Configure CA certificate with SnapCenter Plug-in Loader (SPL) service on Linux host

SnapCenter Software

Nirupama Sriram, Soumik Das
June 11, 2021

Table of Contents

Configure CA certificate with SnapCenter Plug-in Loader (SPL) service on Linux host

You should manage the password of SPL keystore and its certificate, configure the CA certificate, configure root or intermediate certificates to SPL trust-store, and configure CA signed key pair to SPL trust-store with SnapCenter Plug-in Loader service to activate the installed digital certificate.

SPL uses the file 'keystore.jks', which is located at '/var/opt/snapcenter/spl/etc' both as its trust-store and key-store.

Manage password for SPL keystore and alias of the CA signed key pair in use

Steps

1. You can retrieve SPL keystore default password from SPL property file.

   It is the value corresponding to the key 'SPL_KEYSTORE_PASS'.

2. Change the keystore password:

   ```
   keytool -storepasswd -keystore keystore.jks
   ```

3. Change the password for all aliases of private key entries in the keystore to the same password used for the keystore:

   ```
   keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
   ```

   Update the same for the key SPL_KEYSTORE_PASS in spl.properties file.

4. Restart the service after changing the password.

Password for SPL keystore and for all the associated alias password of the private key should be same.

Configure root or intermediate certificates to SPL trust-store

You should configure the root or intermediate certificates without the private key to SPL trust-store.

Steps

1. Navigate to the folder containing the SPL keystore: */var/opt/snapcenter/spl/etc*.
2. Locate the file 'keystore.jks'.

3. List the added certificates in the keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Add a root or intermediate certificate:

```
keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported>
-file /<CertificatePath> -keystore keystore.jks
```

5. Restart the service after configuring the root or intermediate certificates to SPL trust-store.

> You should add the root CA certificate and then the intermediate CA certificates.

Configure CA signed key pair to SPL trust-store

You should configure the CA signed key pair to the SPL trust-store.

Steps

1. Navigate to the folder containing the SPL's keystore /var/opt/snapcenter/spl/etc.
2. Locate the file 'keystore.jks'.
3. List the added certificates in the keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Add the CA certificate having both private and public key.

```
keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. List the added certificates in the keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verify that the keystore contains the alias corresponding to the new CA certificate, which was added to the keystore.
7. Change the added private key password for CA certificate to the keystore password.

   Default SPL keystore password is the value of the key SPL_KEYSTORE_PASS in spl.properties file.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
```

8. If the alias name in the CA certificate is long and contains space or special characters ("*",","), change the alias name to a simple name:

```
keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
```

9. Configure the alias name from the keystore located in spl.properties file.

   Update this value against the key SPL_CERTIFICATE_ALIAS.

10. Restart the service after configuring the CA signed key pair to SPL trust-store.

Configure certificate revocation list (CRL) for SPL

You should configure the CRL for SPL

About this task

- SPL will look for the CRL files in a pre-configured directory.
- Default directory for the CRL files for SPL is */var/opt/snapcenter/spl/etc/crl*.

Steps

1. You can modify and update the default directory in spl.properties file against the key SPL_CRL_PATH.
2. You can place more than one CRL file in this directory.

   The incoming certificates will be verified against each CRL.