Certificates

Retaining the CA Signed Certificate

Perform this procedure if you need to retain the CA signed SSL Certificate after upgrade.

Note that if you change the keystore password or alias, you need to update it in the **standalone-san.xml** document located at:

`<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\standalone-san.xml`

Update the password in the **keystore** tag and alias:

```
<keystore key-password>="fmserver_1_2_3 key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks">
```

Procedure

Step 1 Backup the signed certificate from the location:

- For Windows: **<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks**
- For Linux: **<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks**

Step 2 Upgrade to Cisco DCNM Release 11.1(1).

Step 3 After upgrade, copy the certificate to the same location on the upgraded version of the Cisco DCNM.

Note You must load the certificates to the same location as mentioned in Step 1, on page 1.

Step 4 Restart the DCNM Services.

Configuring Certificates for Cisco DCNM

This section describes three ways on how to configure the certificates in Cisco DCNM.

Note that if you change the keystore password or alias, you need to update it in the **standalone-san.xml** document located at:

`<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\standalone-san.xml`

Update the password in the **keystore** tag and alias in the **key-alias** tag:

```
<keystore key-password>="fmserver_1_2_3 key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks">
```

This section contains the following topics:

Using a self signed SSL Certificate

Procedure

Step 1 Stop the DCNM services.

Step 2 Rename the keystore located at

`<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks`

to

`<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks.old`

Step 3 From command prompt, navigate to `<DCNM install root>\dcm\java\jre1.8\bin\`.

Step 4 Generate a self signed certificate using following command:

keytool -genkey -trustcacerts -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore <DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks -storepass fmserver_1_2_3 -validity 360 -keysize 2048

Step 5 Start the DCNM services.

Using a SSL Certificate when certificate request is generated using Keytool on Windows

Procedure

Step 1 Stop the DCNM services.

Step 2 Rename the keystore located at:

`<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks`

to

`<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks.old`

Step 3 From command prompt, navigate to the appropriate folder:

`<DCNM install root>\dcm\java\jre1.8\bin\`

Step 4 Generate the public-private key pair in DCNM keystore by using the following command:

keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore "<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3 -validity 360 -keysize 2048

Step 5 Generate the certificate-signing request (CSR) from the public key generated in Step 4, on page 3.

keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3

Note The `dcnm.csr` file is created in the keytool directory, located at `/usr/local/cisco/dcm/java/jre1.8/bin`.

Step 6 Submit the CSR to CA, and download the signed certificate chain in Base-64 format which creates the .p7b file.

CA may provide the certificate and signing certificate as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provided PKCS 7 format go to Step 7, on page 3 to convert it to PEM format. If CA provided PEM format, then go to Step 8, on page 3.

Step 7 Convert the PKCS 7 certificate chain to X509 certificate chain using openssl.

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Note Ensure that the user provides either absolute or relative path to the correct location of `cert-chain.p7b` file in the above command.

Step 8 Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

keytool -importcert -trustcacerts -file cert-chain.pem -keystore "<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3 -alias sme

Note Ensure that the user provides either the absolute path or relative path to the correct location of the `cert-chain.pem` file in the above command.

Step 9 Start the DCNM service.

Using an SSL Certificate When Certificate Request Is Generated Using Keytool on Linux

Procedure

Step 1 Stop the DCNM services, or the DCNM application by using the **appmgr stop dcnm** command.

Step 2 Rename the keystore that is located at:

`<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks`

To

`<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks.old`

Step 3 From command prompt, navigate to the appropriate folder:

`<DCNM install root>/dcm/java/jre1.8/bin/`

Step 4 Generate the public-private key pair in DCNM keystore by using the following command:

./keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore <DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks -storepass fmserver_1_2_3 -validity 360 -keysize 2048

Step 5 Generate the certificate-signing request (CSR) from the public key that is generated in Step 7, on page 4.

./keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks" -storepass fmserver_1_2_3

Note The dcnm.csr file is created in the keytool directory, which is located at `/usr/local/cisco/dcm/java/jre1.8/bin`.

Step 6 Submit the CSR to CA, and download the signed certificate chain in Base-64 format which creates the `.p7b` file.

CA may provide the certificate and signing certificate as a certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provided the certificate chain in PKCS 7 format, go to Step 7, on page 4 to convert it to PEM format. If CA provided the certificate chain in PEM format, then go to Step 8, on page 4.

Step 7 Convert the PKCS 7 certificate chain to the X509 certificate chain using OpenSSL.

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Note Ensure that the user provides either absolute or relative path to the correct location of cert-`chain.p7b` file in the above command.

Step 8 Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

./keytool -importcert -trustcacerts -file cert-chain.pem -keystore <DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks -storepass fmserver_1_2_3 -alias sme

Note Ensure that the user provides either the absolute path or relative path to the correct location of the `cert-chain.pem` file in the above command.

Step 9 Start the applications in the server by using the **appmgr start dcnm** command.

Using a SSL Certificate when certificate request is generated using OpenSSL on Linux

To configure SSL certificates in Cisco DCNM, using certificate request generated using open SSL, perform the following steps.

Procedure

Step 1 Stop the DCNM services, or the DCNM application by using the **appmgr stop dcnm** command.

Step 2 Rename the keystore located at:

`<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks`

to

`<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks.old`

Step 3 From command prompt, navigate to `<DCNM install root>/dcm/java/jre1.8/bin/`.

Step 4 Generate the RSA private key using OpenSSL.

openssl genrsa -out dcnm.key 2048

Step 5 Generate a certificate-signing request (CSR) by using following command:

openssl req -new -key dcnm.key –sha256 -out dcnm.csr

Step 6 Submit the CSR to Certificate signing authority, and download the signed certificate chain in Base-64 format which creates the **.p7b** file.

CA may provide the certificate and signing certificate as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provids the PKCS 7 format, go to Step 7, on page 5 to convert it to PEM format. If CA provides the PEM format, go to Step 8, on page 5.

Step 7 Convert the PKCS 7 certificate chain to X509 certificate chain.

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Step 8 Convert the X509 certificate chain and private key to PKCS 12 format

openssl pkcs12 -export -in cert-chain.pem -inkey dcnm.key -out dcnm.p12 -password pass fmserver_1_2_3 -name sme

Note Ensure that the user provides either absolute path or relative path to the correct location of dcnm.key & `dcnm.p12` files in the above command.

Step 9 Import the intermediate certificate, the root certificate, and the signed certificate in the same order.

./keytool -importkeystore -srckeystore dcnm.p12 -srcstoretype PKCS12 -destkeystore <DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks -deststoretype JKS -alias sme

Note Ensure that the user provides either absolute path or relative path to the correct location of `cert-chain.pem`, `dcnm.key`, and `dcnm.p12` files in the above command.

Step 10 Start the DCNM services, or the DCNM applications in the server by using the **appmgr start dcnm** command.

Collecting PM Data

To setup a shared rrd path to collect PM data, perform these steps:

Procedure

Step 1 Locate the **server.properties** file under **C:\Program Files\Cisco Systems\dcm\fm\conf**.

Step 2 Add the **pm.rrdpath** property file information to the server.properties file. For example, add the server location that needs to be accessible from the DCNM server.

Step 3 Save the server.properties file.

Step 4 Restart the Cisco DCNM-SAN server.

What to do next

Once PM server is ready, the new shared location will be used by the PM server to save .rrd files. PM will create a new directory called db under pm. Ensure you do not open or change these .rrd files as PM server is actively writing into the .rrd files.