivos de registro específicos de la instalación se encuentran en */custom_location/snapcenter/logs*.

Resultado

Todos los sistemas de archivos montados en el host se descubren automáticamente y se muestran en la página Recursos. Si no se muestra nada, haga clic en **Actualizar recursos**.

Supervisar el estado de la instalación

Puede supervisar el progreso de la instalación del paquete de complementos de SnapCenter mediante la página Trabajos. Es posible que desees verificar el progreso de la instalación para determinar cuándo está completa o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Trabajos e indican el estado de la operación:

- En curso
- Completado exitosamente
- Fallido
- Completado con advertencias o no se pudo iniciar debido a advertencias
- En cola

Pasos

1. En el panel de navegación izquierdo, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **Trabajos**.
3. En la página **Trabajos**, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de complementos, haga lo siguiente:
   a. Haga clic en **Filtro**.
   b. Opcional: especifique la fecha de inicio y finalización.
   c. En el menú desplegable Tipo, seleccione **Instalación de complemento**.
   d. En el menú desplegable Estado, seleccione el estado de la instalación.
   e. Haga clic en **Aplicar**.
4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

Configurar el servicio de Loader de complementos de SnapCenter

El servicio SnapCenter Plug-in Loader carga el paquete de complementos para Linux para interactuar con el servidor SnapCenter . El servicio SnapCenter Plug-in Loader se instala cuando instala el paquete de complementos de SnapCenter para Linux.

Acerca de esta tarea

Después de instalar el paquete de complementos de SnapCenter para Linux, el servicio SnapCenter Plug-in Loader se inicia automáticamente. Si el servicio SnapCenter Plug-in Loader no se inicia automáticamente, debe:

- Asegúrese de que el directorio donde está funcionando el complemento no se elimine
- Aumentar el espacio de memoria asignado a la máquina virtual Java

El archivo spl.properties, que se encuentra en */custom_location/ NetApp/snapcenter/spl/etc/*, contiene los siguientes parámetros. A estos parámetros se les asignan valores predeterminados.

Nombre del parámetro	Descripción
NIVEL DE REGISTRO	Muestra los niveles de registro admitidos. Los valores posibles son TRACE, DEBUG, INFO, WARN, ERROR y FATAL.
PROTOCOLO SPL	Muestra el protocolo compatible con SnapCenter Plug-in Loader. Sólo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.
PROTOCOLO DEL SERVIDOR SNAPCENTER	Muestra el protocolo compatible con SnapCenter Server. Sólo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.
SALTAR ACTUALIZACIÓN DE JAVAHOME	De forma predeterminada, el servicio SPL detecta la ruta de Java y actualiza el parámetro JAVA_HOME. Por lo tanto, el valor predeterminado se establece en FALSO. Puede establecerlo en VERDADERO si desea deshabilitar el comportamiento predeterminado y corregir manualmente la ruta de Java.
CONTRASEÑA DEL ALMACÉN DE LLAVES SPL	Muestra la contraseña del archivo del almacén de claves. Puede cambiar este valor solo si cambia la contraseña o crea un nuevo archivo de almacén de claves.
SPL_PORT	Muestra el número de puerto en el que se ejecuta el servicio SnapCenter Plug-in Loader . Puede agregar el valor si falta el valor predeterminado. No debe cambiar el valor después de instalar los complementos.
HOST DEL SERVIDOR SNAPCENTER	Muestra la dirección IP o el nombre de host del servidor SnapCenter .
RUTA DEL ALMACÉN DE LLAVES SPL	Muestra la ruta absoluta del archivo del almacén de claves.

Nombre del parámetro	Descripción
PUERTO DEL SERVIDOR SNAPCENTER	Muestra el número de puerto en el que se ejecuta el servidor SnapCenter .
CONTEO MÁXIMO DE REGISTROS	Muestra la cantidad de archivos de registro del Loader de complementos de SnapCenter que se conservan en la carpeta */custom_location/snapcenter/spl/logs*. El valor predeterminado se establece en 5000. Si el recuento es mayor que el valor especificado, se conservan los últimos 5000 archivos modificados. La verificación de la cantidad de archivos se realiza automáticamente cada 24 horas desde que se inicia el servicio SnapCenter Plug-in Loader . Si elimina manualmente el archivo spl.properties, la cantidad de archivos que se conservarán se establecerá en 9999.
JAVA_HOME	Muestra la ruta absoluta del directorio JAVA_HOME que se utiliza para iniciar el servicio SPL. Esta ruta se determina durante la instalación y como parte del inicio de SPL.
TAMAÑO MÁXIMO DE REGISTRO	Muestra el tamaño máximo del archivo de registro de trabajo. Una vez que se alcanza el tamaño máximo, el archivo de registro se comprime y los registros se escriben en el nuevo archivo de ese trabajo.
RETENCIÓN DE REGISTROS DE LOS ÚLTIMOS DÍAS	Muestra el número de días que se conservan los registros.
HABILITAR VALIDACIÓN DE CERTIFICADO	Se muestra como verdadero cuando la validación del certificado CA está habilitada para el host. Puede habilitar o deshabilitar este parámetro editando spl.properties o utilizando la GUI o el cmdlet de SnapCenter .

Si alguno de estos parámetros no está asignado al valor predeterminado o si desea asignar o cambiar el valor, puede modificar el archivo spl.properties. También puede verificar el archivo spl.properties y editarlo para solucionar cualquier problema relacionado con los valores asignados a los parámetros. Después de modificar el archivo spl.properties, debe reiniciar el servicio SnapCenter Plug-in Loader .

Pasos

1. Realice una de las siguientes acciones, según sea necesario:
   - Inicie el servicio SnapCenter Plug-in Loader :
     - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - Detener el servicio de Loader de complementos de SnapCenter :
     - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     Puede utilizar la opción -force con el comando stop para detener a la fuerza el servicio SnapCenter Plug-in Loader . Sin embargo, debe tener cuidado antes de hacerlo porque también termina las operaciones existentes.

   - Reinicie el servicio del Loader de complementos de SnapCenter :
     - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
   - Encuentre el estado del servicio Loader de complementos de SnapCenter :
     - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
     - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
   - Encuentre el cambio en el servicio SnapCenter Plug-in Loader :
     - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
     - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configurar el certificado de CA con el servicio SnapCenter Plug-in Loader (SPL) en el host Linux

Debe administrar la contraseña del almacén de claves SPL y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza SPL y configurar el par de claves firmadas de CA para el almacén de confianza SPL con el servicio SnapCenter Plug-in Loader para activar el certificado digital instalado.

SPL utiliza el archivo 'keystore.jks', que se encuentra en '/var/opt/snapcenter/spl/etc' como almacén de confianza y almacén de claves.

Administrar la contraseña para el almacén de claves SPL y el alias del par de claves firmadas por la CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves SPL desde el archivo de propiedades SPL.

   Es el valor correspondiente a la clave 'SPL_KEYSTORE_PASS'.

2. Cambiar la contraseña del almacén de claves:

```
 keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña de todos los alias de las entradas de clave privada en el almacén de claves a la misma contraseña utilizada para el almacén de claves:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

   Actualice lo mismo para la clave SPL_KEYSTORE_PASS en el archivo spl.properties.

3. Reinicie el servicio después de cambiar la contraseña.

> La contraseña para el almacén de claves SPL y para todas las contraseñas de alias asociadas de la clave privada deben ser las mismas.

Configurar certificados raíz o intermedios para el almacén de confianza SPL

Debe configurar los certificados raíz o intermedios sin la clave privada en el almacén de confianza SPL.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves SPL: */var/opt/snapcenter/spl/etc*.
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
 keytool -list -v -keystore keystore.jks
. Agregar un certificado raíz o intermedio:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Reinicie el servicio después de configurar los certificados raíz o
intermedios en el almacén de confianza SPL.
```

Debe agregar el certificado de CA raíz y luego los certificados de CA intermedios.

Configurar el par de claves firmadas de CA para el almacén de confianza SPL

Debe configurar el par de claves firmadas por CA en el almacén de confianza SPL.

Pasos

1. Navegue a la carpeta que contiene el almacén de claves de SPL /var/opt/snapcenter/spl/etc.
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

```
 keytool -list -v -keystore keystore.jks
. Agregue el certificado CA que tenga clave privada y pública.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Enumere los certificados agregados en el almacén de claves.
```

```
 keytool -list -v -keystore keystore.jks
. Verifique que el almacén de claves contenga el alias correspondiente
al nuevo certificado de CA, que se agregó al almacén de claves.
. Cambie la contraseña de clave privada agregada para el certificado de
CA a la contraseña del almacén de claves.
```

La contraseña del almacén de claves SPL predeterminada es el valor de la clave SPL_KEYSTORE_PASS en el archivo spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Si el nombre de alias en el certificado de CA es largo y contiene
espacios o caracteres especiales ("*",","), cambie el nombre de alias a
un nombre simple:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure el nombre de alias desde el almacén de claves ubicado en el
archivo spl.properties.
```

Actualice este valor con la clave SPL_CERTIFICATE_ALIAS.

4. Reinicie el servicio después de configurar el par de claves firmadas por CA en el almacén de confianza SPL.

Configurar la lista de revocación de certificados (CRL) para SPL

Debe configurar la CRL para SPL

Acerca de esta tarea

- SPL buscará los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL para SPL es */var/opt/snapcenter/spl/etc/crl*.

Pasos

1. Puede modificar y actualizar el directorio predeterminado en el archivo spl.properties contra la clave SPL_CRL_PATH.
2. Puede colocar más de un archivo CRL en este directorio.

   Los certificados entrantes se verificarán con cada CRL.

Habilitar certificados CA para complementos

Debe configurar los certificados de CA e implementarlos en el servidor SnapCenter y en los hosts de complementos correspondientes. Debe habilitar la validación del certificado CA para los complementos.

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet run *Set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los complementos mediante *Get-SmCertificateSettings*.

La información sobre los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help command_name*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets del software SnapCenter" .

Pasos

1. En el panel de navegación izquierdo, haga clic en **Hosts**.
2. En la página Hosts, haga clic en **Hosts administrados**.
3. Seleccione uno o varios hosts de complementos.
4. Haga clic en **Más opciones**.
5. Seleccione **Habilitar validación de certificado**.

Después de terminar

La pestaña Hosts administrados muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del complemento.

- *  * indica que el certificado CA no está habilitado ni asignado al host del complemento.
- *  * indica que el certificado CA se ha validado correctamente.
- *  * indica que no se pudo validar el certificado CA.

- * 🔒 * indica que no se pudo recuperar la información de conexión.

> ⓘ Cuando el estado es amarillo o verde, las operaciones de protección de datos se completaron con éxito.