Configurar el certificado de CA

SnapCenter software

NetApp
November 06, 2025

Tabla de contenidos

Configurar el certificado de CA

Generar archivo CSR de certificado de CA

Puede generar una solicitud de firma de certificado (CSR) e importar el certificado que se puede obtener de una autoridad de certificación (CA) utilizando la CSR generada. El certificado tendrá una clave privada asociada.

CSR es un bloque de texto codificado que se entrega a un proveedor de certificados autorizado para obtener el certificado CA firmado.

La longitud de la clave RSA del certificado CA debe ser como mínimo de 3072 bits.

Para obtener información sobre cómo generar un CSR, consulte "Cómo generar un archivo CSR de certificado CA" .

Si posee el certificado CA para su dominio (*.domain.company.com) o su sistema (machine1.domain.company.com), puede omitir la generación del archivo CSR del certificado CA. Puede implementar el certificado CA existente con SnapCenter.

Para las configuraciones de clúster, el nombre del clúster (FQDN del clúster virtual) y los nombres de host respectivos deben mencionarse en el certificado de CA. El certificado se puede actualizar completando el campo Nombre alternativo del sujeto (SAN) antes de obtener el certificado. Para un certificado comodín (*.dominio.empresa.com), el certificado contendrá todos los nombres de host del dominio implícitamente.

Importar certificados de CA

Debe importar los certificados de CA al servidor SnapCenter y a los complementos del host de Windows mediante la consola de administración de Microsoft (MMC).

Pasos

1. Vaya a la consola de administración de Microsoft (MMC) y haga clic en **Archivo** > **Agregar o quitar complemento**.
2. En la ventana Agregar o quitar complementos, seleccione **Certificados** y luego haga clic en **Agregar**.
3. En la ventana del complemento Certificados, seleccione la opción **Cuenta de equipo** y haga clic en **Finalizar**.
4. Haga clic en **Consola raíz** > **Certificados – Equipo local** > **Autoridades de certificación raíz de confianza** > **Certificados**.
5. Haga clic con el botón derecho en la carpeta “Autoridades de certificación raíz de confianza” y luego seleccione **Todas las tareas** > **Importar** para iniciar el asistente de importación.
6. Complete el asistente de la siguiente manera:

En esta ventana del asistente…	Haz lo siguiente…
Importar clave privada	Seleccione la opción **Sí**, importe la clave privada y luego haga clic en **Siguiente**.

En esta ventana del asistente…	Haz lo siguiente…
Formato de archivo de importación	No realice cambios; haga clic en **Siguiente**.
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y luego haga clic en **Siguiente**.
Cómo completar el Asistente para importar certificados	Revise el resumen y luego haga clic en **Finalizar** para iniciar la importación.

El certificado de importación debe incluirse junto con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.p7b).

7. Repita el paso 5 para la carpeta “Personal”.

Obtenga la huella digital del certificado CA

Una huella digital de certificado es una cadena hexadecimal que identifica un certificado. La huella digital se calcula a partir del contenido del certificado utilizando un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la GUI:
   a. Haga doble clic en el certificado.
   b. En el cuadro de diálogo Certificado, haga clic en la pestaña **Detalles**.
   c. Desplácese por la lista de campos y haga clic en **Huella digital**.
   d. Copia los caracteres hexadecimales del cuadro.
   e. Eliminar los espacios entre los números hexadecimales.

      Por ejemplo, si la huella digital es: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", después de eliminar los espacios, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Realice lo siguiente desde PowerShell:
   a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado recientemente instalado por el nombre del sujeto.

      Get-ChildItem -Path Certificado:\LocalMachine\Mi

   b. Copiar la huella digital.

Configurar el certificado de CA con los servicios del complemento de host de Windows

Debe configurar el certificado CA con los servicios del complemento de host de Windows para activar el certificado digital instalado.

Realice los siguientes pasos en el servidor SnapCenter y en todos los hosts de complementos donde ya están implementados los certificados de CA.

Pasos

1. Elimine la vinculación del certificado existente con el puerto predeterminado 8145 de SMCore, ejecutando el siguiente comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Por ejemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Vincule el certificado recién instalado con los servicios del
   complemento de host de Windows, ejecutando los siguientes comandos:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Por ejemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Configurar el certificado CA para el servicio de complementos compatibles con NetApp en el host Linux

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

Los complementos utilizan el archivo 'keystore.jks', que se encuentra en */opt/ NetApp/snapcenter/scc/etc* como almacén de confianza y almacén de claves.

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

Pasos

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

de propiedades del agente del complemento.

Es el valor correspondiente a la clave '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_in_cert" -keystore keystore.jks
```

Actualice lo mismo para la clave KEYSTORE_PASS en el archivo *agent.properties*.

3. Reinicie el servicio después de cambiar la contraseña.

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

Configurar certificados raíz o intermedios para conectar el almacén de confianza

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

Pasos

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

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

4. Agregar un certificado raíz o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Reinicie el servicio después de configurar los certificados raíz o
intermedios para complementar el almacén de confianza.
```

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

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

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

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento /opt/NetApp/snapcenter/scc/etc.
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

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

4. Agregue el certificado CA que tenga clave privada y pública.

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

5. Enumere los certificados agregados en el almacén de claves.

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

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. 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 del complemento predeterminado es el valor de la clave KEYSTORE_PASS en el archivo agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -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 "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configure el nombre de alias del certificado de CA en el archivo
   agent.properties.
   ```

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

8. Reinicie el servicio después de configurar el par de claves firmadas por CA para complementar el almacén de confianza.

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

Acerca de esta tarea

- Los complementos de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos de SnapCenter es ' opt/NetApp/snapcenter/scc/etc/crl'.

Pasos

1. Puede modificar y actualizar el directorio predeterminado en el archivo agent.properties contra la clave CRL_PATH.

   Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán con cada CRL.

Configurar el certificado CA para el servicio de complementos compatibles con NetApp en el host de Windows

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

Los complementos utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* como almacén de confianza y almacén de claves.

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

Pasos

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

   Es el valor correspondiente a la clave *KEYSTORE_PASS*.

2. Cambiar la contraseña del almacén de claves:

   keytool -storepasswd -keystore keystore.jks

   > Si el comando "keytool" no se reconoce en el símbolo del sistema de Windows, reemplace el comando keytool con su ruta completa.

   C:\Archivos de programa\Java\<versión_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. 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 "nombre_alias_en_certificado" -keystore keystore.jks

   Actualice lo mismo para la clave KEYSTORE_PASS en el archivo *agent.properties*.

4. Reinicie el servicio después de cambiar la contraseña.

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

Configurar certificados raíz o intermedios para conectar el almacén de confianza

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

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localice el archivo 'keystore.jks'.
3. Enumere los certificados agregados en el almacén de claves:

   keytool -list -v -keystore keystore.jks

4. Agregar un certificado raíz o intermedio:

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

5. Reinicie el servicio después de configurar los certificados raíz o intermedios para complementar el almacén de confianza.

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

Configurar el par de claves firmadas por CA para el complemento de almacén de confianza

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

Pasos

1. Navegue hasta la carpeta que contiene el almacén de claves del complemento *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localice el archivo *keystore.jks*.
3. Enumere los certificados agregados en el almacén de claves:

   keytool -list -v -keystore keystore.jks

4. Agregue el certificado CA que tenga clave privada y pública.

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

5. Enumere los certificados agregados en el almacén de claves.

   keytool -list -v -keystore keystore.jks

6. Verifique que el almacén de claves contenga el alias correspondiente al nuevo certificado de CA, que se agregó al almacén de claves.
7. 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 del complemento predeterminado es el valor de la clave KEYSTORE_PASS en el archivo agent.properties.

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

8. Configure el nombre de alias del certificado de CA en el archivo *agent.properties*.

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

9. Reinicie el servicio después de configurar el par de claves firmadas por CA para complementar el almacén de confianza.

Configurar la lista de revocación de certificados (CRL) para los complementos de SnapCenter

Acerca de esta tarea

- Para descargar el último archivo CRL para el certificado CA relacionado, consulte "Cómo actualizar el archivo de lista de revocación de certificados en SnapCenter CA Certificate" .
- Los complementos de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de los complementos de SnapCenter es *'C:\Archivos de programa\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\crl'*.

Pasos

1. Puede modificar y actualizar el directorio predeterminado en el archivo *agent.properties* contra la clave 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.