



Configure y habilite la comunicación SSL bidireccional en el host Linux

SnapCenter Software 6.0

NetApp
July 23, 2024

Tabla de contenidos

- Configure y habilite la comunicación SSL bidireccional en el host Linux 1
 - Configure la comunicación SSL bidireccional en el host Linux 1
 - Active la comunicación SSL en el host Linux 2

Configure y habilite la comunicación SSL bidireccional en el host Linux

Configure la comunicación SSL bidireccional en el host Linux

Debe configurar la comunicación SSL bidireccional para proteger la comunicación mutua entre el servidor de SnapCenter en el host de Linux y los plugins.

Antes de empezar

- Debe haber configurado el certificado de CA para el host Linux.
- Debe haber habilitado la comunicación SSL bidireccional en todos los hosts del plugin y el servidor de SnapCenter.

Pasos


1. Copie **certificate.pem** a `/etc/pki/ca-trust/source/anchors/`.
2. Añada los certificados en la lista de confianza del host Linux.
 - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
 - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
 - `update-ca-trust extract`
3. Compruebe si los certificados se han agregado a la lista de confianza. `trust list | grep "<CN of your certificate>"`
4. Actualice **ssl_certificate** y **ssl_certificate_key** en el archivo **nginx** de SnapCenter y reinicie.
 - `vim /etc/nginx/conf.d/snapcenter.conf`
 - `systemctl restart nginx`
5. Actualice el enlace de la GUI del servidor de SnapCenter.
6. Actualice los valores de las siguientes claves en **snapmanager.web.ui.dll.config** que están ubicadas en `_/<installation path>/NetApp/snapcenter/SnapManagerWeb_` y **SMCoreServiceHost.dll.config** que están ubicadas en `_/<installation path>/NetApp/snapcenter/SMCore`.
 - `<add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />`
 - `<add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>" />`
7. Reinicie los siguientes servicios.
 - `systemctl restart smcore.service`
 - `systemctl restart snapmanagerweb.service`
8. Compruebe que el certificado esté conectado al puerto web de SnapManager. `openssl s_client -connect localhost:8146 -brief`
9. Compruebe que el certificado está conectado al puerto smcore. `openssl s_client -connect localhost:8145 -brief`
10. Gestione la contraseña del almacén de claves y el alias de SPL.

- a. Recuperar la contraseña predeterminada del almacén de claves SPL asignada a la clave **spl_KEYSTORE_PASS** en el archivo de propiedades spl.
 - b. Cambie la contraseña del almacén de claves. `keytool -storepasswd -keystore keystore.jks`
 - c. Cambie la contraseña de todos los alias de las entradas de clave privada. `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
 - d. Actualice la misma contraseña para la clave **spl_KEYSTORE_PASS** en *spl.properties*.
 - e. Reinicie el servicio.
11. En el host Linux del plugin, añada los certificados raíz e intermedios en el almacén de claves del plugin de SPL.
- `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
 - `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`
 - i. Compruebe las entradas en keystore.jks. `keytool -list -v -keystore <path to keystore.jks>`
 - ii. Cambie el nombre de cualquier alias si es necesario. `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. Actualice el valor de **spl_CERTIFICATE_ALIAS** en el archivo *spl.properties* con el alias **certificate.pfx** almacenado en *keystore.jks* y reinicie el servicio spl: `systemctl restart spl`
13. Compruebe que el certificado está conectado al puerto smcore. `openssl s_client -connect localhost:8145 -brief`

Active la comunicación SSL en el host Linux

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

Paso

1. Realice lo siguiente para activar la comunicación SSL unidireccional.
 - a. Inicie sesión en la GUI de SnapCenter.
 - b. Haga clic en **Ajustes > Ajustes globales** y seleccione **Habilitar validación de certificados en el servidor SnapCenter**.
 - c. Haga clic en **Hosts > Managed Hosts** y seleccione el host del plugin para el que desea habilitar SSL unidireccional.
 - d. Haga clic en  el icono y, a continuación, haga clic en **Habilitar validación de certificado**.
2. Active la comunicación SSL bidireccional desde el host Linux del servidor SnapCenter.
 - `Open-SmConnection`

- `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin Host Name>`
- `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost`
- `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

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.