



Configurez et activez la communication SSL bidirectionnelle sur l'hôte Linux

SnapCenter Software 6.0

NetApp
July 23, 2024

Sommaire

- Configurez et activez la communication SSL bidirectionnelle sur l'hôte Linux 1
- Configurez la communication SSL bidirectionnelle sur l'hôte Linux 1
- Activez la communication SSL sur l'hôte Linux 2

Configurez et activez la communication SSL bidirectionnelle sur l'hôte Linux

Configurez la communication SSL bidirectionnelle sur l'hôte Linux

Vous devez configurer la communication SSL bidirectionnelle pour sécuriser la communication mutuelle entre le serveur SnapCenter sur l'hôte Linux et les plug-ins.

Avant de commencer

- Vous devez avoir configuré le certificat CA pour l'hôte Linux.
- Vous devez avoir activé la communication SSL bidirectionnelle sur tous les hôtes de plug-in et sur le serveur SnapCenter.

Étapes

1. Copiez **certificate.pem** dans `/etc/pki/ca-trust/source/anchors/`.
2. Ajoutez les certificats dans la liste de confiance de votre hôte 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. Vérifiez si les certificats ont été ajoutés à la liste de confiance. `trust list | grep "<CN of your certificate>"`
4. Mettez à jour **ssl_certificate** et **ssl_certificate_key** dans le fichier SnapCenter **nginx** et redémarrez.
 - `vim /etc/nginx/conf.d/snapcenter.conf`
 - `systemctl restart nginx`
5. Actualisez le lien de l'interface graphique du serveur SnapCenter.
6. Mettez à jour les valeurs des clés suivantes dans **SnapManager.Web.UI.dll.config** situées à l'adresse `<installation path>/NetApp/snapcenter/SnapManagerWeb_` et **SMCoreServiceHost.dll.config** situées à l'adresse `<installation path>/NetApp/snapcenter/SMCore`.
 - `<add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />`
 - `<add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>" />`
7. Redémarrez les services suivants.
 - `systemctl restart smcore.service`
 - `systemctl restart snapmanagerweb.service`
8. Vérifiez que le certificat est connecté au port Web SnapManager. `openssl s_client -connect localhost:8146 -brief`
9. Vérifiez que le certificat est connecté au port smcore. `openssl s_client -connect localhost:8145 -brief`
10. Gérer le mot de passe pour la base de stockage de clés SPL et l'alias.

- a. Récupérer le mot de passe par défaut de la SPL KEYSTORE attribué à la clé **SPL_KEYSTORE_PASS** dans le fichier de propriétés de la SPL.
 - b. Modifiez le mot de passe de la base de stockage de clés. `keytool -storepasswd -keystore keystore.jks`
 - c. Modifiez le mot de passe pour tous les alias des entrées de clé privée. `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
 - d. Mettez à jour le même mot de passe pour la clé **SPL_KEYSTORE_PASS** dans *spl.properties*.
 - e. Redémarrez le service.
11. Sur l'hôte Linux du plug-in, ajoutez les certificats racine et intermédiaire dans la base de stockage de clés du 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. Vérifiez les entrées dans *keystore.jks*. `keytool -list -v -keystore <path to keystore.jks>`
 - ii. Renommez tout alias si nécessaire. `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. Mettez à jour la valeur de **SPL_CERTIFICATE_ALIAS** dans le fichier *spl.properties* avec l'alias de **certificate.pfx** stocké dans *keystore.jks* et redémarrez le service SPL : `systemctl restart spl`
13. Vérifiez que le certificat est connecté au port smcore. `openssl s_client -connect localhost:8145 -brief`

Activez la communication SSL sur l'hôte Linux

Vous pouvez activer la communication SSL bidirectionnelle pour sécuriser la communication mutuelle entre le serveur SnapCenter sur l'hôte Linux et les plug-ins à l'aide des commandes PowerShell.

Étape

1. Procédez comme suit pour activer la communication SSL unidirectionnelle.
 - a. Connectez-vous à l'interface graphique de SnapCenter.
 - b. Cliquez sur **Paramètres > Paramètres globaux** et sélectionnez **Activer la validation du certificat sur le serveur SnapCenter**.
 - c. Cliquez sur **hosts > Managed Hosts** et sélectionnez l'hôte plug-in pour lequel vous souhaitez activer le protocole SSL unidirectionnel.
 - d. Cliquez sur  l'icône, puis sur **Activer la validation du certificat**.
2. Activez la communication SSL bidirectionnelle à partir de l'hôte Linux du serveur 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"}`

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.