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

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/ancres/*.
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

Informations sur les marques commerciales