Using Keytool to Import SSL Certificates into Sun JDK

Posted At : July 1, 2004 7:10 AM | Posted By : Steven Erat
Related Categories: Java, Learning, ColdFusion, Macromedia

I've recently seen a little discussion on CFTalk about importing SSL certificates into the JVM keystore used by the JVM under ColdFusion MX in order to connect to SSL enabled resources, such as LDAP servers or Web Servers while using either the tags CFLDAP, CFHTTP, or CFINVOKE. I've also found myself having to do this for the first time recently. During that process I stumbled on what turned out to be a bug in the JVM 1.4.2-b28 that ships with ColdFusion MX 6.1 by default.

I saved the SSL certificate to my ColdFusion directory runtime/jre/lib/security, as shown in this image. When using that JVM's keytool utility, described here in the Sun documentation, to import the certificate, I received an error indicating that the certificate which I exported from the SSL website was not valid, and I knew that was incorrect as someone else had just imported the same certificate their machine.

```
C:CFusionMX untimejrelibsecurity>....inkeytool -import -trustcacerts -keystore cacerts -storepass changeit -noprompt -alias mycert -file
mycert.cer
keytool error: java.lang.Exception: Input not an X.509 certificate
```

(view image)

I learned that this was a known issue in some early 1.4.2 Sun JVMs, so I downloaded the most recent JVM from Sun, v. 1.4.2_05. I then configured ColdFusion MX to run on this new JVM, and tried again. This time the keytool imported the certificate without complaint, and the command keytool -storepass changeit -list -keystore cacerts confirmed the alias for my certificate. CFHTTP calls to the particular SSL enabled website now worked successfully.

Note that the cacerts keystore that comes with ColdFusion already contains about 128 certificates types from well known certificate authorities, so if you wanted to consume the page https://login.yahoo.com with CFHTTP it would work out of the box without having to import any extra certificate. You should only need to import a site's SSL certificate if the site does not use one of the certs already in the cacerts file in CFMX.

The Sun 1.4.2_05 JDK comes with a cacerts keystore that has about 25 cert types built in, so you'd probably want to swap that cacerts file with the one found under ColdFusion's root directory. If you choose to not run ColdFusion MX on the newer JVM, you could copy CFMX's cacerts file to the newer JVM's jre/lib/security directory to overwrite the existing one, then complete the steps to import the SSL certificate into the that cacerts keystore file, and then copy that cacerts file back under ColdFusion's runtime/jre/lib/security directory. Restart ColdFusion and the imported certificate will be ready for use.

A good litmus test is that if your CFHTTP call to an SSL site fails with the following error (cfdump of cfhttp variable), then you should import that certificate into the keystore file cacerts:

```
ErrorDetail I/O Exception: peer not authenticated
Filecontent Connection Failure
Mimetype Unable to determine MIME type of file.
Statuscode Connection Failure. Status code unavailable.<
```

For convenience, I wrote a set of batch files to be used on Windows when working with the keytool utility. They save a fair bit of typing. One batch file for example requires that you set 4 parameters for the JAVA_HOME, cert name & cert alias, and the keytool password. You can download the collection of bat files to customize yourself here.

An example of the import batch file is shown here:

```
@echo off
echo
echo This will import an X.509 SSL certificate into the keystore for the JVM
specified
echo
echo Press Control+C to abort.
pause
SETLOCAL

rem -----------------------------------------------------
rem 1) SET COLDFUSION JVM'S JAVA_HOME HERE
rem THIS SHOULD BE THE JVM USED FOR COLDFUSION MX
rem -----------------------------------------------------
set JAVA_HOME=C:j2sdk1.4.2_05

rem -----------------------------------------------------
rem 2) SET THE CERTIFICATE NAME AND ALIAS HERE
rem -----------------------------------------------------
set CERT_NAME=mycert.cer
set CERT_ALIAS=mycert

rem -----------------------------------------------------
rem 3) SET THE KEYTOOL PASSWORD HERE
rem -------------------------------------------------
set KEYTOOL_PASS=changeit

rem -------------------------------------------------
rem DO NOT EDIT BELOW THIS LINE
rem -------------------------------------------------
set JAVA_SECURITY=%JAVA_HOME%jrelibsecurity
set CERT=%JAVA_SECURITY%\%CERT_NAME%
%JAVA_HOME%jreinkeytool -import -trustcacerts -keystore %JAVA_SECURITY%cacerts
-storepass %KEYTOOL_PASS% -noprompt -alias %CERT_ALIAS% -file %CERT%
ENDLOCAL
pause
```

Exporting the SSL certificate (on Windows)

1. Browse to the SSL website
2. Double click the Lock icon in the status bar
3. Click the Details Tab
4. Click the button Copy to File...
5. Click Next in the Export Wizard
6. Choose the first option (default) for DER encoded
7. Click Next
8. Browse to C:
9. Type any filename for certificate such as mycert.cer
10. Click Next, Click Finish

Using the keytool to import a certificate
There is a Sun SDK bug in early version of 1.4.2 JVM where the keytool doesn't work. You must download a recent JDK such as **JDK 1.4.2_05** from java.sun.com.

1. Install the SDK, for example to C:j2sdk1.4.2_05
2. Move the mycert.cer file from C: to C:j2sdk1.4.2_05jrelibsecurity
3. Rename C:j2sdk1.4.2_05jrelibsecuritycacerts to C:j2sdk1.4.2_05jrelibsecuritycacerts_orig
4. Copy C:CFusionMX untimejrelibsecuritycacerts to C:j2sdk1.4.2_05jrelibsecuritycacerts
5. Unzip the zipped bat files anywhere on the system
6. Edit each of the *.bat files that were unpacked
7. Change bat file JAVA_HOME as needed
8. Change certificate name and certificate alias
9. Save bat files
10. Double click the import bat file to import the certificate into the keystore
11. Double click the list bat file and read the output file to confirm that the certificate was imported
12. Copy C:j2sdk1.4.2_05jrelibsecuritycacerts to C:CFusionMX untimejrelibsecuritycacerts
13. Restart ColdFusion Server

Other resources for using the keytool include:

- **Macromedia Technote**
- **Brandon Purcell's Blog**
- **Stacey Young's CFTalk Thread**
- **Sun Documenation**

Updated May 2, 2007: Adding examples for use with *nix:

List All (listkeys.sh)

```
#!/bin/sh
JAVA_HOME=/opt/AppServer/java
JAVA_SECURITY=$JAVA_HOME/jre/lib/security
$JAVA_HOME/jre/bin/keytool -storepass changeit -list -keystore $JAVA_SECURITY/cacerts > keytool_list_result.txt
cat keytool_list_result.txt
```

Import my certificate bogart9.cer then list to confirm (importkeys.sh)

```
#!/bin/sh
MYCERT_NAME=bogart9.cer #should be in jre/lib/security
MYCERT_ALIAS=bogart9
JAVA_HOME=/opt/AppServer/java
JAVA_SECURITY=$JAVA_HOME/jre/lib/security
CERT=$JAVA_SECURITY/$MYCERT_NAME
$JAVA_HOME/jre/bin/keytool -import -trustcacerts  -keystore  $JAVA_SECURITY/cacerts -storepass changeit -noprompt -alias $MYCERT_ALIAS -file $CERT
echo Keytool has imported $MYCERT_ALIAS into $JAVA_SECURITY/cacerts
```

```
./listkeys.sh | grep $MYCERT_ALIAS
```