Configure la autenticación basada en certificados

SnapCenter Software 4.9

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/es-es/snapcenter-49/install/task_export_ca_certificates_from_snapcenter_server.html on September 26, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Configure la autenticación basada en certificados . . . 1
- Exporte certificados de entidad de certificación (CA) del servidor SnapCenter . . . 1
- Importe el certificado de una entidad de certificación (CA) en los hosts del plugin de Windows . . . 2
- Importe el certificado de CA a los plugins de host UNIX y configure los certificados raíz o intermedios en el almacén de confianza de SPL . . . 2
  - Importe el certificado de CA en los hosts del plugin UNIX . . . 2
  - Configure los certificados intermedios o de raíz para el almacén de confianza SPL . . . 3
- Habilite la autenticación basada en certificados . . . 4

Configure la autenticación basada en certificados

Exporte certificados de entidad de certificación (CA) del servidor SnapCenter

Es necesario exportar los certificados de CA del servidor de SnapCenter a los hosts del plugin mediante la consola de gestión de Microsoft (MMC).

Antes de empezar

Debe haber configurado el SSL bidireccional.

- 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 Certificados Snap-in, seleccione la opción **Cuenta de computadora** y luego haga clic en **Finalizar**.
  4. Haga clic en **Console root** > **Certificados - Equipo local** > **Personal** > **Certificados**.
  5. Haga clic con el botón derecho en el certificado de CA adquirido, que se utiliza para el servidor SnapCenter y, a continuación, seleccione **Todas las tareas** > **Exportar** para iniciar el asistente de exportación.
  6. Realice las siguientes acciones en el asistente.

Para esta opción…	Haga lo siguiente…
Exportar clave privada	Seleccione **No, no exporte la clave privada** y luego haga clic en **Siguiente**.
Exportar formato de archivo	Haga clic en **Siguiente**.
Nombre de archivo	Haga clic en **Examinar** y especifique la ruta del archivo para guardar el certificado, y haga clic en **Siguiente**.
Finalización del Asistente para exportación de certificados	Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la exportación.

La autenticación basada en certificados no se admite para las configuraciones de alta disponibilidad de SnapCenter y el plugin de SnapCenter para VMware vSphere.

Importe el certificado de una entidad de certificación (CA) en los hosts del plugin de Windows

Para usar el certificado de CA de servidor de SnapCenter exportado, es necesario importar el certificado relacionado a los hosts del plugin de Windows de SnapCenter 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 Certificados Snap-in, seleccione la opción **Cuenta de computadora** y luego haga clic en **Finalizar**.
  4. Haga clic en **Console root** > **Certificados - Equipo local** > **Personal** > **Certificados**.
  5. Haga clic con el botón derecho en la carpeta “Personal” y seleccione **Todas las tareas** > **Importar** para iniciar el asistente de importación.
  6. Realice las siguientes acciones en el asistente.

Para esta opción…	Haga lo siguiente…
Ubicación de tienda	Haga clic en **Siguiente**.
Archivo para importar	Seleccione el certificado de servidor SnapCenter que termina con la extensión .cer.
Almacén de certificados	Haga clic en **Siguiente**.
Finalización del Asistente para exportación de certificados	Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la importación.

Importe el certificado de CA a los plugins de host UNIX y configure los certificados raíz o intermedios en el almacén de confianza de SPL

Importe el certificado de CA en los hosts del plugin UNIX

Debe importar el certificado de CA a los hosts del plugin de UNIX.

Acerca de esta tarea

- Puede gestionar la contraseña del almacén de claves del SPL y el alias de la pareja de claves firmada de CA en uso.
- La contraseña para el almacén de claves SPL y para toda la contraseña de alias asociada de la clave privada deben ser la misma.

- Pasos*

1. Puede recuperar la contraseña predeterminada del almacén de claves del SPL desde el archivo de propiedades del SPL. Es el valor correspondiente a la clave `SPL_KEYSTORE_PASS`.
2. Cambie la contraseña del almacén de claves: `$ keytool -storepasswd -keystore 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>" -keystore keystore.jks`
4. Actualice lo mismo para la clave spl_KEYSTORE_PASS IN `spl.properties` archivo.
5. Reinicie el servicio después de cambiar la contraseña.

Configure los certificados intermedios o de raíz para el almacén de confianza SPL

Debe configurar los certificados intermedios o raíz para el almacén de confianza de SPL. Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

- Pasos*

1. Desplácese hasta la carpeta que contiene el almacén de claves de SPL: `/var/opt/snapcenter/spl/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 <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. Reinicie el servicio después de configurar los certificados raíz o intermedios en el almacén de confianza de SPL.

Configure la pareja de claves firmados de CA para el almacén de confianza SPL

Debe configurar el par de claves firmado de CA como el almacén de confianza del SPL.

- Pasos*

1. Navegue a la carpeta que contiene el almacén de claves del SPL `/var/opt/snapcenter/spl/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 <CertificatePathToImport> -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 almacén de claves de SPL es el valor de la clave spl_KEYSTORE_PASS in `spl.properties` archivo.

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks`
```

1. 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 "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
2. Configure el nombre de alias desde el almacén de claves ubicado en `spl.properties` archivo. Actualice este valor contra la clave SPL_CERTIFICATE_ALIAS.
3. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza SPL.

Habilite la autenticación basada en certificados

Para habilitar la autenticación basada en certificados para SnapCenter Server y los hosts del plugin de Windows, ejecute el siguiente cmdlet de PowerShell. Para los hosts del plugin de Linux, se habilita la autenticación basada en certificado cuando se habilita SSL bidireccional.

- Para habilitar la autenticación basada en certificados de cliente:

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- Para desactivar la autenticación basada en certificados de cliente:

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

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.