



Configure y habilite la comunicación SSL bidireccional

SnapCenter Software 5.0

NetApp
July 18, 2024

Tabla de contenidos

- Configure y habilite la comunicación SSL bidireccional 1
 - Configure la comunicación SSL bidireccional 1
 - Active la comunicación SSL bidireccional 3

Configure y habilite la comunicación SSL bidireccional

Configure la comunicación SSL bidireccional

Debe configurar la comunicación SSL bidireccional para asegurar la comunicación mutua entre el servidor de SnapCenter y los plugins.

Antes de empezar

- Generó el archivo CSR de certificado de CA con la longitud mínima admitida de clave de 3072.
- El certificado de CA debe admitir la autenticación de servidor y la autenticación de cliente.
- Debe tener un certificado de CA con detalles de clave privada y huella digital.
- Debe haber activado la configuración SSL unidireccional.

Para obtener información detallada, consulte ["Configurar sección de certificado de CA."](#)

- Debe haber habilitado la comunicación SSL bidireccional en todos los hosts del plugin y el servidor de SnapCenter.

El entorno con algunos hosts o servidor no habilitado para la comunicación SSL bidireccional no está soportado.

• Pasos*

1. Para enlazar el puerto, ejecute los siguientes pasos en el host de servidor SnapCenter para el puerto 8146 del servidor web IIS de SnapCenter (predeterminado) y otra vez para el puerto 8145 de SMCore (predeterminado) mediante comandos de PowerShell.

- a. Quite la vinculación de puertos de certificado autofirmado de SnapCenter existente mediante el siguiente comando de PowerShell.

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
```

Por ejemplo:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

```
> netsh http delete sslcert ipport=0.0.0.0:8146
```

- b. Enlace el certificado de CA recién adquirido con el servidor SnapCenter y el puerto SMCore.

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>  
certhash=$certappid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

Por ejemplo:

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8146
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

2. Para acceder al permiso al certificado de CA, añada el usuario del servidor web IIS predeterminado «**IIS AppPool\SnapCenter**» de SnapCenter en la lista de permisos de certificados siguiendo los siguientes pasos para acceder al certificado de CA recién adquirido.
 - a. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo > Agregar o quitar SnapIn**.
 - b. En la ventana Agregar o quitar complementos, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
 - c. En la ventana del complemento certificados, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
 - d. Haga clic en **raíz de consola > certificados – Equipo local > personal > certificados**.
 - e. Seleccione el certificado SnapCenter.
 - f. Para iniciar el asistente para agregar usuarios/permisos, haga clic con el botón derecho en el certificado de CA y seleccione **Todas las tareas > Gestionar claves privadas**.
 - g. Haga clic en **Agregar**, en el Asistente de selección de usuarios y grupos cambie la ubicación a nombre de equipo local (en la parte superior de la jerarquía)
 - h. Añada el usuario IIS AppPool\SnapCenter y proporcione permisos de control completos.
3. Para el permiso IIS del certificado **CA**, agregue la nueva entrada de claves de registro DWORD en el servidor SnapCenter desde la siguiente ruta:

En el editor del registro de Windows, vaya a la ruta mencionada a continuación,

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityPro  
viders\SCHANNEL
```

4. Cree una nueva entrada de clave de registro DWORD en el contexto de la configuración del registro SCHANNEL.

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

Configure el plugin de Windows de SnapCenter para la comunicación SSL bidireccional

Es necesario configurar el plugin de Windows de SnapCenter para la comunicación SSL bidireccional mediante comandos de PowerShell.

Antes de empezar

Asegúrese de que la huella digital del certificado de CA esté disponible.

- Pasos*

1. Para enlazar el puerto, realice las siguientes acciones en el host del plugin de Windows para el puerto SMCORE 8145 (predeterminado).

- a. Quite la vinculación de puertos de certificado autofirmado de SnapCenter existente mediante el siguiente comando de PowerShell.

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

Por ejemplo:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- b. Enlace el certificado de CA recién adquirido con el puerto SMCORE.

```
> $cert = "<CA_certificate thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert  
appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

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

Por ejemplo:

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

Active la comunicación SSL bidireccional

Es posible habilitar la comunicación SSL bidireccional para proteger la comunicación mutua entre el servidor SnapCenter y los plugins mediante comandos de PowerShell.

Antes de empezar

Ejecute los comandos para todos los plugins y el agente de SMCORE primero y luego para el servidor.

- Pasos*

1. Para habilitar la comunicación SSL bidireccional, ejecute los siguientes comandos en el servidor de SnapCenter para los plugins, el servidor y para cada uno de los agentes para los que se necesita la comunicación SSL bidireccional.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName <Plugin_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

1. Realice la operación de reciclaje del pool de aplicaciones de SnapCenter de IIS con el siguiente comando. > Restart-WebAppPool -Name "SnapCenter"
2. Para los plugins de Windows, reinicie el servicio SMCORE ejecutando el siguiente comando de PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Desactive la comunicación SSL bidireccional

Puede deshabilitar la comunicación SSL bidireccional mediante comandos de PowerShell.

Acerca de esta tarea

- Ejecute los comandos para todos los plugins y el agente de SMCORE primero y luego para el servidor.
- Cuando deshabilita la comunicación SSL bidireccional, el certificado de CA y su configuración no se eliminan.
- Para añadir un nuevo host a SnapCenter Server, es necesario deshabilitar el SSL bidireccional para todos los hosts del plugin.
- NLB y F5 no son compatibles.

- Pasos*

1. Para deshabilitar la comunicación SSL bidireccional, ejecute los siguientes comandos en servidor de SnapCenter para todos los hosts del plugin y el host de SnapCenter.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName <Agent_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

1. Realice la operación de reciclaje del pool de aplicaciones de SnapCenter de IIS con el siguiente

comando. > Restart-WebAppPool -Name "SnapCenter"

2. Para los plugins de Windows, reinicie el servicio SMCORE ejecutando el siguiente comando de PowerShell:

> Restart-Service -Name SnapManagerCoreService

Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.