Using Certificates with HP Network Automation

HP Network Automation / October 2010

This document provides an overview of how certificates are used within HP Network Automation (NA), including information on Keystores and how to manage and import keys.

Table of Contents

Overview

A Keystore is a store for keys and trusted certificate entries. Within a NA Core installation, there are two Keystores:

- *<install-dir>/jre/lib/security/cacerts*
- *<install dir>/server/ext/jboss/server/default/conf/na.keystore*

The NA Keystore stores all certificates to be used with the Tomcat server. This is the Keystore that you initially control when importing a third-party, CA-signed certificate or creating your own self-signed certificate.

When adding a certificate to NA, be sure to adjust all paths accordingly, depending on your install location and operating system. For example:

```
[root@hostname root]# export PATH=$PATH: <install-dir>/jre/bin/
```

In addition, make sure you are using the correct version of Keytool, otherwise, use *<install-dir>/jre/bin/keytool*.

Note: Some operating systems, such as RH EL 5, include a Keytool. However, if the version does not match the NA version, you will receive an error message.

The following Keytool command lists the contents:

```
keytool -list -keystore <install-dir>/server/ext/jboss/server/
default/conf/na.keystore
```

You will be prompted for the password. In this case, the password is `sentinel`, for example:

```
Enter keystore password: sentinel
Keystore type: JKS
Keystore provider: SUN
```

You will see the following output:

```
Your keystore contains 1 entry sentinel, Aug 14, 2009,
PrivateKeyEntry,sentinel, Jun 10, 2010, keyEntry,
Certificate fingerprint (MD5):
65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8
```

You can obtain more information on the single key entry by using the `-v` (verbose) switch, for example:

```
[root@hostname root]# keytool -list -v -keystore <install-dir>/
server/ext/jboss/server/default/conf/na.keystore

Enter keystore password: sentinel
Keystore type: JKS
Keystore provider: SUN
```

You will see the following output:

```
Your keystore contains 1 entry
Alias name: sentinel
Creation date: Jun 10, 2010
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=localhost, OU=Hewlett Packard Company, O=Hewlett Packard
Company, L=Palo Alto, ST=CA, C=US
Issuer: CN=localhost, OU=Hewlett Packard Company, O=Hewlett
Packard Company, L=Palo Alto, ST=CA, C=US
Serial number: 484e9d84
Valid from: Tue Jun 10 08:28:04 PDT 2010 until: Fri Jun 08
08:28:04 PDT 2020
Certificate fingerprints:
  MD5:  65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8
  SHA1:
05:DE:DC:68:58:45:CA:EA:88:FF:16:05:E7:65:A9:5B:23:29:D7:65
  Signature algorithm name: SHA1withRSA
  Version: 3
*******************************************
*******************************************
```

This is the same certificate that you will see when connecting to a NA Core via the NA Web UI.

Cacerts Keystore

The Cacerts Keystore contains the keys used by the NA Core's JRE to set up SSL communications with external entities.

The Keytool Utility manipulates Keystores. You can list the contents of a Keystore using the `keytool` command. You can also add the location of the NA Core's Java binaries to your environment. As a result, Keytool can be run without entering the path.

To run Keytool to examine the Cacerts Keystore, enter:

```
[root@hostname root]# keytool -list -keystore <install-dir>/jre/
lib/security/cacerts
```

You are prompted for the Keystore password (which is left blank for listing contents and *changeit* for importing). You should see the following output:

```
Enter keystore password:
*****************  WARNING WARNING WARNING  *****************
* The integrity of the information stored in your keystore  *
* has NOT been verified!  In order to verify its integrity, *
* you must provide your keystore password.                  *
*****************  WARNING WARNING WARNING  *****************
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 11 entries

thawtepersonalfreemailca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5):
1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9
thawtepersonalbasicca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5):
E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41
verisignclass3ca, Jun 29, 1998, trustedCertEntry,
Certificate fingerprint (MD5):
78:2A:02:DF:DB:2E:14:D5:A7:5F:0A:DF:B6:8E:9C:5D
thawteserverca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5):
C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D
thawtepersonalpremiumca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5):
```

```
3A:B2:DE:22:9A:20:93:49:F9:ED:C8:D2:8A:E7:68:0D
verisignclass4ca, Jun 29, 1998, trustedCertEntry,
Certificate fingerprint (MD5):
1B:D1:AD:17:8B:7F:22:13:24:F5:26:E2:5D:4E:B9:10
sentinel, Aug 14, 2007, trustedCertEntry,
Certificate fingerprint (MD5):
72:3C:4B:38:9C:5D:89:77:B2:0F:F7:C7:01:C4:81:CD
verisignclass1ca, Jun 29, 1998, trustedCertEntry,
Certificate fingerprint (MD5):
51:86:E8:1F:BC:B1:C3:71:B5:18:10:DB:5F:DC:F6:20
verisignserverca, Jun 29, 1998, trustedCertEntry,
Certificate fingerprint (MD5):
74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
thawtepremiumserverca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5):
06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A
verisignclass2ca, Jun 29, 1998, trustedCertEntry,
Certificate fingerprint (MD5):
EC:40:7D:2B:76:52:67:05:2C:EA:F2:3A:4F:65:F0:D8
```

Note: In addition to recognizable certificates from known CAs, there is an entry for *sentinel*. This self-signed certificate is used so that the NA Core can communicate with itself. If you change the certificate and do not import it into the Cacerts Keystore, you will receive "httpmonitor" errors. Refer to "Adding a Self-signed Certificate to NA" on page 6 for information.

Adding a Self-signed Certificate to NA

To add a self-signed certificate to NA, do the following:

1. Use the Keytool Utility to initiate the certificate creation process, for example:

   ```
   [root@hostname root]# keytool -genkey -keyalg RSA -keysize
   1024 -validity 3650 -alias mycert -keystore <install-dir>/
   server/ext/jboss/server/default/conf/NA.keystore
   ```

   Note: You will need to change the mycert alias to something meaningful to you. This is the name under which the certificate will be stored and displayed in the Keystore. You can also change the algorithm, size, and validity values, or run the Keytool Utility with no arguments, to see the full list of options.

2. Keytool prompts you for the Keystore password. Enter the Keystore password. The Certificate Setup Wizard opens. Enter the appropriate values for the remaining options.
3. When prompted to confirm the values, for example,

   ```
   Is CN=hostname, OU=someOU, O=someORG, L=someCITY,
   ST=someSTATE, C=AB correct? [no]:
   ```

   type yes and press Enter.
4. Type a password for the certificate or press Enter to keep the password the same as the Keystore password.
5. Export the newly created certificate to a file. Type the NA Keystore password when prompted, for example:

   ```
   keytool -export -alias mycert -file mycert.cer -keystore
   <install-dir>/server/ext/jboss/server/default/conf/
   NA.keystore
   Enter keystore password:
   Certificate stored in file <mycert.cer>
   ```

6. Import the certificate into the Cacerts Keystore, for example:

```
[root@hostname root]# keytool -import -file mycert.cer -alias
mycert -keystore <install-dir>/jre/lib/security/cacerts
Enter keystore password:
Owner: CN=hostname, OU=someOU, O=someORG, L=someCITY,
ST=someSTATE, C=AB
Issuer: CN=hostname, OU=someOU, O=someORG, L=someCITY,
ST=someSTATE, C=AB
Serial number: 4833f371
Valid from: Wed May 21 06:03:29 EDT 2008 until: Sat May 19
06:03:29 EDT 2018
Certificate fingerprints:
MD5:  E8:C3:B4:B9:38:C3:52:FC:93:EA:8B:02:53:46:87:A1
SHA1:
6C:B4:B7:0E:AE:D6:EF:B4:EE:2F:F3:2D:B1:1E:1C:3B:F2:D8:ED:33
Signature algorithm name: SHA1withRSA
Version: 3
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

   Note: The password requested here is the import password for the Cacerts Keystore, "changeit".

7. Restart the NA Core services.

Note: Your Web browser could issue a warning message regarding the validity of the certificate. This is because the certificate has been signed by a CA, but is not in the Web browser's trusted list. Follow the instructions in your Web browser to add the certificate to its store.

Adding a CA-signed Certificate

There are several ways to add a CA-signed certificate into an NA Core server. They are dependent on the way in which your CA accepts requests for and provides certificates. You can:

- Create a server cert with the hostname of the NA server, for example:

  ```
  keytool -genkey -dname cn=na1.zso.hp.com -validity 365 -
  keystore tmpks -keypass tmppass -storepass somethingcool
  ```

- Create a Certificate Signing Request (CSR) from the server cert, for example:

  ```
  keytool -certreq -file na1.csr -keystore tmpks -keypass
  tmppass -storepass somethingcool
  ```

- Obtain a signed server cert from your CA. This requires the CA private key. Ask your CA administrator for a signed server cert. Note that there might be an internal site where you can obtain a server cert signed.

Note: If you do have the CA private key, you can sign the CSR using *openssl*. If you are on Linux, you might already have *openssl* installed, or can install it easily (run *yum install openssl*). If you are on Windows, you can use this Windows installer.

The following is an example of the signing command:

```
openssl x509 -req -days 365 -in na1.csr -out server.crt -CA ca.crt
-CAkey ca.key -CAcreateserial
```

This creates a signed server certificate in x509 format. The Tomcat servlet engine used in NA does not support x509 format. As a result, the certificate needs to be converted into JKS, PKCS11, or PKCS12 format. This can be done with *openssl*, for example:

```
openssl pkcs12 -export -in server.crt -inkey ca.key \
   -out server.p12 -name tomcat -CAfile myCA.crt \
   -caname root -chain
```

The server certificate format should be appropriate for an Apache Web server (which is compatible with the Tomcat Servlet container used in NA).

To add a CA-signed Certificate, do the following:

1. Obtain the CA certificate from your CA.
2. Open a Command prompt.
3. Import the CA's public key into the NA keystore, for example:

   ```
   keytool -import -alias ca -file ca.cer -keystore <install-
   dir>/server/ext/jboss/server/default/conf/NA.keystore
   ```

   Note: Replace `ca.cer` with the actual name of your CA's public key certificate. The `NA.keystore` password is *sentinel*.

4. Import the signed server certificate into the NA keystore, for example:

   ```
   keytool -import -alias opsware -file server.p12 -keystore
   <install-dir>/server/ext/jboss/server/default/conf/
   NA.keystore
   ```

   Note: Replace `server.p12` with the actual name of your signed server certificate.The NA.keystore password is *sentinel*.

5. Restart the NA server.

Note: The method used for obtaining and importing CA-signed certificates can vary between CA's. Refer to the following links for more examples:

https://www.thawte.com/ssl-digital-certificates/technical-support/keygen/tomcat_keygen.html.

https://knowledge.verisign.com/support/mpki-for-ssl-support/index?page=content&id=AR278.

For further Reading:

http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html.