



Konfigurieren und aktivieren Sie die bidirektionale SSL-Kommunikation auf dem Linux-Host

SnapCenter Software 6.0

NetApp
July 23, 2024

Inhalt

- Konfigurieren und aktivieren Sie die bidirektionale SSL-Kommunikation auf dem Linux-Host 1
- Konfigurieren Sie die bidirektionale SSL-Kommunikation auf dem Linux-Host 1
- Aktivieren Sie die SSL-Kommunikation auf Linux-Host 2

Konfigurieren und aktivieren Sie die bidirektionale SSL-Kommunikation auf dem Linux-Host

Konfigurieren Sie die bidirektionale SSL-Kommunikation auf dem Linux-Host

Sie sollten die bidirektionale SSL-Kommunikation konfigurieren, um die gegenseitige Kommunikation zwischen SnapCenter-Server auf Linux-Host und den Plug-ins zu sichern.

Bevor Sie beginnen

- Sie sollten das CA-Zertifikat für den Linux-Host konfiguriert haben.
- Sie müssen die bidirektionale SSL-Kommunikation auf allen Plug-in-Hosts und dem SnapCenter-Server aktiviert haben.

Schritte

1. Kopieren Sie **Certificate.pem** nach `/etc/pki/Ca-Trust/source/Anchors/`.
2. Fügen Sie die Zertifikate in die Vertrauensliste Ihres Linux-Hosts ein.
 - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
 - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
 - `update-ca-trust extract`
3. Überprüfen Sie, ob die Zertifikate zur Vertrauensliste hinzugefügt wurden. `trust list | grep "<CN of your certificate>"`
4. Aktualisieren Sie **ssl_Certificate** und **ssl_Certificate_key** in der SnapCenter **nginx**-Datei und starten Sie neu.
 - `vim /etc/nginx/conf.d/snapcenter.conf`
 - `systemctl restart nginx`
5. Aktualisieren Sie den GUI-Link des SnapCenter-Servers.
6. Aktualisieren Sie die Werte der folgenden Schlüssel in **SnapManager.Web.UI.dll.config** unter `<installation path>/NetApp/snapcenter/SnapManagerWeb_` und **SMCoreServiceHost.dll.config** unter `<installation path>/NetApp/snapcenter/SMCore`.
 - `<add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />`
 - `<add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>`
7. Starten Sie die folgenden Dienste neu.
 - `systemctl restart smcore.service`
 - `systemctl restart snapmanagerweb.service`
8. Vergewissern Sie sich, dass das Zertifikat an den SnapManager-Webport angeschlossen ist. `openssl s_client -connect localhost:8146 -brief`
9. Vergewissern Sie sich, dass das Zertifikat an den smcore-Port angeschlossen ist. `openssl s_client`

```
-connect localhost:8145 -brief
```

10. Kennwort für SPL-Keystore und Alias verwalten.

- a. Rufen Sie das SPL-Keystore-Standardpasswort ab, das dem Schlüssel **SPL_KEYSTORE_PASS** in der SPL-Eigenschaftsdatei zugewiesen wurde.
- b. Ändern Sie das Passwort für den Keystore. `keytool -storepasswd -keystore keystore.jks`
- c. Ändern Sie das Passwort für alle Aliase von privaten Schlüsseleinträgen. `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
- d. Aktualisieren Sie dasselbe Passwort für den Schlüssel **SPL_KEYSTORE_PASS** in *spl.properties*.
- e. Starten Sie den Dienst neu.

11. Fügen Sie auf dem Plug-in-Linux-Host die Root- und Zwischenzertifikate im Keystore des SPL-Plug-ins hinzu.

- ° `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. Überprüfen Sie die Einträge in *keystore.jks*. `keytool -list -v -keystore <path to keystore.jks>`
 - ii. Benennen Sie bei Bedarf alle Alias um. `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`


12. Aktualisieren Sie den Wert von **SPL_CERTIFICATE_ALIAS** in der Datei *spl.properties* mit dem Alias **Certificate.pfx**, der in *keystore.jks* gespeichert ist, und starten Sie den SPL-Dienst neu: `systemctl restart spl`

13. Vergewissern Sie sich, dass das Zertifikat an den smcore-Port angeschlossen ist. `openssl s_client -connect localhost:8145 -brief`

Aktivieren Sie die SSL-Kommunikation auf Linux-Host

Sie können bidirektionale SSL-Kommunikation aktivieren, um die gegenseitige Kommunikation zwischen SnapCenter Server auf Linux-Host und den Plug-ins mithilfe von PowerShell-Befehlen zu sichern.

Schritt

1. Führen Sie die folgenden Schritte aus, um die einfache SSL-Kommunikation zu aktivieren.
 - a. Melden Sie sich bei der SnapCenter GUI an.
 - b. Klicken Sie auf **Einstellungen > Globale Einstellungen** und wählen Sie **Zertifikatvalidierung auf dem SnapCenter-Server aktivieren**.
 - c. Klicken Sie auf **Hosts > verwaltete Hosts** und wählen Sie den Plug-in-Host aus, für den Sie One-Way-SSL aktivieren möchten.
 - d. Klicken Sie auf das  Symbol, und klicken Sie dann auf **Zertifikatvalidierung aktivieren**.

2. Aktivieren Sie die bidirektionale SSL-Kommunikation vom SnapCenter-Server-Linux-Host.

- `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"}`

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.