# Configure la autenticación basada en certificados

SnapCenter Software 5.0

NetApp
July 18, 2024

# Tabla de contenidos

# 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 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`
4. Actualice lo mismo con la clave spl_KEYSTORE_PASS en `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. Navegue a la carpeta que contiene el almacén de claves SPL `/var/opt/snapcenter/spl/etc`: .
2. Busque el archivo `keystore.jks`.
3. Enumere los certificados agregados en el almacén de claves: `$ keytool -list -v -keystore keystore.jks`
4. Agregue 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 agregados en el almacén de claves: `$ keytool -list -v -keystore keystore.jks`
4. Agregue el certificado de CA que tenga la clave privada y pública. `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. Enumere los certificados agregados en el 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 en `spl.properties` archivo.

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

1. Si el nombre del alias del certificado de CA es largo y contiene espacios 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 del alias desde el almacén de claves ubicado en `spl.properties` el 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



## Información de la marca comercial