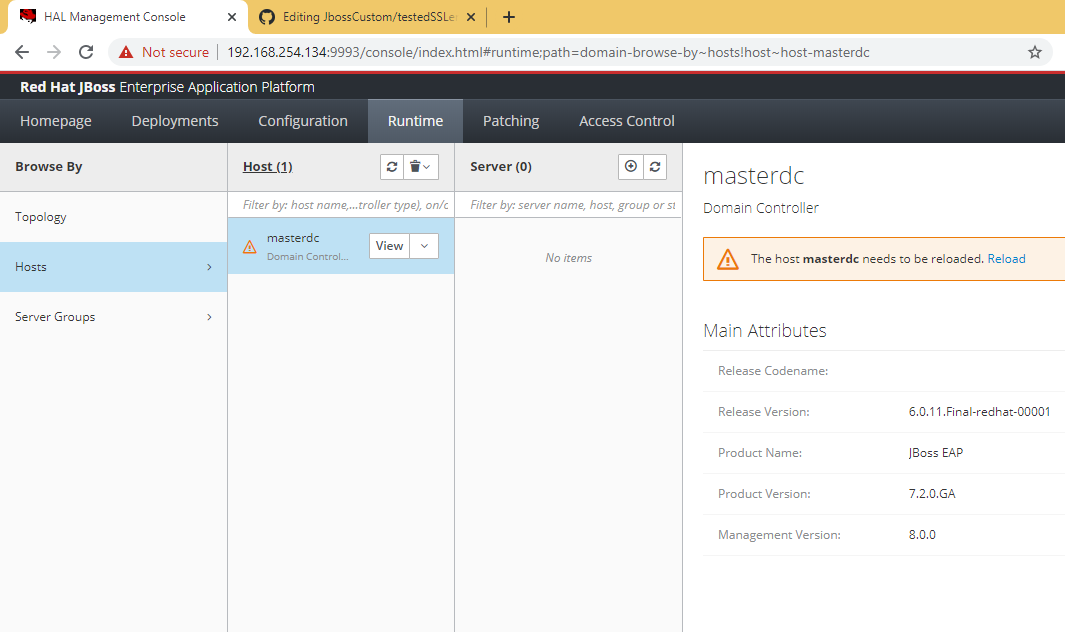
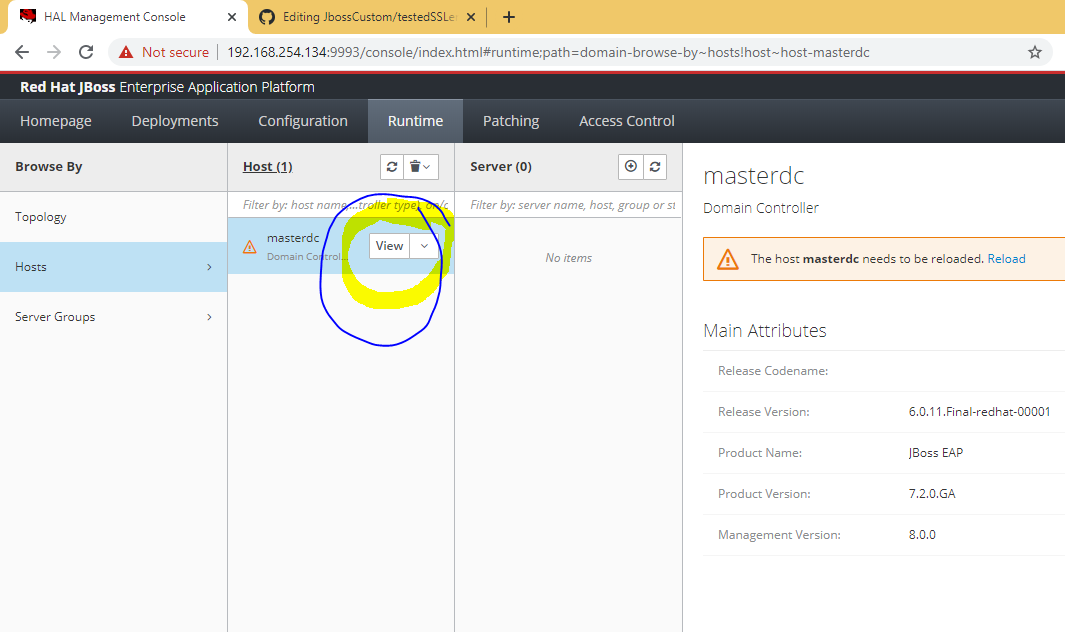
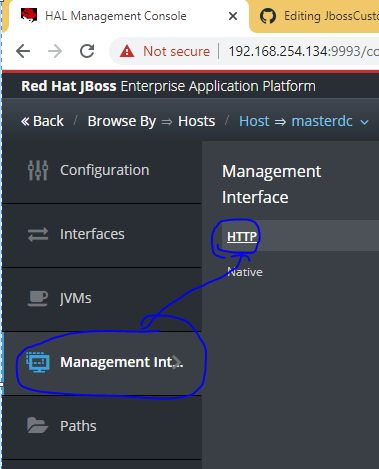
Enable SSL /TLS from Domain Controller GUI.

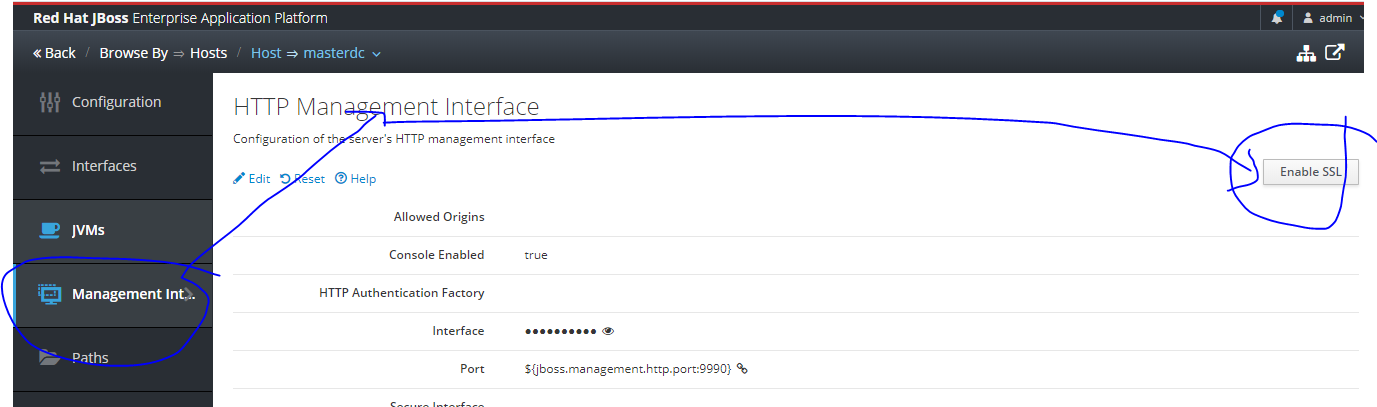
/ql/java/current-java/bin/keytool -genkeypair -alias serverdc -keyalg RSA -keysize 1024 -validity 365 -keystore serverdc.keystore.jks -dname "CN=serverdc" -keypass secret -storepass secret

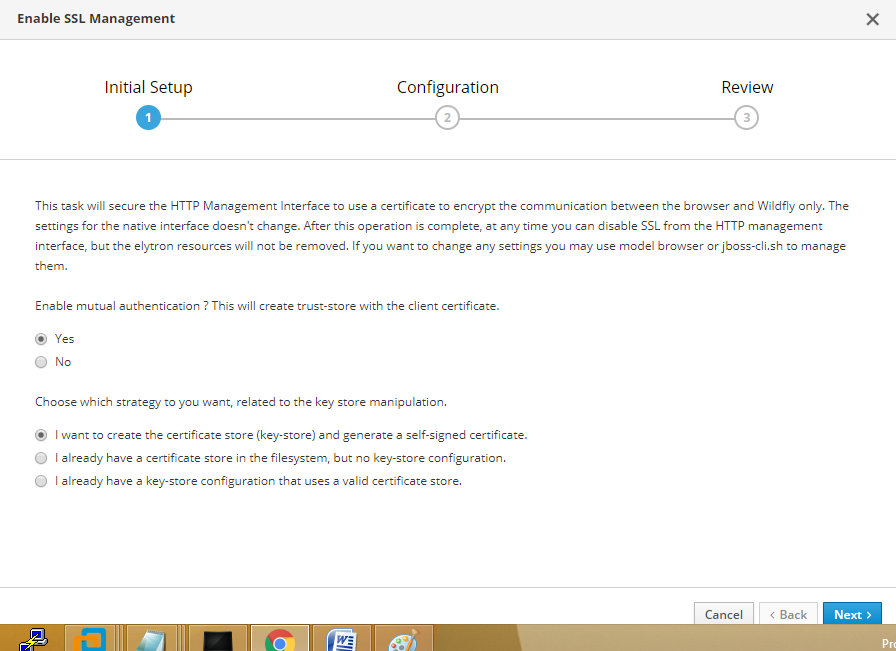
/ql/java/current-java/bin/keytool -exportcert -keystore serverdc.keystore.jks -alias serverdc -keypass secret -storepass secret -file /path/to/serverdc.cer

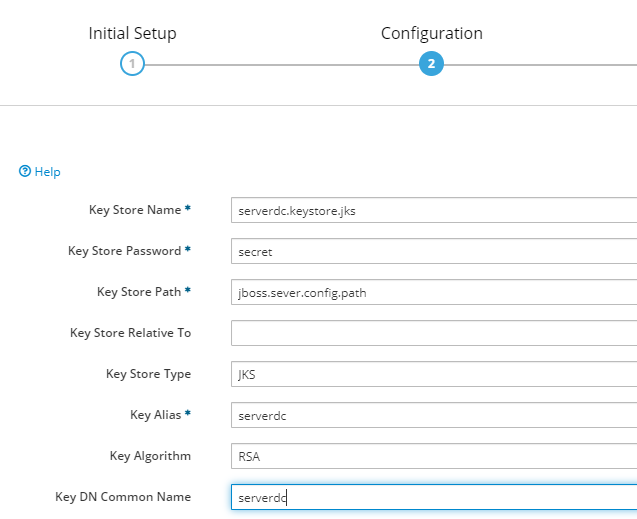




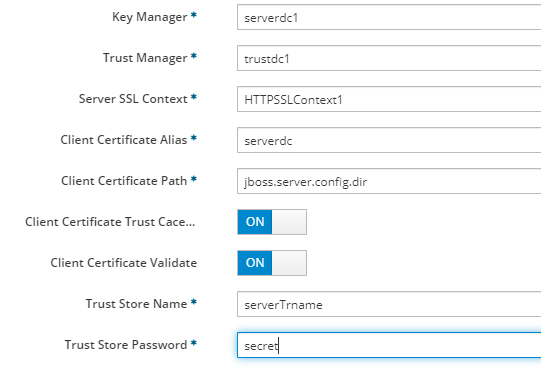


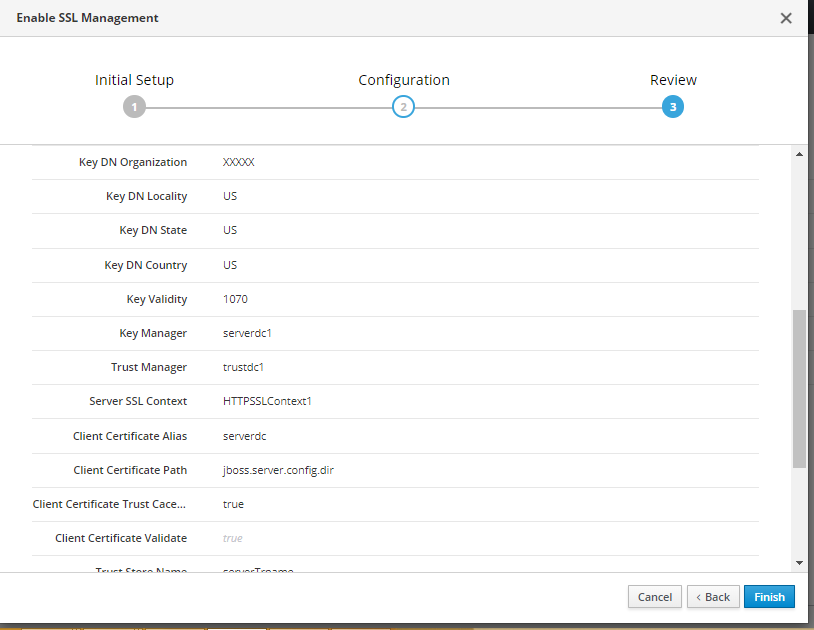
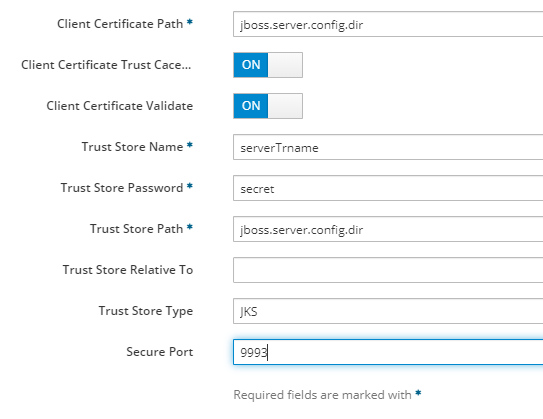






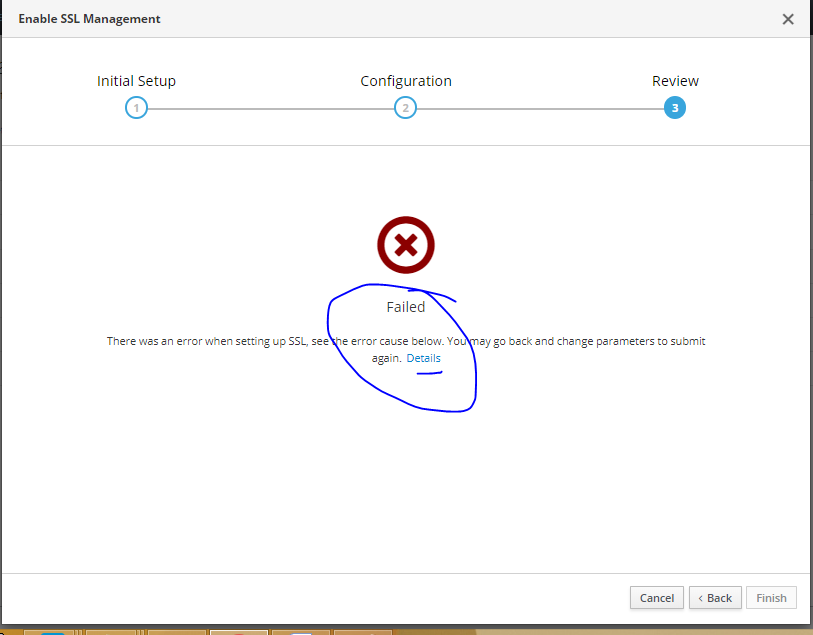




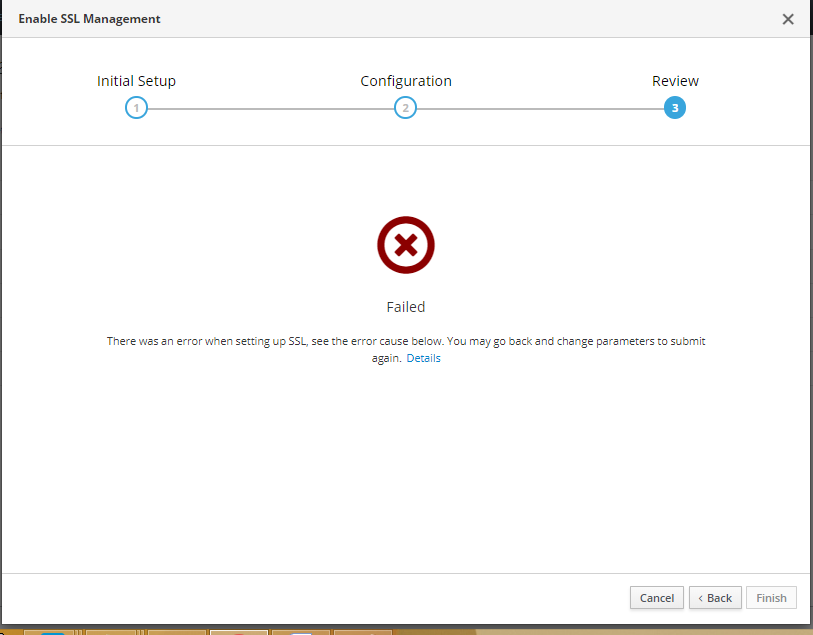


you need to back 2 times

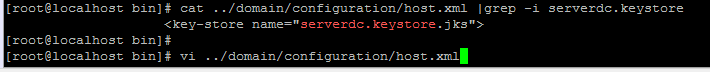
First time it will show you



Once you back again then you will get this Back button.



Now need to go to DC (Domain controller from putty) and search for Keystore name that you filed in above wizard.



[root@localhost bin]# cat ../domain/configuration/host.xml |grep -i serverdc.keystore

<key-store name="serverdc.keystore.jks">

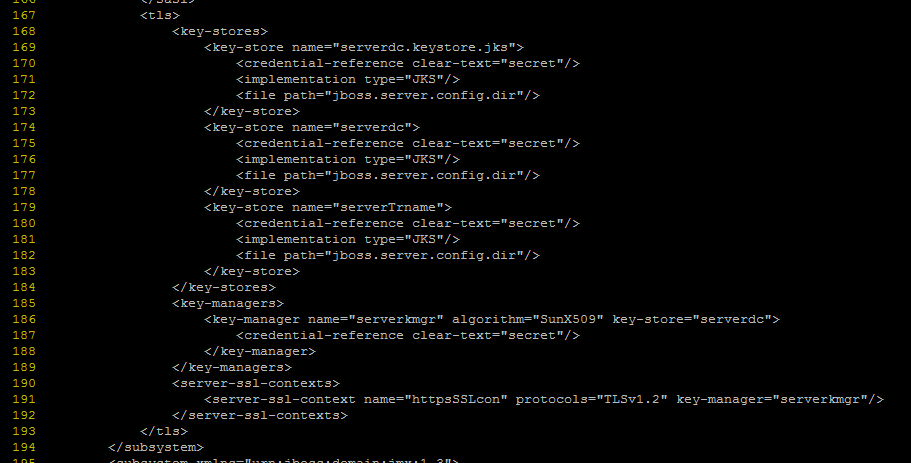


go to

146 <sasl>

147 <sasl-authentication-factory name="management-sasl-authentication" sasl-server-factory="configured" security-domain="Manageme ntDomain">

and see TLS will be there.



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

166 </sasl>

167 <tls>

168 <key-stores>

169 <key-store name="serverdc.keystore.jks">

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

171 <implementation type="JKS"/>

172 <file path="jboss.server.config.dir"/>

173 </key-store>

174 <key-store name="serverdc">

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

176 <implementation type="JKS"/>

177 <file path="jboss.server.config.dir"/>

178 </key-store>

179 <key-store name="serverTrname">

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

181 <implementation type="JKS"/>

182 <file path="jboss.server.config.dir"/>

183 </key-store>

184 </key-stores>

185 <key-managers>

186 <key-manager name="serverkmgr" algorithm="SunX509" key-store="serverdc">

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

188 </key-manager>

189 </key-managers>

190 <server-ssl-contexts>

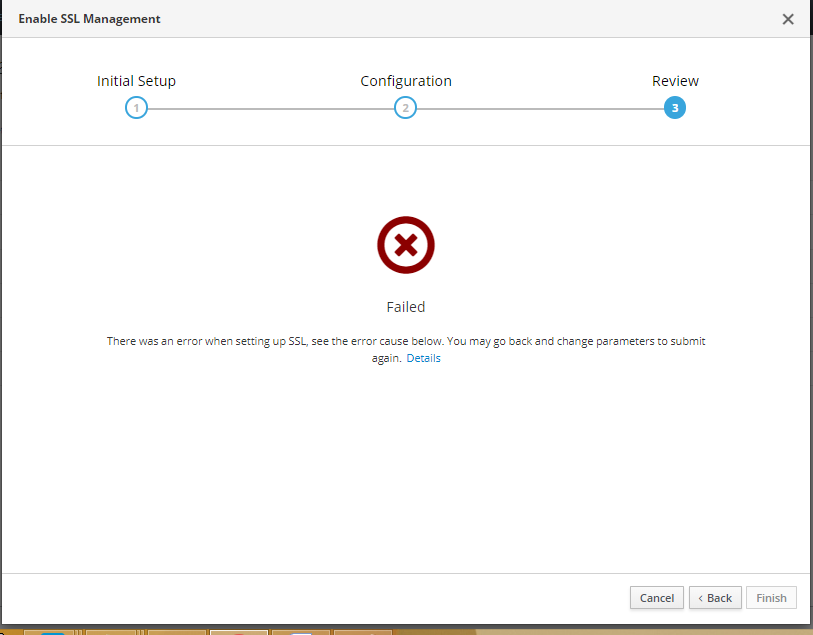
191 <server-ssl-context name="httpsSSLcon" protocols="TLSv1.2" key-manager="serverkmgr"/>

192 </server-ssl-contexts>

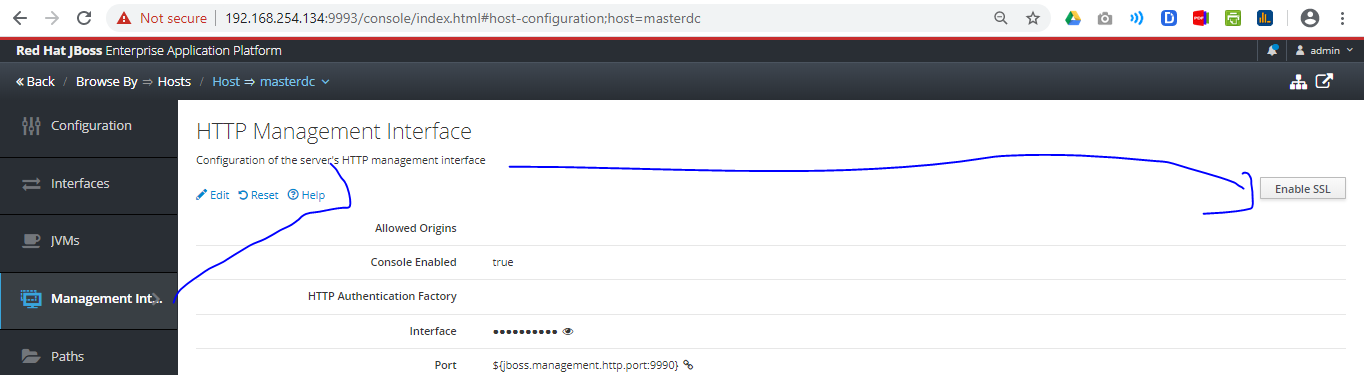
193 </tls>

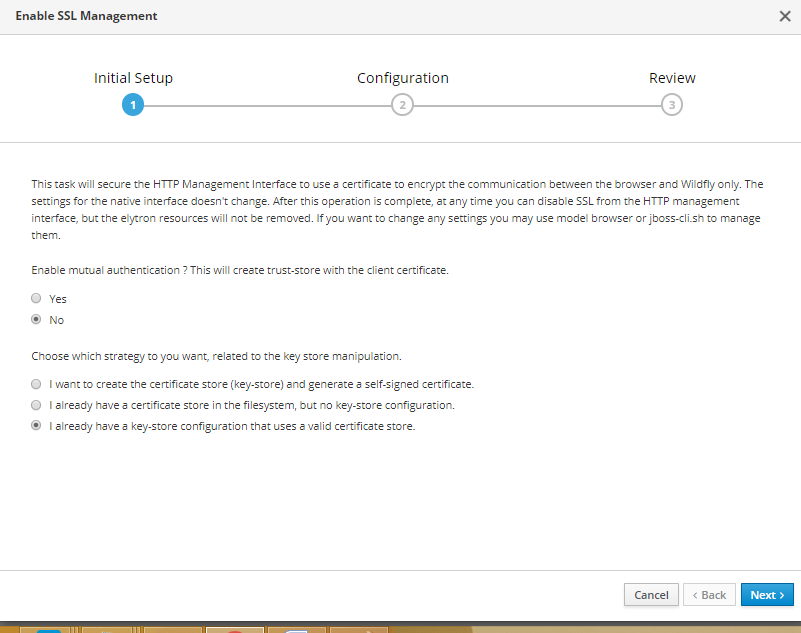
194 </subsystem>

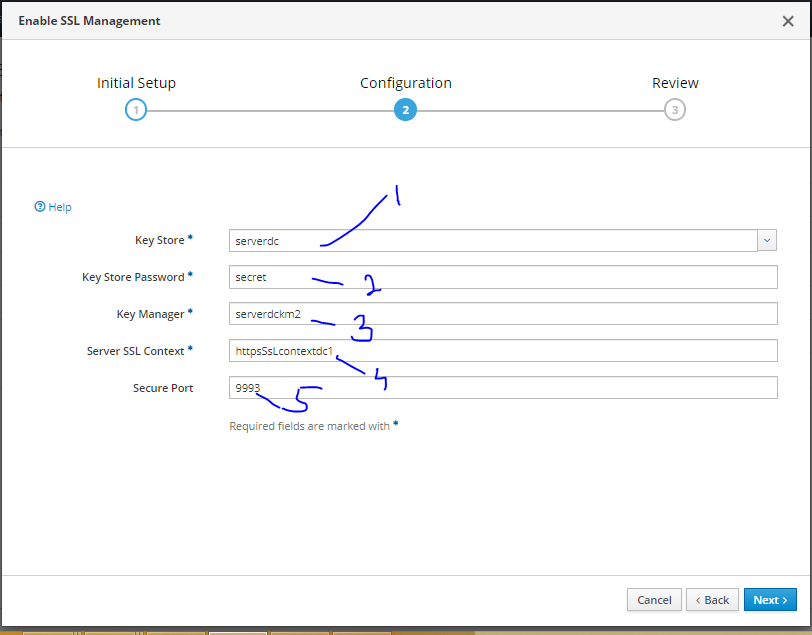
Now cancel the wizard that we have open



Again go to







1. Keystore name that we filled before getting error

174 <key-store name="serverdc">

2. Password that we set before (secret)

3. provide New KeyManager name , if you used the old provided name it will give you duplicate name issue.

4. SSL Context also need to be new name every time.

