DC

**Secure management interface with HTTPS/TLS in JBoss EAP 7.1+ with Elytron**

https://access.redhat.com/solutions/3669891

Obtain or generate the keystore :

keytool -genkeypair -alias localhost -keyalg RSA -keysize 1024 -validity 365 -keystore keystore.jks -dname "CN=localhost" -keypass secret -storepass secret

"

openssl genrsa -des3 -out server.key 2048

openssl req -new -key server.key -out server.csr

openssl x509 -req -sha256 -days 365 -in server.csr -signkey server.key -out server.crt

openssl pkcs12 -export -out serverpkcs12.cer -inkey server.key -in server.crt -name server

/ql/java/jdk1.8.0\_152/bin/keytool -importkeystore -deststorepass secret -destkeypass secret -destkeystore server.keystore -srckeystore serverpkcs12.cer -srcstoretype PKCS12 -srcstorepass secret -alias server

/ql/java/jdk1.8.0\_152/bin/keytool -exportcert -keystore server.keystore -alias server -keypass secret -storepass secret -file server\_selfsigned.cer

/ql/java/jdk1.8.0\_152/bin/keytool -import -keystore ServerTRKS.jks -storepass secret -alias server -trustcacerts -file server\_selfsigned.cer"'

2 Copy the keystore.jks file to $EAP\_HOME/domain/configuration when using domain mode or $EAP\_HOME/standalone/configuration when using standalone mode.

1. Create a key-store, key-manager, and server-ssl-context :

[Raw](https://access.redhat.com/solutions/3669891)

/host=master/subsystem=elytron/key-store=httpsKS:add(path=keystore.jks,relative-to=jboss.domain.config.dir,credential-reference={clear-text=secret},type=JKS)

/host=master/subsystem=elytron/key-manager=httpsKM:add(key-store=httpsKS,algorithm="SunX509",credential-reference={clear-text=secret})

/host=master/subsystem=elytron/server-ssl-context=httpsSSC:add(key-manager=httpsKM,protocols=["TLSv1.2"])

Configure the management console to use ssl-context :

/host=master/core-service=management/management-interface=http-interface:write-attribute(name=ssl-context, value=httpsSSC)

Configure the management interface to use a secure interface and port :

/host=master/core-service=management/management-interface=http-interface:write-attribute(name=secure-interface, value=management)

/host=master/core-service=management/management-interface=http-interface:write-attribute(name=secure-port, value=9443)

5. reload --host=masterdc

Domain Controller's - Host.xml

165 <provider-sasl-server-factory name="global"/>

166 </sasl>

167 <tls>

168 <key-stores>

169 <key-store name="httpsKS">

170 <credential-reference clear-text="secret"/>

171 <implementation type="JKS"/>

172 <file path="keystore.jks" relative-to="jboss.domain.config.dir"/>

173 </key-store>

174 </key-stores>

175 <key-managers>

176 <key-manager name="httpsKM" algorithm="SunX509" key-store="httpsKS">

177 <credential-reference clear-text="secret"/>

178 </key-manager>

179 </key-managers>

180 <server-ssl-contexts>

181 <server-ssl-context name="httpsSSC" protocols="TLSv1.2" key-manager="httpsKM"/>

182 </server-ssl-contexts>

183 </tls>

184 </subsystem>

185 <subsystem xmlns="urn:jboss:domain:jmx:1.3">

"

<tls>

<key-stores>

<key-store name="httpsKS">

<credential-reference clear-text="secret"/>

<implementation type="JKS"/>

<file path="keystore.jks" relative-to="jboss.domain.config.dir"/>

</key-store>

</key-stores>

<key-managers>

<key-manager name="httpsKM" algorithm="SunX509" key-store="httpsKS">

<credential-reference clear-text="secret"/>

</key-manager>

</key-managers>

<server-ssl-contexts>

<server-ssl-context name="httpsSSC" protocols="TLSv1.2" key-manager="httpsKM"/>

</server-ssl-contexts>

</tls>

"

After that on Node.

configuration/host.xml

add these lines

</mechanism-provider-filtering-sasl-server-factory>

<provider-sasl-server-factory name="global"/>

Find </sasl>

" </sasl>

<tls>

<key-stores>

<key-store name="ServerKS-1">

<credential-reference type="text" clear-text="secret"/>

<implementation type="JKS"/>

<file path="/ql/jboss-eap-7.2/domain/configuration/SSL/server.keystore"/>

</key-store>

<key-store name="ClientKS-2">

<credential-reference type="text" clear-text="secret"/>

<implementation type="JKS"/>

<file path="/ql/jboss-eap-7.2/domain/configuration/SSL/client.keystore"/>

</key-store>

</key-stores>

<key-managers>

<key-manager name="severKSMGR-1" key-store="ServerKS-1">

<credential-reference type="text" clear-text="secret"/>

</key-manager>

<key-manager name="ClientKSMGR-2" key-store="ClientKS-2">

<credential-reference type="text" clear-text="secret"/>

</key-manager>

<key-manager name="severKSMGR-2" algorithm="SunX509" key-store="ServerKS-1">

<credential-reference clear-text="secret"/>

</key-manager>

</key-managers>

<trust-managers>

<trust-manager name="ServerTSMGR-1" key-store="ServerKS-1"/>

<trust-manager name="ClientTSMGR-2" key-store="ClientKS-2"/>

</trust-managers>

<server-ssl-contexts>

<server-ssl-context name="ServerSSLContext-1" key-manager="severKSMGR-1"/>

<server-ssl-context name="ServerSSLContext-2" key-manager="severKSMGR-2"/>

</server-ssl-contexts>

<client-ssl-contexts>

<client-ssl-context name="ClientSSLContext-2" protocols="TLSv1.2" key-manager="ClientKSMGR-2" trust-manager="ClientTSMGR-2"/>

</client-ssl-contexts>

</tls>

"

180 <filter provider-name="WildFlyElytron"/>

181 </filters>

182 </mechanism-provider-filtering-sasl-server-factory>

183 <provider-sasl-server-factory name="global"/>

184 </sasl>

185 <tls>

186 <key-stores>

187 <key-store name="ServerKS-1">

188 <credential-reference type="text" clear-text="secret"/>

189 <implementation type="JKS"/>

190 <file path="/ql/jboss-eap-7.2/domain/configuration/SSL/server.keystore"/>

191 </key-store>

192 <key-store name="ClientKS-2">

193 <credential-reference type="text" clear-text="secret"/>

194 <implementation type="JKS"/>

195 <file path="/ql/jboss-eap-7.2/domain/configuration/SSL/client.keystore"/>

196 </key-store>

197 </key-stores>

198 <key-managers>

199 <key-manager name="severKSMGR-1" key-store="ServerKS-1">

200 <credential-reference type="text" clear-text="secret"/>

201 </key-manager>

202 <key-manager name="ClientKSMGR-2" key-store="ClientKS-2">

203 <credential-reference type="text" clear-text="secret"/>

204 </key-manager>

205 <key-manager name="severKSMGR-2" algorithm="SunX509" key-store="ServerKS-1">

206 <credential-reference clear-text="secret"/>

207 </key-manager>

208 </key-managers>

209 <trust-managers>

210 <trust-manager name="ServerTSMGR-1" key-store="ServerKS-1"/>

211 <trust-manager name="ClientTSMGR-2" key-store="ClientKS-2"/>

212 </trust-managers>

213 <server-ssl-contexts>

214 <server-ssl-context name="ServerSSLContext-1" key-manager="severKSMGR-1"/>

215 <server-ssl-context name="ServerSSLContext-2" key-manager="severKSMGR-2"/>

216 </server-ssl-contexts>

217 <client-ssl-contexts>

218 <client-ssl-context name="ClientSSLContext-2" protocols="TLSv1.2" key-manager="ClientKSMGR-2" trust-manager="ClientTSMGR-2"/>

219 </client-ssl-contexts>

220 </tls>

221

222

reload the server