Using a Self-Signed Certificate

Overview

For several security features that you want to use over a secure connection (such as LDAPS, Secure Active Directory, or Secure OAuth), you may configure Artifactory to allow a non-trusted self-signed certificate.

Page Contents

Configuring a Self-Signed Certificate

For outbound Artifactory connections (remote repositories, external authentication servers...) intended for SSL self-signed/internal CA signed certificates URL endpoints, you may use use one of the following ways to establish trusts based on **your** certificates:

- **Use the instructions described on Oracle's documentation to import a single/chain of certificates to your JVM's keystore.**
- **Point Artifactory to use a custom certificate store.** Follow the steps below (thanks to Marc Schoechlin for providing this information):

1. Download/acquire the certificate(s) of the SSL secured server openssl s_client -connect **`<secure authentication server IP and port>`** -showcerts < /dev/null > `server.ca.`

   Examples

   RED HAT CDN

   openssl s_client -connect cdn.redhat.com:443 -showcerts < /dev/null > server.ca

   LDAP or Active Directory:
   openssl s_client -connect **the.ldap.server.net:636** -showcerts < /dev/null > server.ca

   OAuth (Use the Authorization URL). For example, with GitHub:
   openssl s_client -connect github.com:443/login/oauth/authorize -showcerts < /dev/null > server.ca

2. Identify the standard `cacerts` file of your Java installation
3. Create a custom `cacerts` file by copying the `cacerts` file to the Artifactory configuration dir. This may vary depending on the installation and its usually under JAVA_HOME/jre/lib/security.
   ```
   Example : cp /usr/lib/jvm/java-1.8.0-openjdk-amd64/jre/lib/security/cacerts /etc/opt/jfrog
   /artifactory/
   ```
4. Import the CA certificate into the **customized** cacerts file. **Note you can store the cacerts in any location as long as you can access it and link it to the JVM on startup.**
   ```
   keytool -import -alias myca -keystore /etc/opt/jfrog/artifactory/cacerts -trustcacerts -file
   server.ca
   => Password: changeit
   => Agree to add the certificate
   ```
5. Change permissions for the `artifactory` user
   ```
   chmod 755 /etc/opt/jfrog/artifactory/cacerts
   chown artifactory:users /etc/opt/jfrog/artifactory/cacerts
   ```
6. Modify the defaults of the Artifactory JVM to use the custom `cacerts` file **OR** you could change the startup script to include the cacerts in the JAVA_OPTIONS.
   ```
   echo "export JAVA_OPTIONS=\"\$JAVA_OPTIONS -Djavax.net.ssl.trustStore=/etc/opt/jfrog/artifactory
   /cacerts\"" >> /etc/opt/jfrog/artifactory/default
   ```
7. Restart Artifactory