Configurar certificado de CA

SnapCenter Software 5.0

NetApp
October 15, 2025

This PDF was generated from https://docs.netapp.com/es-es/snapcenter-50/protect-scc/reference_generate_CA_certificate_CSR_file.html on October 15, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Configurar certificado de CA . . . 1
- Genere un archivo CSR de certificado de CA . . . 1
- Importar certificados de CA . . . 1
- Obtenga la huella digital del certificado de CA . . . 2
- Configure el certificado de CA con servicios de plugins de host de Windows . . . 2
- Configure el certificado de CA para el servicio de plugins personalizados de SnapCenter en el host Linux . . . 3
  - Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso . . . 3
  - Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado . . . 4
  - Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado . . . 5
  - Configurar la lista de revocación de certificados (CRL) para los plugins personalizados de SnapCenter . . . 6
- Configure el certificado de CA para el servicio de plugins personalizados de SnapCenter en el host de Windows . . . 6
  - Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso . . . 6
  - Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado . . . 7
  - Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado . . . 7
  - Configurar la lista de revocación de certificados (CRL) para los plugins personalizados de SnapCenter . . . 8
- Habilite certificados de CA para plugins . . . 8

Configurar certificado de CA

Genere un archivo CSR de certificado de CA

Es posible generar una solicitud de firma de certificación (CSR) e importar el certificado que puede obtenerse de una entidad de certificación (CA) con la CSR generada. El certificado tendrá una clave privada asociada.

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

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

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

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

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

Importar certificados de CA

Debe importar los certificados de CA a SnapCenter Server y a los plugins de host de Windows mediante la consola de gestión de Microsoft (MMC).

Pasos

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

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

En esta ventana del asistente…	Haga lo siguiente…
Importar formato de archivo	No realice cambios; haga clic en **Siguiente**.
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y, a continuación, haga clic en **Siguiente**.
Finalización del Asistente para importación de certificados	Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la importación.

El certificado de importación se debe empaquetar 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 de 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 mediante un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la interfaz gráfica de usuario:
   a. Haga doble clic en el certificado.
   b. En el cuadro de diálogo Certificado, haga clic en la ficha **Detalles**.
   c. Desplácese por la lista de campos y haga clic en **Thumbprint**.
   d. Copie los caracteres hexadecimales del cuadro.
   e. Quite los espacios entre los números hexadecimales.

      Por ejemplo, si la huella digital es: "a9 09 50 2d 2a e4 e4 14 33 f8 38 86 b0 0d 42 77 a3 2a 7b", después de quitar los espacios, será: "a90d8 2dd82a41433e6f83886b00d4277a32a7b".

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

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie la huella digital.

Configure el certificado de CA con servicios de plugins de host de Windows

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

Realice los siguientes pasos en el servidor de SnapCenter y en todos los hosts del plugin donde ya se hayan implementado certificados de CA.

Pasos

1. Elimine el enlace existente del certificado con el puerto 8145 predeterminado de SMCore. Para ello, ejecute 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
   . Enlace el certificado recientemente instalado con los servicios de
   plugins del host de Windows mediante la ejecución de 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"
   ```

Configure el certificado de CA para el servicio de plugins personalizados de SnapCenter en el host Linux

Debe gestionar la contraseña del almacén de claves de los plugins personalizados y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios en el almacén de confianza de plugins personalizados y configurar la pareja de claves firmada de CA en el almacén de confianza de plugins personalizados con el servicio de plugins personalizados de SnapCenter para activar el certificado digital instalado.

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

Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso

Pasos

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

   Es el valor correspondiente a la clave 'KEYSTORE_PASS'.

2. Cambie la contraseña del almacén de claves:

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

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

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

3. Reinicie el servicio después de cambiar la contraseña.

> La contraseña para el almacén de claves de plugin personalizado y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado

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

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado: /Opt/NetApp/snapcenter/scc/etc.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

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

4. Añada 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 en el almacén de confianza del plugin personalizado.
   ```

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

Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado /opt/NetApp/snapcenter/scc/etc.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

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

4. Agregue el certificado de CA con clave pública y privada.

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

5. Enumere los certificados añadidos al almacén de claves.

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

6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.
7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

   La contraseña predeterminada del plugin personalizado keystore es el valor de key KEYSTORE_PASS en el archivo agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Si el nombre del alias del certificado de CA es largo y contiene
   espacio o caracteres especiales ("*",","), cambie el nombre del alias
   por un nombre simple:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configure el nombre del 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 firmado de CA en el almacén de confianza del plugin personalizado.

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

Acerca de esta tarea

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

Pasos

1. Puede modificar y actualizar el directorio predeterminado del archivo agent.properties en función de la CLAVE CRL_PATH.

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

Configure el certificado de CA para el servicio de plugins personalizados de SnapCenter en el host de Windows

Debe gestionar la contraseña del almacén de claves de los plugins personalizados y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios en el almacén de confianza de plugins personalizados y configurar la pareja de claves firmada de CA en el almacén de confianza de plugins personalizados con el servicio de plugins personalizados de SnapCenter para activar el certificado digital instalado.

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

Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso

Pasos

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

   Es el valor que corresponde a la clave *KEYSTORE_PASS*.

2. Cambie la contraseña del almacén de claves:

   keytool -storepasswd -keystore.jks

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

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

3. Cambie la contraseña para todos los alias de las entradas de clave privada en el almacén de claves por la misma contraseña utilizada para el almacén de claves:

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

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

4. Reinicie el servicio después de cambiar la contraseña.

> La contraseña para el almacén de claves de plugin personalizado y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado

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

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

   keytool -list -v -keystore.jks

4. Añada un certificado raíz o intermedio:

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

5. Reinicie el servicio después de configurar los certificados raíz o intermedios en el almacén de confianza del plugin personalizado.

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

Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Busque el archivo *keystore.jks*.
3. Enumere los certificados añadidos al almacén de claves:

   keytool -list -v -keystore.jks

4. Agregue el certificado de CA con clave pública y privada.

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

5. Enumere los certificados añadidos al almacén de claves.

keytool -list -v -keystore.jks

6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.
7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

   La contraseña predeterminada del plugin personalizado keystore es el valor de key KEYSTORE_PASS en el archivo agent.properties.

   Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks

8. Configure el nombre del 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 firmado de CA en el almacén de confianza del plugin personalizado.

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

Acerca de esta tarea

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

Pasos

1. Puede modificar y actualizar el directorio predeterminado del archivo *agent.properties* en función de la CLAVE CRL_PATH.
2. Puede colocar más de un archivo CRL en este directorio.

   Los certificados entrantes se verificarán en cada CRL.

Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

Antes de empezar

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet run *set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los plugins con el *Get-SmCertificateSettings*.

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

Pasos

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. En la página hosts, haga clic en **Managed hosts**.
3. Seleccione uno o varios hosts de plugins.
4. Haga clic en **más opciones**.
5. Seleccione **Activar validación de certificados**.

Después de terminar

El host de la pestaña Managed hosts muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del plugin.

- * * Indica que el certificado de CA no está habilitado ni asignado al host del plugin.
- * * Indica que el certificado CA se ha validado correctamente.
- * * Indica que el certificado CA no se pudo validar.
- * * indica que no se ha podido recuperar la información de conexión.

> Cuando el estado es amarillo o verde, las operaciones de protección de datos se completan correctamente.

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.