

mod17_ex02: Creating Global Truststore

The purpose of this exercise is to create a `global.jks` and a `global.pem` file. The `cacerts` file is a Java keystore list of all approved Certificate Authorities. RHEL's default location is `$JAVA_HOME/jre/lib/security/cacerts`. Cloudera Manager requires the list of approved Certificate Authorities as both a Java keystore and a PEM file. The location for both of these files will be `/var/lib/cloudera-scm-agent/agent-cert`. This exercise is a simulation of the steps Cloudera Manager goes through to create both of these files.

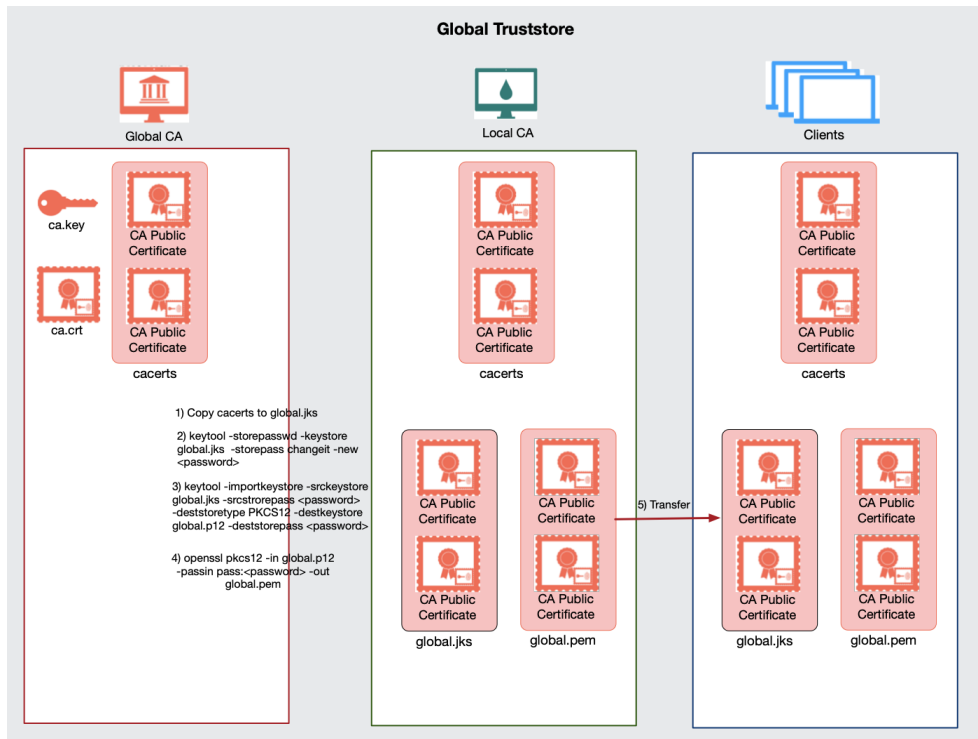
Reference Information

The following documents provide information related to this exercise.

[Use Cloudera Manager to generate internal CA and corresponding certificates](#)

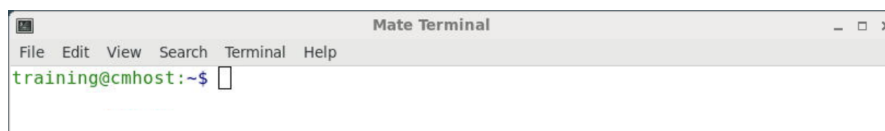
[Converting file encodings for TLS/SSL certificates and keys](#)

1. Creating Global Keystores.



1. Copy the Java keystore cacerts to global.jks.
2. Change the password on global.jks.
3. Use the keytool command to convert the global.jks into global.p12.
4. Use the openssl command to convert the file to PEM format.
5. Transfer both of these files to all hosts.

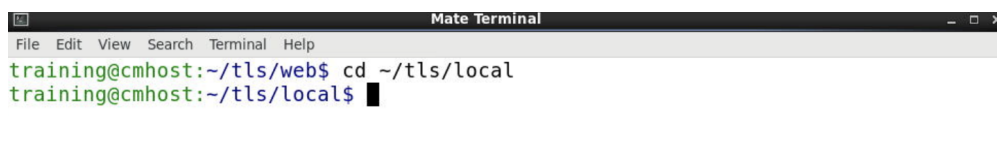
2. Open a Mate terminal as the user training.



3. Create the global keystore.

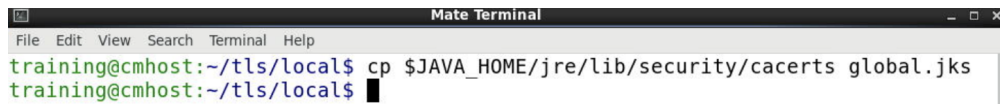
The file cacerts is an approved list of Certificate Authorities. You will find many of the primary CA's in this file. The file is a Java keystore even though it does not end with .jks.

3.1 Change directory to local.



```
$ cd ~/tls/local
```

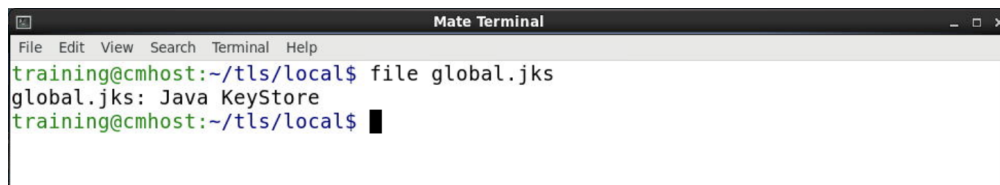
3.2 Copy the cacerts file.



```
Mate Terminal
File Edit View Search Terminal Help
training@cmhost:~/tls/local$ cp $JAVA_HOME/jre/lib/security/cacerts global.jks
training@cmhost:~/tls/local$
```

```
$ cp $JAVA_HOME/jre/lib/security/cacerts global.jks
```

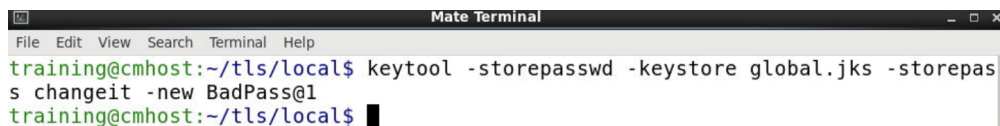
3.3 Verify global.jks is a Java KeyStore.



```
Mate Terminal
File Edit View Search Terminal Help
training@cmhost:~/tls/local$ file global.jks
global.jks: Java KeyStore
training@cmhost:~/tls/local$
```

```
$ file global.jks
global.jks: Java KeyStore
```

3.4 Change the password from the default of changeit to <password>.



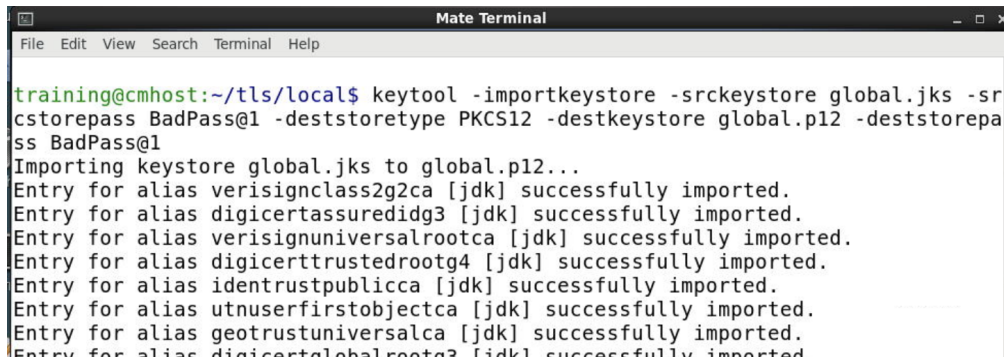
```
Mate Terminal
File Edit View Search Terminal Help
training@cmhost:~/tls/local$ keytool -storepasswd -keystore global.jks -storepass changeit -new BadPass@1
training@cmhost:~/tls/local$
```

```
$ keytool -storepasswd -keystore global.jks
-storepass changeit -new <password>
```

4. Convert the Java keystore to PKCS12 format.

One of uses of the openssl command is to convert certificates from one format to another.

4.1 Use the keytool command to export the keystore to the pkcs12 format.



```

training@cmhost:~/tls/local$ keytool -importkeystore -srckeystore global.jks -srcstorepass BadPass@1 -deststoretype PKCS12 -destkeystore global.p12 -deststorepass BadPass@1
Importing keystore global.jks to global.p12...
Entry for alias verisignclass2g2ca [jdk] successfully imported.
Entry for alias digicertassuredidg3 [jdk] successfully imported.
Entry for alias verisignuniversalrootca [jdk] successfully imported.
Entry for alias digicerttrustedrootg4 [jdk] successfully imported.
Entry for alias identrustpublicca [jdk] successfully imported.
Entry for alias utnuserfirstobjectca [jdk] successfully imported.
Entry for alias geotrustuniversalca [jdk] successfully imported.
Entry for alias digicertglobalrootg2 [jdk] successfully imported.

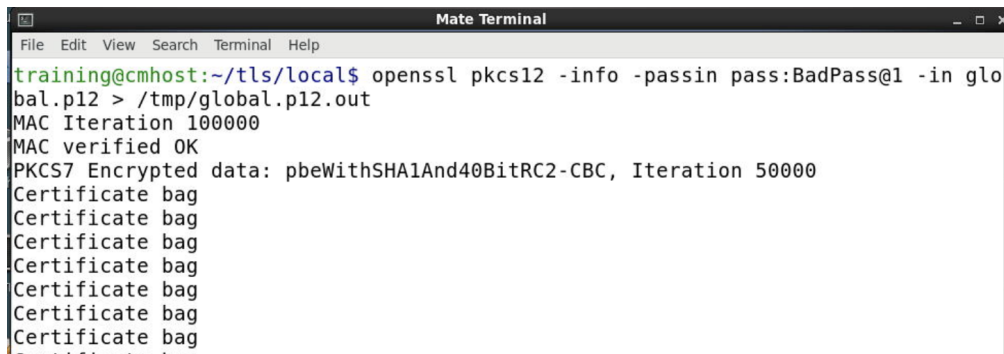
```

```

$ keytool -importkeystore \
    -srckeystore global.jks \
    -srcstorepass <password> \
    -deststoretype PKCS12 \
    -destkeystore global.p12 \
    -deststorepass <password>

```

4.2 Use the openssl command to export the contents of the pkcs12 file to /tmp. Do not miss the use of the redirect > special character. This is not a required step but it is a recommend practice for reviewing the file.



```

training@cmhost:~/tls/local$ openssl pkcs12 -info -passin pass:BadPass@1 -in global.p12 > /tmp/global.p12.out
MAC Iteration 100000
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 50000
Certificate bag
Certificate bag
Certificate bag
Certificate bag
Certificate bag
Certificate bag
Certificate bag
Certificate bag

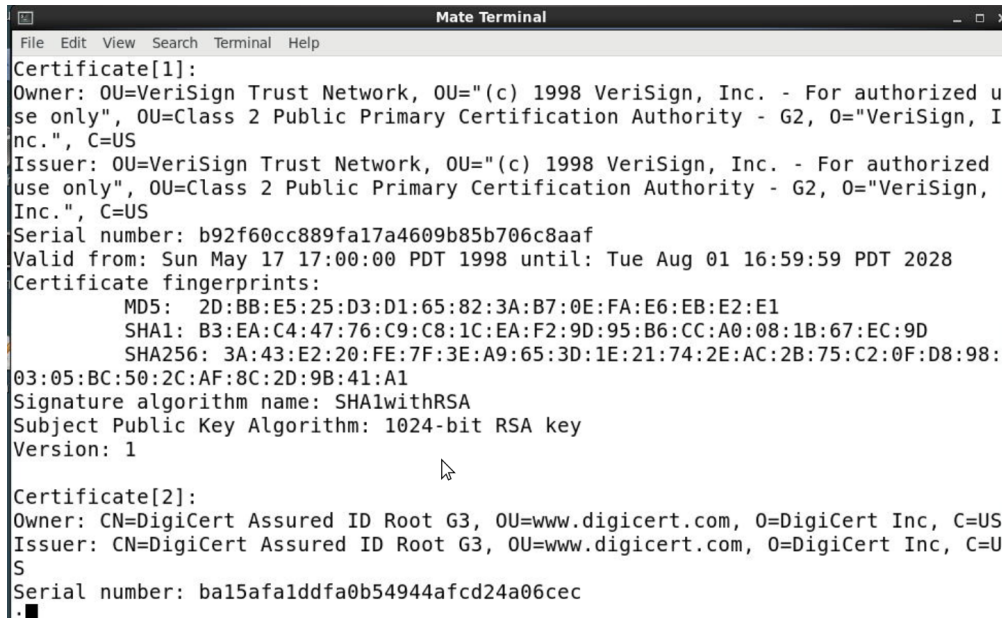
```

```

$ openssl pkcs12 -info \
    -passin pass:<password> \
    -in global.p12 > \
    /tmp/global.p12.out

```


5.2 Use the keytool command to verify the certificates in global.pem. Pipe the output to less and page through. Type q to quit.



```

Certificate[1]:
Owner: OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US
Issuer: OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US
Serial number: b92f60cc889fa17a4609b85b706c8aaf
Valid from: Sun May 17 17:00:00 PDT 1998 until: Tue Aug 01 16:59:59 PDT 2028
Certificate fingerprints:
    MD5:  2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
    SHA1: B3:EA:C4:47:76:C9:C8:1C:EA:F2:9D:95:B6:CC:A0:08:1B:67:EC:9D
    SHA256: 3A:43:E2:20:FE:7F:3E:A9:65:3D:1E:21:74:2E:AC:2B:75:C2:0F:D8:98:03:05:BC:50:2C:AF:8C:2D:9B:41:A1
Signature algorithm name: SHA1withRSA
Subject Public Key Algorithm: 1024-bit RSA key
Version: 1

Certificate[2]:
Owner: CN=DigiCert Assured ID Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer: CN=DigiCert Assured ID Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US
Serial number: ba15afa1ddfa0b54944afcd24a06cec

```

```
# keytool -printcert -v -file global.pem | less
```

6. Transfer global truststores to hosts.

6.1 Copy both files to the client directory.



```

training@cmhost:~/tls/local$ ls
global.jks  global.p12  global.pem
training@cmhost:~/tls/local$ cp global.jks global.pem ~/tls/client/
training@cmhost:~/tls/local$

```

```
$ cp global.jks global.pem ~/tls/client/
```