SETUP IBM MQ SSL

Project Name: IBM MQ Configuring SSL Document

Date: 5/11/2016
Technical Architect: Chuck Misuraca
TABLE OF CONTENTS

PURPOSE .................................................................................................................. 3

REVISION LOG ......................................................................................................... 4

1.0 INTRODUCTION .................................................................................................. 5

2.0 KEY DATABASE ................................................................................................... 5

2.1 CONFIGURE THE KEY DATABASE ..................................................................... 5

3.0 CERTIFICATES ..................................................................................................... 6

3.1 ADD THE SIGNER CERTIFICATE ....................................................................... 6

3.2 CREATING A PERSONAL CERTIFICATE REQUEST ....................................... 6

3.3 ADD THE PERSONAL CERTIFICATE ............................................................... 8

3.4 EXPORT THE PUBLIC CERTIFICATE ................................................................ 8

3.5 ADD THE PUBLIC CERTIFICATE ...................................................................... 9

3.6 UPDATE QMGR WITH KEY DB INFO IF NEEDED ............................................. 9

5.2 UTILITY CMDS FOR SSL KEY DB: ................................................................. 10

List key DB info: ................................................................. 10
List Key DB expiry date: .......................................................... 10
List Certs: ...................................................................................... 10
List Certs expiry date and more: ..................................................... 10
List Cert Requests: ........................................................................ 10
Delete Cert Requests: .......................................................................... 11
Get Cert from another Key DB: ............................................................... 11
Recreate stash file for Key DB: ............................................................... 11
Recreate Cert request for an Expired CERT: ........................................... 11

APPENDIX A – KEY DATABASE PASSWORD MISSING .......................................... 11
Purpose

The purpose of this document is to provide a cookbook level instructions on setting up SSL/TLS for IBM MQ without using a GUI.

This document is a supplement to any official document that IBM has provided on the topic of IBM MQ Multi-instance installation and configuration. Official documents on this subject from IBM can be obtained on the Info Center for the specific version of MQ.

NOTE: if you cut and paste from this MS word doc to Linux. Make should the quote makes(“” or “”’) and dashes(-) are text and not word symbols.
## Revision Log

<table>
<thead>
<tr>
<th>Release No.</th>
<th>Date</th>
<th>Revision Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5/11/2016</td>
<td>Initial Documentation</td>
<td>C. Misuraca</td>
</tr>
</tbody>
</table>

Perficient
1.0 Introduction

This document is a command line version for setting up the key database, requesting, adding and exporting certs. Once all of that is done then SSL can be turned on for the sender/receiver channels that connect queue managers and MQ Clients.

2.0 Key Database

2.1 Configure the Key Database

The key database is where the SSL certificates are stored. The location is in the /var/mqm/qmgrs/<QMGR_NAME>/ssl directory.

1. Change to the following directory.

   cd /var/mqm/bin

2. Run the following command to create a new Key database. NOTE: Password –pw option can be whatever you want. DO NOT forget it.

   ./runmqakm -keydb -create -db /var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW -type cms -expire 360 -stash
3.0 Certificates

3.1 Add the Signer Certificate

The Signer Certificates tells MQ that the Private Certificate that you received back from Clients Security Department.

```
./runmqakm -cert -add -db /var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW -label ‘<Client’s Corporation Name> CA’ -file /var/mqm/qmgrs/<QMGR_NAME>/ssl/<Client’s Corporation Name>CA.cer -format ascii
```

This step may need to be repeated several times.

3.2 Creating a Personal Certificate Request

1. Create a Personal Certificate Request.

2. **Important!** For the Key Label enter in “ibmwebsheremq<QMgr name in lower case>”.

Examples: `ibmwebsphereemqlax.qm` or `ibmwebsphereemqny.qm`

The name is depend on the mq environment.

**Distinguished Name or –dn is dependent on the clients IT security standards.**
/runmqakm -certreq -create -db /var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW -label ibmwebspheremqnyqrcmqm -size 2048 -dn “CN=LAX.QM,DC=<Client’s Corporation Name>,DC=com” -file /var/mqm/qmgrs/<QMGR_NAME>/ssl/LAX.QMqmcertreq.arm

Send the arm file to the clients Security department so they can provide you with the SSL Certificate. This step is very dependent on the clients CERT creation process.

3. The information that you receive back from the Security Department will be the Private Certificate for that Queue Manager.

4. Change the name of the file to <qm>privatecert.arm or <qm>privatecert.cert
Example: LAX.QMprivatecert.arm

5. Move the Private Certificate to the /var/mqm/qmgrs/<QMGR_NAME>/ssl directory.

6. Continue to the next section to implement the Certificate.
3.3 Add the Personal Certificate

The Personal Certificate that you received from the Security Department goes back on the same Queue Manager that you requested it from.

3. Run this command with your names. Put everything on one line to receive the new Certificates:

```bash
/var/mqm/bin/runmqakm -cert -receive -db
/var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW -file
/var/mqm/qmgrs/<QMGR_NAME>/ssl/LAX.QMprivatecert.arm -format ascii
```

3.4 Export the Public Certificate

The Public Certificate must be generated/export and then moved over to the other Queue Manager or MQ Client that this queue manager will be communicating with. As well as we need to import the Public Certificate of the other queue manager into this one.

7. Extract the public(trust store) Cert from the Key database by using the label from the cert request step. Name it so that it will be distinguish from other certificates. In this case it is LAX.QMpubliccert.arm.

8. Run this command with your values.

```bash
/var/mqm/bin/runmqakm -cert -extract -db
/var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW -label
ibmwebspheremqnyq.cqm -target
/var/mqm/qmgrs/<QMGR_NAME>/ssl/LAX.QMpubliccert.arm -format ascii
```

Perficient
9. Retrieve the `<qmgrpname>`publiccert.arm file from the `ssl` directory on the system and copy it to the same location on the other Queue Manager(s) or MQ Clients(i.e. MQ Explorer) that this queue manager will be communication with.

10. Continue to the next section to import the Public Certificate.

### 3.5 Add the Public Certificate

Importing the Public Certificate from the other Queue Manager.

11. Run this command with your values to add a Signer Certificates:

```
 /var/mqm/bin/runmqakm -cert -add -db 
 /var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW -label ibmwebspheremqnc.yc.qm -file /var/mqm/qmgrs/<QMGR_NAME>/ssl/<Other Qmgr>/publiccert.arm -format ascii
```

### 3.6 Update Qmgr with Key db info if needed

**NOTE** -> * key is the first half of the key db name. Not a directory.

```
 echo "dis QMGR"| runmqsc <Qmgr Name>
 echo "ALTER QMGR SSLKEYR(' var/mqm/qmgrs/<QMGR_NAME>/ssl/ key')" | runmqsc <Qmgr Name>
 echo "dis QMGR"| runmqsc <Qmgr Name>
```

Perficient
**5.2 UTILITY CMDS for SSL key DB:**
Change values to match your MQ install.

**List key DB info:**
/var/mqm/bin/runmqakm -keydb -list -db
/var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW

**List Key DB expiry date:**
/var/mqm/bin/runmqakm -keydb -expiry -db
/var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW

**List Certs:**
/var/mqm/bin/runmqakm -cert -list -db /var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW

**List Certs expiry date and more:**
/var/mqm/bin/runmqakm -cert -details -db
/var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW -label ibmwebspheremq<Qmgr Name>

**List Cert Requests:**
/var/mqm/bin/runmqakm -certreq list -db
/var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW

Perficient
Delete Cert Requests:
/var/mqm/bin/runmqakm -certreq –delete -db
/var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw ibmsslDBPW -label ibmwebspheremq<Qmgr Name>

Get Cert from another Key DB:
/var/mqm/bin/runmqakm -cert -import -db /var/mqm/qmgrs/<QMGR_NAME>/ssl
/devStoremq.kdb -pw pass1 -type cms -label ibmwebspheremqstore_QM -target
/var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -target_pw Su7ap$sup -new_label ibmwebspheremqstore_QM –target_type cms –fips

Recreate stash file for Key DB:
/var/mqm/bin/runmqakm -keydb -stashpw -db
/var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw Su7ap$sup

Recreate Cert request for an Expired CERT:
/var/mqm/bin/runmqakm -certreq -recreate -db
/var/mqm/qmgrs/<QMGR_NAME>/ssl/key.kdb -pw Su7ap$sup -label ibmwebspheremq<QMGR_NAME lower case> -target
/var/mqm/qmgrs/<QMGR_NAME>/ssl/<QMGR_NAME>qmcertreq.arm

Appendix A – key database password missing
Use this carefully!

URL: https://websphereapplicationservernotes.files.wordpress.com/2012/04/websphere-doctor-7-recover-kdb-password.pdf

Perficient