WebSphere MQ : Mise en oeuvre de SSL

Principe

Ce document décrit la procédure utilisée pour mettre en œuvre une liaison SSL entre deux systèmes WebSphere MQ. Il suppose la maîtrise de l'environnement WebSphere MQ sur les plates-formes considérées.

Les Etapes

Les différentes étapes à réaliser sont les suivantes :

- Génération des certificats
- Importation des certificats dans l'environnement et copie des certificats dans l'environnement WebSphere MQ
- Affectation du certificat personnel au Queue Manager
- Modification de la configuration MQ et tests SSL

Certificats

Deux certificats sont nécessaires pour la configuration :

- Le certificat personnel (relatif au Queue Manager). Il est fourni sous la forme d'un fichier binaire PKCS12, avec une extension « *.p12* », protégé par un mot de passe d'exportation. Il faut un certificat personnel par Queue Manager.

  Ce certificat doit avoir un label (= friendly name, = key label) constitué ainsi : *ibmwebspheremq<nom_du_qm_en_minuscules>*. Par exemple, si le Queue Manager est LMD01, le label du certificat doit être : ibmwebspheremqlmd01. La syntaxe de ce label est facultative sous Windows, mais impérative sous Unix. Il est renseigné lors de la création du certificat.

  Attention, les règles de composition du label sont différentes sur z/OS : si le Queue Manager est CSQ1, le label du certificat doit être : ibmwebspheremqCSQ1

- Le certificat « *Root* » qui a servit à signer le certificat personnel. Il est fourni sous la forme d'un fichier texte X509, avec une extension « *.crt* ».

Si votre entreprise ne dispose pas d'une PKI, elle doit se procurer (acheter) les certificats SSL auprès d'une société fournissant ce type de service. Pour éviter de dépendre des délais d'un fournisseur de certificats pendant les tests, il est préférable d'utiliser un produit type « OpenSSL », qui est un freeware disponible sous Unix et Windows, permettant de créer ses propres certificats SSL.

La procédure d'importation des certificats varie suivant que le système cible est Windows NT, Windows 2000/XP, Unix ou z/OS.

L'ensemble des opérations est détaillé dans le document IBM : SC34-6079-01, « WebSphere MQ Security ».

Contact : ftwmq@demey-consulting.fr - http://demey-consulting.fr

WebSphere MQ : Mise en oeuvre de SSL

Importation des certificats dans l'environnement WMQ Windows

Note : On suppose que l'on utilise Windows 2000/XP/2003, et que le produit WMQ 5.3 / CSD 4 ou + est installé sur le système.

L'importation est effectuée à partir de l'Explorateur WebSphere MQ, ce qui permet d'effectuer en une seule opération l'importation des certificats et leur copie dans l'environnement WMQ.

Le « Certificate Store » (*Magasin de certificats* ou *Référentiels de clés* suivant les ouvrages) par défaut pour un Queue Manager se nomme « key.sto » dans le répertoire « ssl » des fichiers du Queue Manager. Lorsque l'on manipule un Certificate Store, on ne précise pas l'extension « .sto ».

A partir de l'Explorateur WMQ, vérifiez que votre Queue Manager est démarré, cliquez droit sur le nom est choisissez « Propriétés» . Dans l'onglet SSL, le nom du Certificate Store par défaut est déjà précisé. Par exemple, si le chemin des fichiers pour les Queue Managers est "*D:\WebSphere MQ*\ " et que le Queue Manager se nomme « LMD », le nom qualifié du Certificate Store est « *D:\WebSphere MQ\qmgrs\LMD\ssl\key* ». Notez que l'extension « .sto » n'est pas indiquée.

Si cet emplacement et/ou ce nom ne vous conviennent pas, vous pouvez préciser d'autres valeurs, le fichier « .sto » sera crée automatiquement à l'endroit et avec le nom souhaités.

Importation du certificat Root

- Dans l'écran « Propriétés » du Queue Manager, cliquez sur « Gérer les certificats SSL », et sur l'écran suivant « Gestion des Certificats » cliquez sur « Ajouter ».
- Choisissez « Importer », et précisez le nom du fichier contenant le certificat « Root ». Ce fichier a un suffixe « .crt ».
- Cliquez sur « Ajout ». Après l'ajout, l'écran « Gestion des Certificats » est affiché.

Importation du certificat utilisateur

- Sur l'écran « Gestion des Certificats » cliquez sur « Ajouter ».
- Choisissez « Importer », et précisez le nom du fichier contenant le certificat utilisateur. Ce fichier a un suffixe « .p12 ».

- Indiquez le mot de passe d'exportation de ce certificat et cliquez sur « Ajout ». Après l'ajout, l'écran « Gestion des Certificats » est affiché.

Importation des certificats dans l'environnement WMQ Unix

La gestion des certificats SSL sous Unix est effectué via l'outil IBM iKeyman, fourni avec WebSphere MQ 5.3. Les certificats sont stockés dans une base de clé (keyring) représenté par dans un fichier d'extension « *.kbd* ».

Cet outil dispose d'un interface ligne de commande (gsk6cmd) et d'une interface graphique X11 (gsk6ikm).

La procédure décrite ici utilise l'interface graphique, le principe reste le même en ligne de commande. Cela suppose que sur le poste utilisé pour la configuration on ait un logiciel serveur X11 (PC-Xware par exemple). Le système utilisé est AIX mais reste valable en environnement Solaris ou HPUx avec des modifications mineures (par exemple en remplaçant /usr/mqm/ par /opt/mqm/).

Préparation de l'environnement

- Positionnement du JAVA_HOME

  En ligne de commande, sous un profil appartenant au groupe « *mqm* », taper :

  ```
  export JAVA_HOME=/usr/mqm/ssl/jre
  ```

- Exportation de la session

  ```
  export DISPLAY=10.126.xxx.xxx:0
  ```

où `10.126.xxx.xxx` est l'IP du poste de travail utilisé pour la configuration.

- Lancement d'iKeyman en mode X11

  ```
  gsk6ikm
  ```

Création de la base de clés

La base de clés peut être créée à l'emplacement de votre choix. Choisissez comme type de base : « *cms* ». Le nom de la base est libre mais le suffixe doit être « *.kdb* ».

Indiquez un mot de passe pour protéger cette base, une date de validité pour ce mot de passe, et cochez l'option « *Stash password to a file ?*».

Lors de la création de la base de clés, celle-ci est pré-chargée avec un certain de certificats (Verisign, Thawte, RSA, …)

Il faut d'abord importer le certificat « *Root* », puis le certificat personnel du Queue Manager.

Certificat Root

- Vérifiez que vous êtes positionné sous l'onglet « *Signer Certificates* ».

- Cliquez sur « *Add* », et dans la boite de dialogue suivante, choisissez « *Browse* ».
- Sélectionnez le fichier contenant le certificat Root (en général avec l'extension « *.crt* »).
- Validez puis indiquez un label pour ce certificat, par exemple « *CA Root pour G72* »

Le certificat importé doit maintenant être visible (parmi d'autres), sous l'onglet « *Signer Certificates* », avec comme nom le label spécifié ci-dessus.

Certificat personnel

- Vérifiez que vous êtes positionné sous l'onglet « *Personnal Certificates* ».
- Cliquez sur « *Import* », et dans la boite de dialogue suivante, vérifiez que le type de fichier est « PKCS12 », et cliquez sur « *Browse* ».
- Sélectionnez le fichier contenant le certificat personnel du Queue Manager (en général avec l'extension « *.p12* »).
- Validez puis indiquez le mot de passe d'exportation de ce certificat.
    - Le certificat importé doit maintenant être visible (parmi d'autres), sous l'onglet « *Personnal Certificates* », avec comme nom le « friendly name ».

Affectation du certificat utilisateur au Queue Manager

Environnement Windows

- A partir de l'écran « Gestion des certificats SSL », cliquez sur « Attribuez ».
- L'écran « Attribution du certificat de gestionnaire de file d'attente » s'affiche, avec la liste de tous les certificats utilisateurs présents dans ce magasin.
- Sélectionnez le certificat utilisateur souhaité, et cliquez sur « Attribuer »
- L'écran « Gestion des certificats SSL » s'affiche, et cette fois précise qu'un certificat a été attribué au Queue Manager.

Il n'est pas nécessaire de re-démarrer le Queue Manager pour prendre en compte cette modification.

Environnement Unix

Il faut affecter au Queue Manager la base de clés créée et renseignée à l'étape précédente. Il n'y a pas besoin de préciser le nom du certificat, car ce nom doit correspondre à celui que Queue Manager : *(ibmwebspheremq + nom_du_qm_en_minuscules)*

Ceci est réalisé via la commande MQSC `alter qmgr :`

```
alter qmgr sslkeyr('<chemin ><nom_du_fichier>')
```

où :

- Chemin : emplacement du la base de clés
- Nom_du_fichier : nom de la base de clés, sans l'extension « .kbd »

Exemple :

Si la base de clé a pour nom : lmd01.kbd, dans le répertoire : `/var/mqm/qmgrs/LMD/ssl/`, la commande sera alors :

```
alter qmgr sslkeyr('/var/mqm/qmgrs/LMD/ssl/lmd01')
```

Il n'est pas nécessaire de re-démarrer le Queue Manager pour prendre en compte cette modification.

Modification de la configuration MQ

Pour activer le SSL sur un channel, il faut ensuite modifier la définition du channel en spécifiant par exemple :

```
ALTER CHANNEL (nom_channel) +
CHLTYPE(SDR) +
SSLCIPH(RC4_MD5_EXPORT) +
SSLCAUTH(REQUIRED)
```

Les modifications doivent bien entendu être effectuées sur le channel sender d'un coté et sur le channel receiver de l'autre coté.

En cas de problèmes SSL lors du démarrage des channels, le détail des incidents rencontrés est disponible dans les fichiers AMQERR01.LOG

Fin du document