Guide MQ du 13 Juin 2017

Introduction à la sécurité IBM MQ

Luc-Michel Demey
Demey® Consulting
LMD@demey-consulting.fr

Approche globale

- La sécurisation d'un environnement MQ nécessite une approche globale :
  - Application locales
  - Protection du Queue Manager
  - Identification des partenaires
    - DQM
    - Client MQ
    - Cluster
  - Chiffrement / Scellement des messages

Rappels des valeurs par défaut

- Jusqu'en version 7.0 inclus :
  - Un Queue Manager partenaire peut déposer des messages dans n'importe quelle file
  - Un client MQ, via un canal SVRCONN, peut visualiser / modifier / déposer des messages dans n'importe quelle file
  - Un client MQ peut, via un outil d'administration, visualiser / modifier la configuration des objets MQ
  - Un service MQ permet d'accéder, sans authentification préalable, à la ligne de commande du serveur
  - Par rebond, l'intrusion dans un QM permet de rebondir vers l'intérieur du réseau
- Ceci reste valable en version 7.1 / 7.5 / 8.0 / 9.0 si :
  - Le QM a été créé avant la migration et n'a pas été modifié
  - Le QM a été créé en 7.1/7.5/8.0/9.0 et la sécurité des canaux a été désactivée (CHLAUTH à DISABLED)

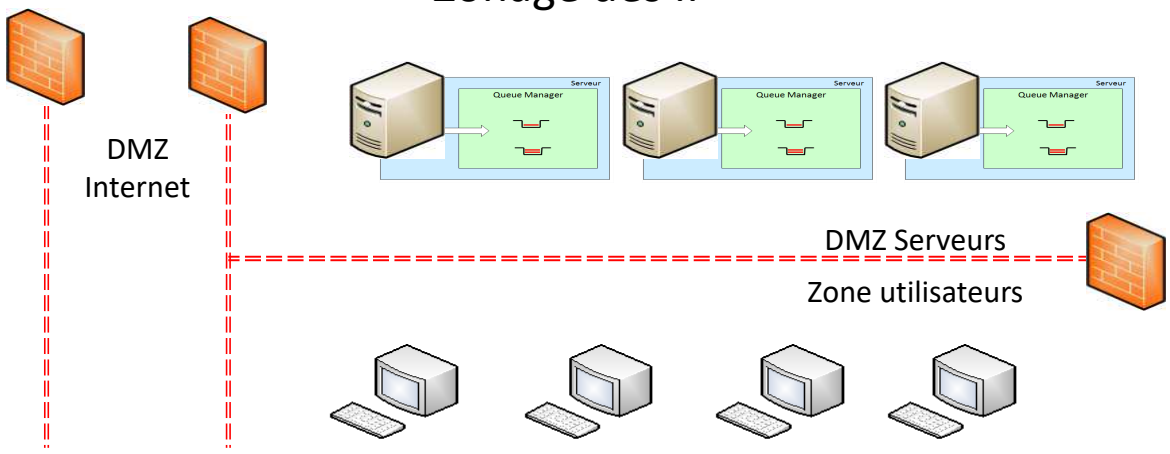
Conséquences

- La configuration par défaut d'un Queue Manager doit être modifiée dés sa création
- Le fonctionnement et les implications de la sécurité MQ doivent être connus et compris
- La stratégie de sécurisation doit être globale, impliquant l'ensemble des acteurs du SI, y compris les partenaires.

Panorama des solutions

- Zonage des IP (firewall)
- OAM
- MCAUSER
- Exits
- SSL/TLS
- AMS
- MQIPT
- CHLAUTH
- CONNAUTH

Zonage des IP



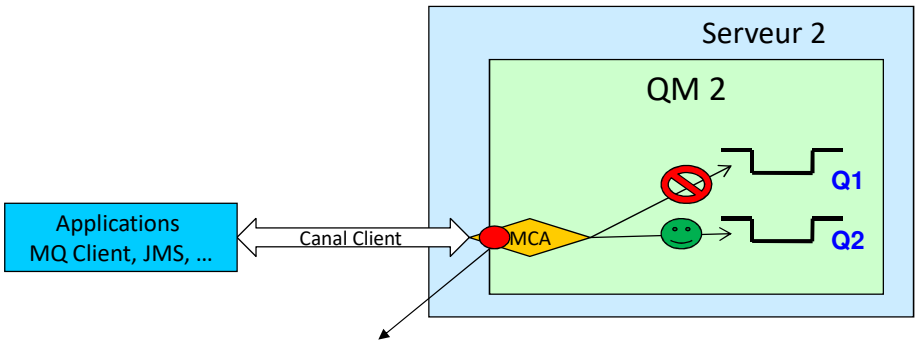
OAM

- OAM : Object Authority Manager
- Gère des ACL pour les objets WMQ / par QM
- Indépendant de la sécurité de l'OS
- Droits pour les comptes ou les groupes
- Attribution très granulaire des droits MQ
- Interface commune sur les QM distribués :
  - setmqaut / dspmqaut / dmpmqaut
  - SET / DISPLAY / DELETE AUTHREC

MCAUSER

- Paramètre d'un canal Receiver ou SVRCONN
- Permet de surcharger le compte utilisé pour déposer les messages à l'arrivée sur le QM
  - En imposant un compte si SVRCONN
  - Avec un compte autre que « mqm » si RECEIVER
- A associer avec l'OAM (setmqaut)
- Usage :
  - Normalisation du compte entrant pour les clients MQ
  - Contrôle des droits pour les clients MQ et le DQM

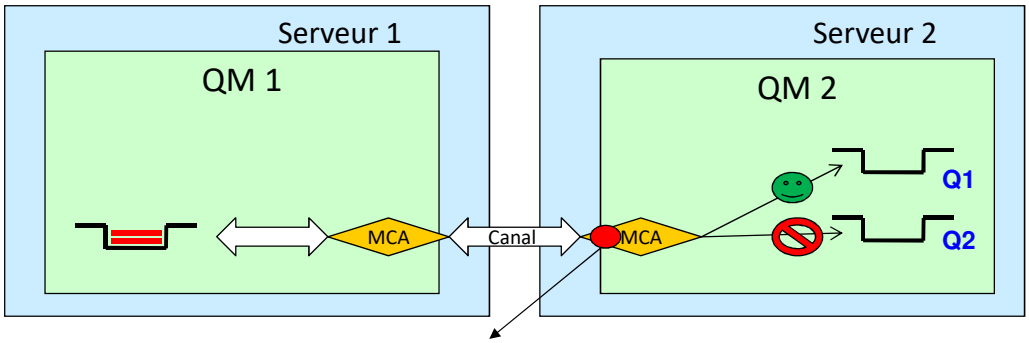
MCAUSER et client MQ



MCAUSER = ‘user_cli1’

Nécessite : setmqaut –m QM2 –n Q2 –t queue –p user_cli1 +put

MCAUSER en DQM



MCAUSER = ‘user_qm1’

Nécessite : setmqaut –m QM2 –n Q1 –t queue –p user_qm1 +put

Exit de Canal

- Utilisation du Security Exit
- Déclenché lors du démarrage du canal
- Usage :
  - Vérification de données envoyées par le partenaire
  - Vérification de l'adresse IP (BlockIP2 - MrMQ.dk)
  - Surcharge dynamique du MCAUSER
  - Authentification
- Inconvénients :
  - Solution non standard, souvent réservée aux échanges internes
  - Développement / maintenance des exits en multiplateforme
- Solutions commerciales
  - MQ Authenticate User Security Exit (MQAUSX) – Capitalware

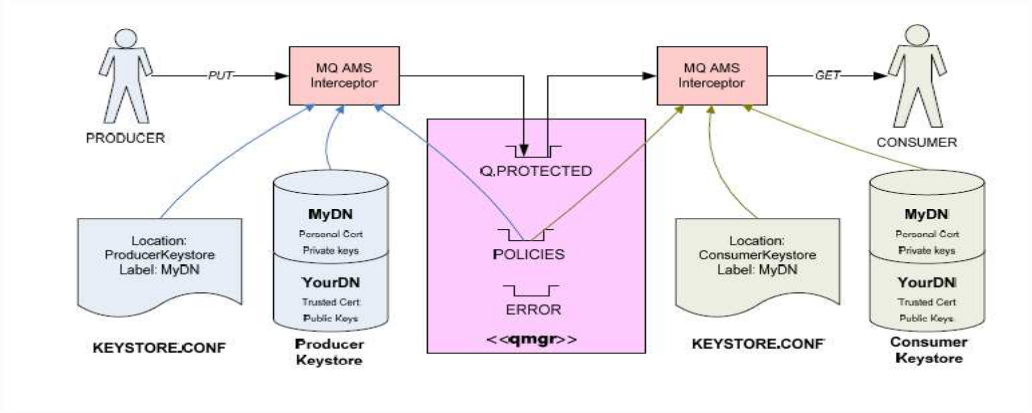
SSL/TLS

- Inclus dans MQ depuis la version 5.3
- Authentification du partenaire (QM ou client)
- Chiffrement du flux sur le canal (messages en transit)
- Choix de CipherSpec
- Pas de protection des messages dans les files
- Invalidation des CipherSpecs vulnérables
  - Avant : 44 CipherSpecs
  - 8.0.0.3 : 17 CipherSpecs

AMS

- IBM MQ Advanced Message Security
- Remplace WebSphere MQ Extended Security Edition
- Utilise SSL pour chiffrement + signature
- Assure le respect de « policies »
- Chiffrement des messages lors du MQPut
- Déchiffrement lors du MQGet
- Transparent pour les applications

IBM MQ Advanced Message Security (AMS)

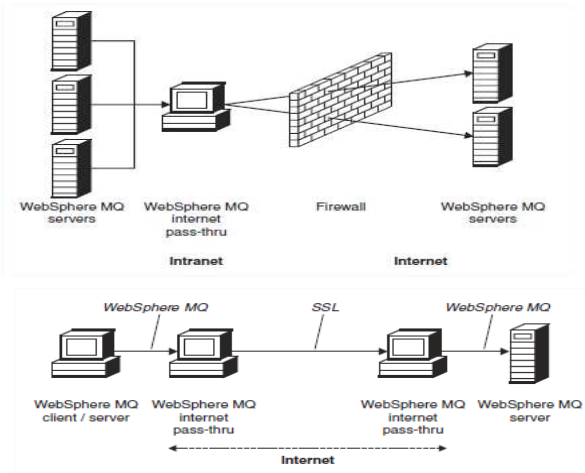


MQIPT

- WebSphere MQ internet pass-thru
- Extension du logiciel, sous forme de Support Pack MS81
- Concentration / Tunneling du flux canal en http(s)
- Co-localisé ou non avec WMQ

MS81: WebSphere MQ internet pass-thru :
http://www-01.ibm.com/support/docview.wss?uid=swg24006386

MQ internet pass-thru (MQ IPT)



Channel Authentication Records

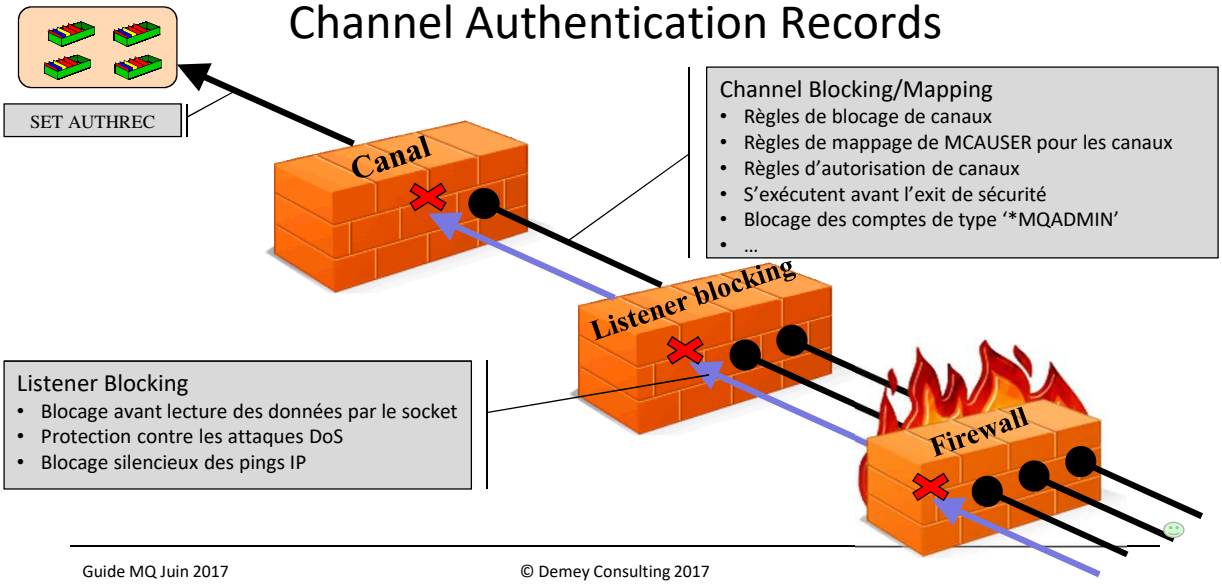
- Permettent le contrôle des flux entrants depuis :
  - Clients MQ
  - Queue Managers
  - Autres (scans, monitor, ...)
- Contrôle canal par canal
- Nouvelle commande MQSC : SET CHLAUTH
- Désactivable :

  ALTER QMGR CHLAUTH(ENABLED|DISABLED)
  - ENABLED pour les QM créés en 7.1/7.5
  - DISABLED pour les QM créés en 7.0

Channel Authentication Records

- Les règles peuvent :
  - Autoriser la connexion
  - Autoriser la connexion et affecter dynamiquement un MCAUSER
  - Interdire la connexion
  - Interdire l'accès depuis un compte de type "mqadmin"
- En utilisant :
  - L'adresse IP distante
  - Le nom du QM distant
  - Le compte fourni par le client distant
  - Tout ou partie du DN du certificat SSL
- Accès aux canaux SVRCONN bloqué par défaut pour les comptes de type « Admin MQ ».

Channel Authentication Records



CONNAUTH : Connection Authentication

Nouveau en MQ 8.0

- Activation de la demande de mot de passe pour les applications MQ
- Y compris pour les connections canal – dont SVRCONN
- Géré par un objet MQ : AUTHINFO de type :
  - IDPWOS : utilisation de la base de comptes locale
  - IDPWLDAP : utilisation de la base de compte LDAP
- Paramètre CONNAUTH du QM pour utiliser une AUTHINFO :
  - SYSTEM.DEFAULT.AUTHINFO.IDPWLDAP
  - SYSTEM.DEFAULT.AUTHINFO.IDPWOS (par défaut)
  - User defined

CONNAUTH & AUTHINFO: valeurs par défaut

- DISPLAY QMGR CONNAUTH :

  CONNAUTH(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)

- DISPLAY AUTHINFO(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)

```
AUTHTYPE(IDPWOS)                ADOPTCTX(NO)
DESCR( )                        CHCKCLNT(REQDADM)
CHCKLOCL(OPTIONAL)              FAILDLAY(1)
ALTDATE(2017-01-04)             ALTTIME(19.41.52)
```

- CHCKCLNT(REQDADM) :
  - Mot de passe facultatif pour les connections client MQ via un compte de base
  - Mot de passe REQUIRED pour les connections client MQ avec un compte de type « admin MQ »

Script MQSC pour administration « full » en mode MQ Client

```
* Création du canal SVRCONN
DEFINE CHANNEL('ADMIN') +
   CHLTYPE(SVRCONN) +
   MCAUSER('%interdit%')  +
   SHARECNV(1) +
   DESCR('Canal pour admin') +
   REPLACE
* Suppression du blocage des comptes *MQADMIN pour ce canal
SET CHLAUTH(ADMIN) +
   TYPE(BLOCKUSER) +
   USERLIST(toto) action (ADD)
* Désactivation de la demande de mot de passe pour comptes
*MQADMIN
ALTER AUTHINFO(SYSTEM.DEFAULT.AUTHINFO.IDPWOS) +
   AUTHTYPE(IDPWOS) +
   CHCKCLNT(OPTIONAL)
```

```
* Mapping de comptes avec le MCAUSER mqm
SET CHLAUTH(ADMIN) +
  TYPE(USERMAP) +
  CLNTUSER('lmd') +
  DESCR('Luc-Michel Demey') +
  MCAUSER('mqm') +
  ACTION(REPLACE)

*-- Purge du cache de sécurité
REFRESH SECURITY TYPE(CONNAUTH)
REFRESH SECURITY TYPE(AUTHSERV)
```

Note : ce script assure une protection minimum du QM en gardant le CHLAUTH activé

Autres options

- LDAP pour authentifier les utilisateurs MQ 8002
  - Définitions des comptes et groupes coté OS plus nécessaire
  - Disponible pour Unix, Windows, IBM i
- Authentification PAM pour Unix
  - Pluggable Authentication Modules
  - Même principe que LDAP en 8002
- Nouveaux events de sécurité
- Masquage du mot de passe database pour XA

Synthèse

- Etudier les besoins en détails
- Impliquer la SSI, les partenaires
- Combiner différentes solutions
- OAM seul ne suffit pas
- OAM + SSL pour éviter le contournement du MCAUSER
- Migrer en version 8.0 et activer le CHLAUTH

Des questions ?

Page blanche intentionnellement