JBOSS SECURITY : Encoding your KET_STORE|TRUST_STORE Password

Problem ## *Faced the security issue in one of audit. The issue captured was that our customized JBOSS structure was having server.xml that was embedded with KET_STORE password in PLIAN_TEXT_FORMAT.*

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
```
/**/opt/app/jboss/server/AInstance/deploy/jbossweb.sar/**server.xml**
```
<Connector protocol="HTTP/1.1" SSLEnabled="true"
       port="443" address="${jboss.bind.address}"
       scheme="https" secure="true" clientAuth="false"
       keystoreFile="/opt/……..
       keystorePass="password123" sslProtocols = "TLS"   //hardcoded password
       ciphers="TLS_RSA_WITH_……. _RSA_EXPO RT1024_WITH_DES_CBC_SHA" server=" "
          maxThreads="150" acceptCount="1000000" connectionTimeout="200000" />
```

Resolve Approach

Implemented following to resolve:

Step I: Modify above <Connector> with

/**/opt/app/jboss/server/AInstance/deploy/jbossweb.sar/**server.xml**
```
<Connector protocol="HTTP/1.1" SSLEnabled="true"
         port="#mhttpsport#" address="${jboss.bind.address}"
         scheme="https" secure="true" clientAuth="false"
         sslProtocol="TLS"
         securityDomain="java:/jaas/encrypt-keystore-password"
         SSLImplementation="org.jboss.net.ssl.JBossImplementation"
                  maxThreads="150" acceptCount="1000000" connectionTimeout="200000" />
```

Step II: Add/Edit security-service.xml file

//opt/app/jboss/server/AInstance/deploy/security-service.xml
```
<server>
   <mbean code="org.jboss.security.plugins.JaasSecurityDomain"
      name="jboss.security:service=PBESecurityDomain">
      <constructor>
         <arg type="java.lang.String" value="encrypt-keystore-password"></arg>
      </constructor>
      <attribute
name="KeyStoreURL">/opt/app/jboss/server/AInstance/conf/cert/product.keystore</attribu
te>
      <attribute
name="KeyStorePass">{CLASS}org.jboss.security.plugins.FilePassword:/opt/app/current/jb
oss/server/AInstance/conf/keystore.password</attribute>
      <attribute name="Salt">welcometojboss</attribute>
      <attribute name="IterationCount">13</attribute>
   </mbean>
</server>
```

Ranjan Kumar

Step III: Generate encoded password in file keystore.password by executing command

java -cp /opt/app/current/jboss/common/lib/jbosssx.jar \org.jboss.security.plugins.FilePassword encodekeystore 19 **password123** keystore.password
Note: Here '**password123**' is getting encoded via FilePassword's encode method.

Step IV: Add <depends> element in jboss-beans.xml
<depends>jboss.security:service=PBESecurityDomain</depends>
//opt/app/jboss/server/AInstance/deploy/jbossweb.sar/META-INF/jboss-beans.xml

Step V: Restart JBOSS server.

Other Approaches:

- ⇨ Encode keystore password that is xml understandable. Found @ http://coderstoolbox.net/string/#!encoding=xml&action=encode&charset=none
  Encoded Password: password123
  //password123

- ⇨ Override encode() of FilePassword jboss inbuilt class with custom encode().

References
https://docs.jboss.org/jbosssecurity/docs/6.0/security_guide