Configurar el certificado CA para el host de Windows

SnapCenter software

NetApp
November 06, 2025

Tabla de contenidos

Configurar el certificado CA para el host de Windows

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**.
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 de CA con el sitio de SnapCenter

Debe configurar el certificado CA con el sitio SnapCenter en el host de Windows.

Pasos

1. Abra el Administrador de IIS en el servidor Windows donde está instalado SnapCenter .
2. En el panel de navegación izquierdo, haga clic en **Conexiones**.
3. Amplíe el nombre del servidor y **Sitios**.
4. Seleccione el sitio web de SnapCenter en el que desea instalar el certificado SSL.

5. Vaya a **Acciones** > **Editar sitio** y haga clic en **Enlaces**.
6. En la página Enlaces, seleccione **enlace para https**.
7. Haga clic en **Editar**.
8. En la lista desplegable del certificado SSL, seleccione el certificado SSL importado recientemente.
9. Haga clic en **Aceptar**.

> El sitio del Programador de SnapCenter (puerto predeterminado: 8154, HTTPS) está configurado con un certificado autofirmado. Este puerto se comunica dentro del host del servidor SnapCenter y no es obligatorio configurarlo con un certificado CA. Sin embargo, si su entorno le exige utilizar un certificado CA, repita los pasos 5 a 9 utilizando el sitio del Programador de SnapCenter .

> Si el certificado CA implementado recientemente no aparece en el menú desplegable, verifique si el certificado CA está asociado con la clave privada.

> Asegúrese de que el certificado se agregue mediante la siguiente ruta: **Raíz de consola > Certificados – Equipo local > Autoridades de certificación raíz de confianza > Certificados**.

Habilitar certificados CA para SnapCenter

Debe configurar los certificados de CA y habilitar la validación de certificados de CA para el servidor SnapCenter .

Antes de empezar

- Puede habilitar o deshabilitar los certificados de CA mediante el cmdlet Set-SmCertificateSettings.
- Puede mostrar el estado del certificado para el servidor SnapCenter mediante el cmdlet 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, puede consultar la "Guía de referencia de cmdlets del software SnapCenter" .

Pasos

1. En la página Configuración, navegue a **Configuración** > **Configuración global** > **Configuración del certificado CA**.
2. Seleccione **Habilitar validación de certificado**.
3. Haga clic en **Aplicar**.

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 no hay ningún certificado CA habilitado o 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.