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.

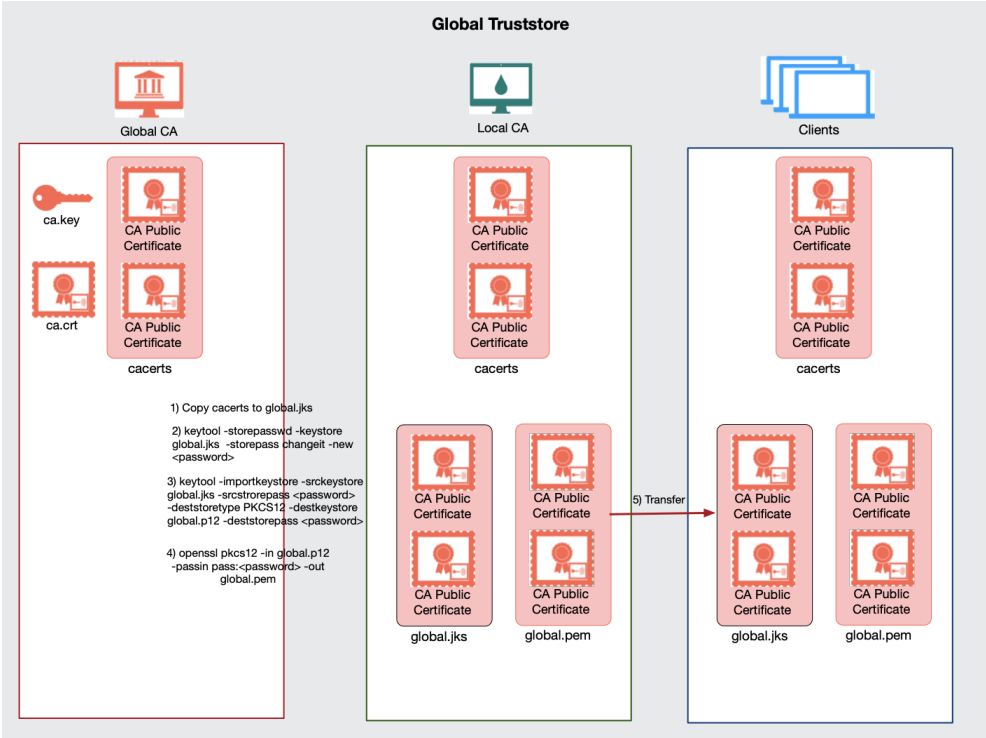
Reference Information

The following documents provide information related to this exercise.

Use Cloudera Manager to generate internal CA and corresponding certificates

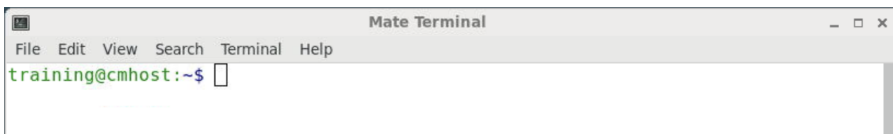
Converting file encodings for TLS/SSL certificates and keys

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
```

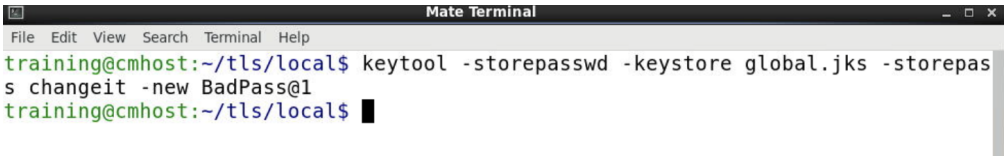
3.2 Copy the cacerts file.


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

3.3 Verify global.jks is a Java KeyStore.


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

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

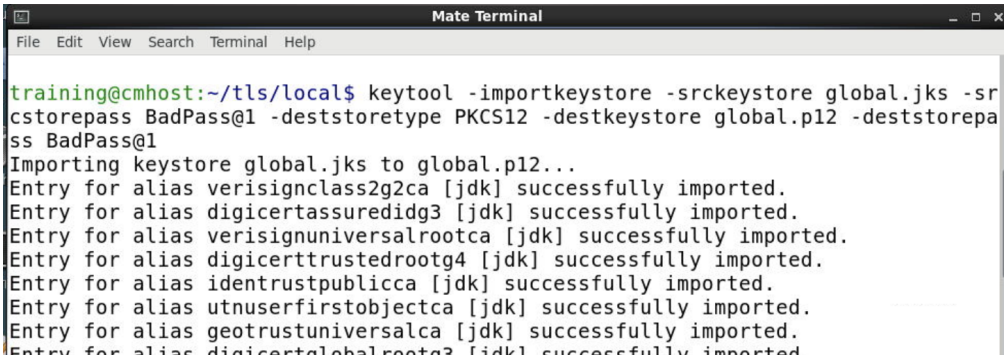



```
$ keytool –storepasswd –keystore global.jks
             –storepass changeit –new <password>
```

4. Convert the Java keystore to PKCS12 format.

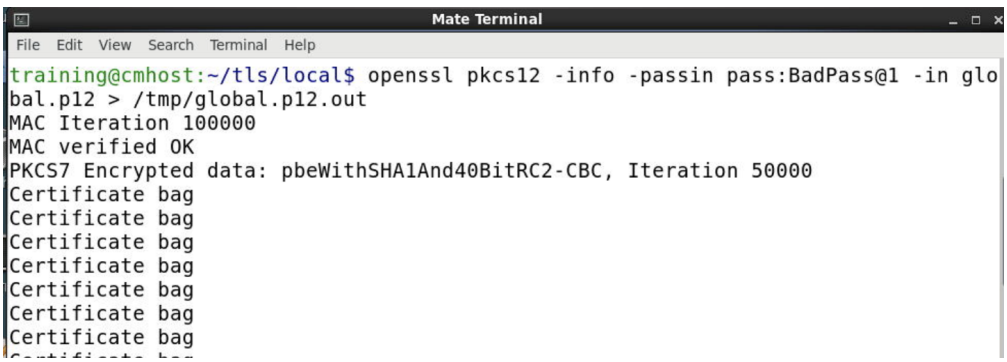
One of uses of the openssl command is to convert certificates from one format to another.

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



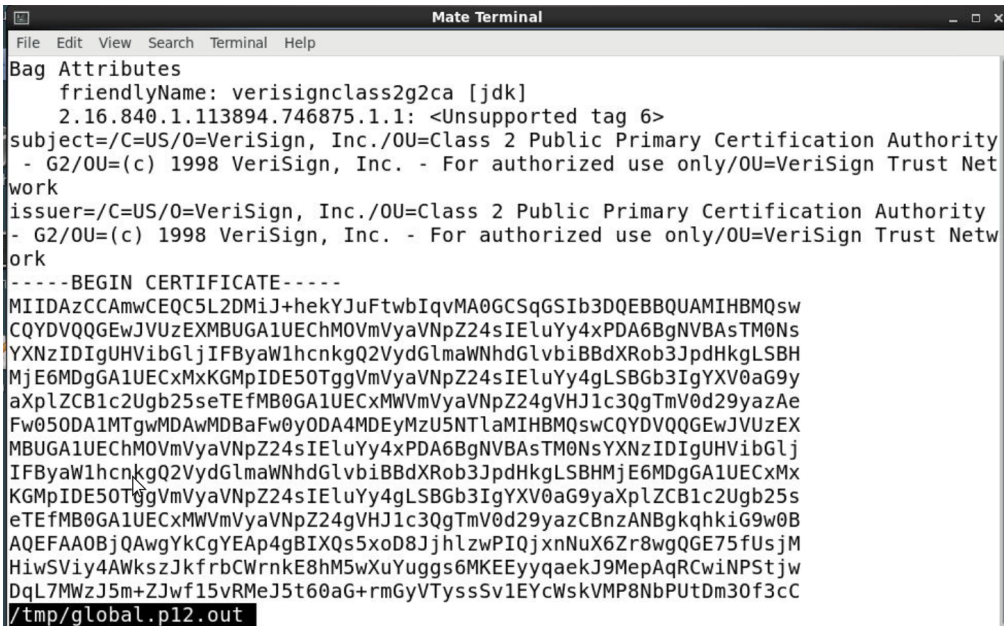

```
$ keytool -importkeystore \
            -srckeystore global.jks \
            -srcstorepass <password> \
            -deststoretype PKCS12 \
            -destkeystore global.p12 \
             -deststorepass <password>
```

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.




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

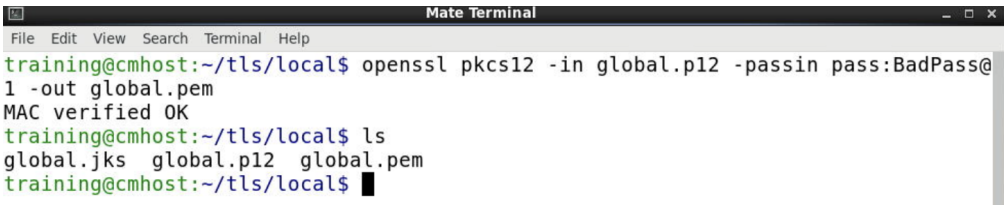
4.3 Use the less command to verify the contents of the /tmp/global.p12.out file. Use the spacebar to scroll through to view certificates. Type q to quit.




```
$ less /tmp/global.p12.out
```

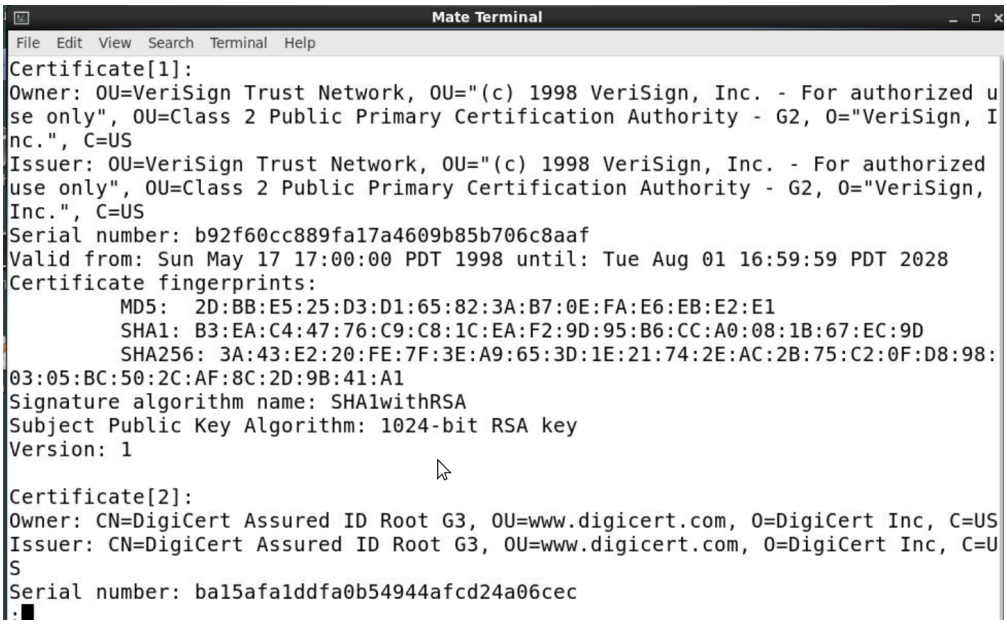
5. Convert PKCS12 file to PEM format.

5.1 Use the openssl command to convert the pkcs12 format to the pem format.




```
$ openssl pkcs12 -in global.p12 \
            -passin pass:<password> \
            -out global.pem
```

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.




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

6. Transfer global truststores to hosts.

6.1 Copy both files to the client directory.


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