



Configurare e abilitare la comunicazione SSL bidirezionale su host Linux

SnapCenter Software 6.0

NetApp
July 23, 2024

Sommario

- Configurare e abilitare la comunicazione SSL bidirezionale su host Linux 1
 - Configurare la comunicazione SSL bidirezionale sull'host Linux 1
 - Abilitare la comunicazione SSL sull'host Linux 2

Configurare e abilitare la comunicazione SSL bidirezionale su host Linux

Configurare la comunicazione SSL bidirezionale sull'host Linux

È necessario configurare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra il server SnapCenter su host Linux e i plug-in.

Prima di iniziare

- Il certificato CA dovrebbe essere stato configurato per l'host Linux.
- È necessario attivare la comunicazione SSL bidirezionale su tutti gli host plug-in e sul server SnapCenter.

Fasi


1. Copiare **certificate.pem** in `/etc/pki/ca-trust/source/anchors/`.
2. Aggiungere i certificati nell'elenco di attendibilità dell'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. Verificare se i certificati sono stati aggiunti all'elenco dei certificati attendibili. `trust list | grep "<CN of your certificate>"`
4. Aggiornare **ssl_certificate** e **ssl_certificate_key** nel file SnapCenter **nginx** e riavviare.
 - `vim /etc/nginx/conf.d/snapcenter.conf`
 - `systemctl restart nginx`
5. Aggiornare il collegamento della GUI del server SnapCenter.
6. Aggiornare i valori delle seguenti chiavi in **SnapManager.Web.UI.dll.config** situato in `_/<installation path>/NetApp/snapcenter/SnapManagerWeb_` e **SMCoreServiceHost.dll.config** situato in `_/<installation path>/NetApp/snapcenter/SMCore`.
 - `<add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />`
 - `<add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>`
7. Riavviare i seguenti servizi.
 - `systemctl restart smcore.service`
 - `systemctl restart snapmanagerweb.service`
8. Verificare che il certificato sia collegato alla porta Web SnapManager. `openssl s_client -connect localhost:8146 -brief`
9. Verificare che il certificato sia collegato alla porta smcore. `openssl s_client -connect localhost:8145 -brief`
10. Gestisci password per archivio chiavi e alias SPL.
 - a. Recuperare la password predefinita del keystore SPL assegnata alla chiave **SPL_KEYSTORE_PASS** nel file di proprietà SPL.

- b. Modificare la password dell'archivio chiavi. `keytool -storepasswd -keystore keystore.jks`
 - c. Modificare la password per tutti gli alias delle voci di chiave privata. `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
 - d. Aggiorna la stessa password per la chiave **SPL_KEYSTORE_PASS** in *spl.properties*.
 - e. Riavviare il servizio.
11. Sul plug-in host Linux, aggiungere i certificati root e intermedi nel keystore del plug-in 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. Controllare le voci in keystore.jks. `keytool -list -v -keystore <path to keystore.jks>`
 - ii. Se necessario, rinominare qualsiasi alias. `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. Aggiornare il valore di **SPL_CERTIFICATE_ALIAS** nel file *spl.properties* con l'alias di **certificate.pfx** memorizzato in *keystore.jks* e riavviare il servizio SPL: `systemctl restart spl`
13. Verificare che il certificato sia collegato alla porta smcore. `openssl s_client -connect localhost:8145 -brief`

Abilitare la comunicazione SSL sull'host Linux

È possibile abilitare la comunicazione bidirezionale SSL per proteggere la comunicazione reciproca tra il server SnapCenter su host Linux e i plug-in utilizzando i comandi PowerShell.

Fase

1. Per attivare la comunicazione SSL unidirezionale, procedere come segue.
 - a. Accedere alla GUI di SnapCenter.
 - b. Fare clic su **Impostazioni > Impostazioni globali** e selezionare **attiva convalida certificato sul server SnapCenter**.
 - c. Fare clic su **hosts > Managed hosts** e selezionare l'host plug-in per cui si desidera abilitare SSL unidirezionale.
 - d. Fare clic  sull'icona, quindi su **Abilita convalida certificato**.
2. Abilitare la comunicazione bidirezionale SSL dall'host SnapCenter Server Linux.
 - `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"}`

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.