ACTIVE MQ SECURITY IMPLEMENTATION

FROM: <https://www.middlewareinventory.com/blog/active-mq-installation-and-security-setup-and-hardening-step-by-step/>

**Broker Security using Simple Authentication Plugin ( Encrypted Password)**

**Step1:** Add the following elements in **conf/activemq.xml**to setup Encryption method, Encryption Key, and Properties file

<bean id="environmentVariablesConfiguration" class="org.jasypt.encryption.pbe.config.EnvironmentStringPBEConfig">

<property name="algorithm" value="PBEWithMD5AndDES" />

<property name="passwordEnvName" value="ACTIVEMQ\_ENCRYPTION\_PASSWORD" />

</bean>

<bean id="configurationEncryptor" class="org.jasypt.encryption.pbe.StandardPBEStringEncryptor">

<property name="config" ref="environmentVariablesConfiguration" />

</bean>

<bean id="propertyConfigurer" class="org.jasypt.spring31.properties.EncryptablePropertyPlaceholderConfigurer">

<constructor-arg ref="configurationEncryptor" />

<property name="location" value="file:${activemq.base}/conf/credentials-enc.properties"/>

</bean>

**Step2:** To add the password into **credentials-enc.properties**file, we must encrypt the password using ActiveMQ **encrypt** command.

/activemq encrypt --password mysecretkey --input c0mp!ex@01

where passwordis a secret used by the encryptor and input is the password you want to encrypt.

While encrypting the password, you are going to issue the password as clear text in terminal which is not recommended use following snippet

I would not recommend it.   Use the following script instead, which does the same thing except it reads your password secretly and not showing on the terminal

#!/bin/bash

echo &quot;Enter the password to encrypt: &quot;

read -s pass

./activemq encrypt --password mysecretkey --input $pass

The Last line of the command will contain encrypted text

Note\*: You must also encrypt the password of activemq default account’s [system] password. The default password for the systemuser account is manager

After encrypting all the passwords, you need to add it to the credentials-enc.properties file

**Step3:**Add the encrypted passwords into credentials-enc.properties file

|  |
| --- |
| #activemq.username=system  #activemq.password=ENC(akuvjz1mFoau15BJwE5Mpg==)  #admin.username=admin  #admin.password=ENC(psJMVHGCcYjyZ+HvZFkBpOzIwnbcZygn)  testuser.username=testuser  testuser.password=ENC(Ci5pGj/RNaP85ZWnwT0zdA==)  #testguest.username=testguest  #testguest.password=EN(Ci5pGj/RNaP85ZWnwT0zdA==) |

Here we have  configured four usernames and its passwords

1. activemq.username and activemq.password for default system account ( this account is used by the web console to access the broker resources )
2. admin.username and admin.password is for admin privileged account
3. testuser.username and testuser.password is for user privileged account
4. testguest.username and testguest.password is for guest privileged account

**Step4:**Add the following Simple authentication plugin into **activemq.xml** file right after the **<broker>** tag starts

<plugins>

<simpleAuthenticationPlugin>

<users>

<!-- <authenticationUser username="${admin.username}"

password="${admin.password}"

groups="users,admins"/>🡪

<authenticationUser username="testuser"

password="${testuser.password}"

groups="users"/>

<!-- <authenticationUser username="testguest"

password="${testguest.password}"

groups="guests"/>-->

</users>

</simpleAuthenticationPlugin>

</plugins>

**Step5:**In order to setup Authorization, we must also add the Authorization plugin. Add the following entry, into **<plugins></plugins>** element

<authorizationPlugin>

<map>

<authorizationMap>

<authorizationEntries>

<authorizationEntry queue=">" read="admins" write="admins" admin="admins"/>

<authorizationEntry queue="USERS.>" read="users" write="users" admin="users"/>

<authorizationEntry queue="GUEST.>" read="guests" write="guests,users" admin="guests,users"/>

<authorizationEntry topic=">" read="admins" write="admins" admin="admins"/>

<authorizationEntry topic="USERS.>" read="users" write="users" admin="users"/>

<authorizationEntry topic="GUEST.>" read="guests" write="guests,users" admin="guests,users"/>

<authorizationEntry topic="ActiveMQ.Advisory.>" read="guests,users" write="guests,users" admin="guests,users"/>

</authorizationEntries>

</authorizationMap>

</map>

</authorizationPlugin>

**Step6:**Run Active-MQ using Encrypted Passwords

To run the Active-MQ broker with encrypted password configuration, follow the following steps:

1. Set environment variable for encryption

|  |  |
| --- | --- |
| 1 | $ export ACTIVEMQ\_ENCRYPTION\_PASSWORD=mysecretkey |

1. Set the AMQ broker

|  |  |
| --- | --- |
| 1 | $ bin/activemq start |

1. Reset the environment variable for encryption

|  |  |
| --- | --- |
| 1 | $ unset ACTIVEMQ\_ENCRYPTION\_PASSWORD |

1. Resetting the environment is important to avoid saving passwords on your system.

**Step7:**Start/Restart the ActiveMQ

#### Secure the console by encrypting the web-console username and password

By default, web console user credentials are stored in **jetty-realm.properties**

It will have a clear text username and password as shown below

|  |  |
| --- | --- |
| 1  2  3  4 | # Defines users that can access the web (console, demo, etc.)  # username: password [,rolename ...]  admin: admin, admin  user: user, user |

Now we need to encrypt this password for better security. This is how you need to do that

Now we need to encrypt this password for better security. This is how you need to do that

1. Download Jetty from<https://www.eclipse.org/jetty/download.html>
2. Unzip and Untar the downloaded package into the desired location on your server. Finally, you will get a directory like this

**jetty-distribution-9.4.10.v20180503** ( Version might change )

1. **cd** to that directory and you need to execute the encryption command

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | aksarav@mwinventory.in:/apps/amq/jetty-distribution-9.4.10.v20180503$ java -cp lib/jetty-util-9.4.10.v20180503.jar org.eclipse.jetty.util.security.Password adminuser admin  2018-05-22 02:48:41.398:INFO::main: Logging initialized @179ms to org.eclipse.jetty.util.log.StdErrLog  admin  OBF:1u2a1toa1w8v1tok1u30  MD5:21232f297a57a5a743894a0e4a801fc3  CRYPT:adpexzg3FUZAk |

Here adminuser is the salt which is used to encrypt the password not the actual username and admin is the password

The last line contains our encrypted password

CRYPT:adpexzg3FUZAk

Now, Copy this password to **jetty-realm.properties** and replace the clear text password

|  |  |
| --- | --- |
| 1  2  3  4 | # Defines users that can access the web (console, demo, etc.)  # username: password [,rolename ...]  admin: CRYPT:adpexzg3FUZAk, admin  user: user, user |

Start/Restart your ActiveMQ instance

Need to add following entry in ACTIVE\_MQ\_HOME/webapps/admin/WEB-INF/webconsole-embedded.xml

<!-- <bean class="org.springframework.beans.factory.config.PropertyPlaceholderConfigurer">

<property name="locations">

<value>file:${activemq.conf}/credentials.properties</value>

</property>

</bean> -->

<bean id="environmentVariablesConfiguration" class="org.jasypt.encryption.pbe.config.EnvironmentStringPBEConfig">

<property name="algorithm" value="PBEWithMD5AndDES" />

<property name="passwordEnvName" value="ACTIVEMQ\_ENCRYPTION\_PASSWORD" />

</bean>

<bean id="configurationEncryptor" class="org.jasypt.encryption.pbe.StandardPBEStringEncryptor">

<property name="config" ref="environmentVariablesConfiguration" />

</bean>

<bean id="propertyConfigurer" class="org.jasypt.spring31.properties.EncryptablePropertyPlaceholderConfigurer">

<constructor-arg ref="configurationEncryptor" />

<property name="location" value="file:${activemq.base}/conf/credentials-enc.properties"/></bean>

==================================================================================Following can also be used <bean id="environmentVariablesConfiguration" class="org.jasypt.encryption.pbe.config.EnvironmentStringPBEConfig">

<property name="algorithm" value="PBEWithMD5AndDES" />

<property name="passwordSysPropertyName" value="activemq\_encryptor\_passphrase" />

</bean>

Instead of

<bean id="environmentVariablesConfiguration" class="org.jasypt.encryption.pbe.config.EnvironmentStringPBEConfig">

<property name="algorithm" value="PBEWithMD5AndDES" />

<property name="passwordEnvName" value="ACTIVEMQ\_ENCRYPTION\_PASSWORD" />

</bean>

In that case we need -Dactivemq\_encryptor\_passphrase=secretkey in start up script

"%\_JAVACMD%" %ACTIVEMQ\_SUNJMX\_START% %ACTIVEMQ\_DEBUG\_OPTS% %ACTIVEMQ\_OPTS% %ACTIVEMQ\_SSL\_OPTS% -Dactivemq.classpath="%ACTIVEMQ\_CLASSPATH**%" -Dactivemq\_encryptor\_passphrase=** **secretkey** -Dactivemq.home="%ACTIVEMQ\_HOME%" -Dactivemq.base="%ACTIVEMQ\_BASE%" -Dactivemq.conf="%ACTIVEMQ\_CONF%" -Dactivemq.data="%ACTIVEMQ\_DATA%" -Djava.io.tmpdir="%ACTIVEMQ\_TMP%" -jar "%ACTIVEMQ\_HOME%/bin/activemq.jar" %\*

And encrypy command have to use this value as secret key(here secretkey)

activemq encrypt --password mysault --input activemq

and do it for every users