De la version 7.0 à la version 8.0 :

Sécurité Client MQ

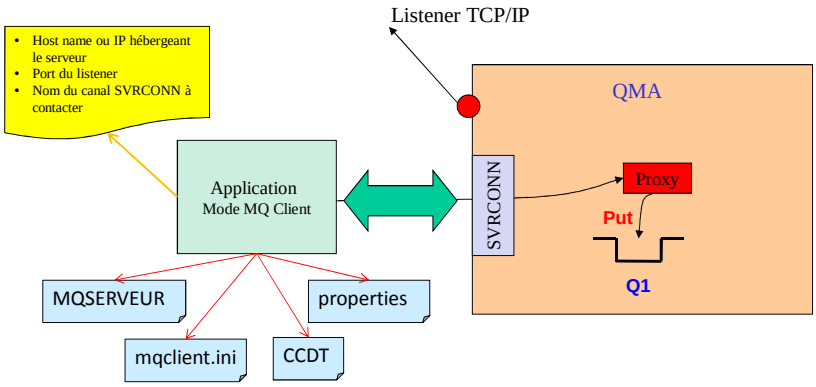
Luc-Michel Demey
LMD@demey-consulting.fr
+33 6 08 755 655

Version 1.01 – Septembre 2013

Objet

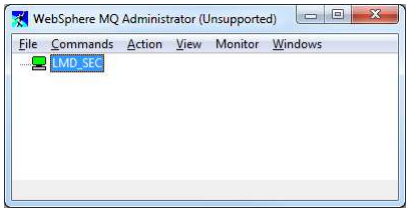
- Accès à un Queue Manager via un client MQ
  - Avec des outils d'administration (MO71, Explorateur MQ)
  - Avec une application client
  - Sous un compte « mqadmin » ou non
- Evolution de la situation entre la V7.0 et la V8.0

Rappel du mode client MQ



Accès au QM en version 7.0

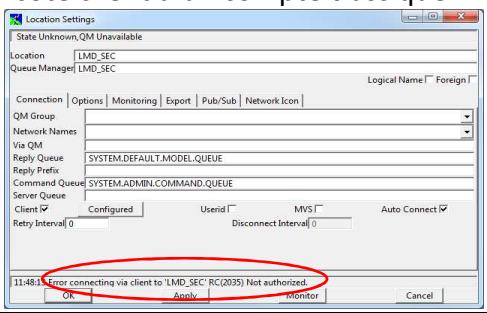
- WMQ 7.0.1.6, Queue Manager : LMD_SEC
- Canal SVRCONN : ADMIN, valeurs par défaut
- Utilisation coté client d'un compte « mqadmin » :



- Rappel : MCAUSER = « » → mode « open bar »

Accès au QM en version 7.0

- WMQ 7.0.1.6, Queue Manager : LMD_SEC
- Canal SVRCONN : ADMIN, valeurs par défaut
- Utilisation coté client d'un compte classique : KO



Accès au QM en version 7.0

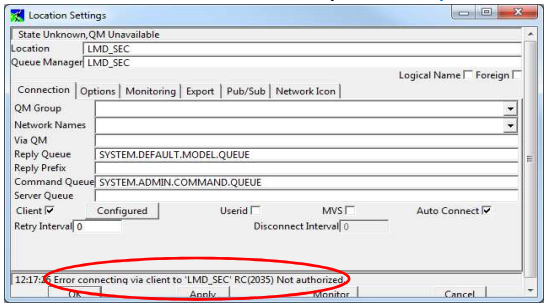
- Solution 1 :
  - Positionnement dans le canal SVRCONN d'un MCAUSER de type « mqadmin » : mqm, MUSR_MQADMIN
  - Mauvaise solution : (Open Bar)²
- Solution 2 :
  - Création d'un compte spécifique : mq_cli
  - N'appartenant pas à un groupe « mqadmin »
  - alter channel(ADMIN) chltype(SVRCONN) mcauser(mq_cli)
  - SETMQAUT sélectifs sur ce compte
  - Problème : protection de ce canal (SSL, exits, …)

Accès au QM en version 7.1 / 7.5

- Nouveauté 7.1 : CHLAUTH
  - « Firewall » sur les canaux
  - Règles par défaut pour les nouveaux QM
  - Comportement inchangé pour les QM migrés depuis la 7.0
  - Paramètre CHLAUTH au niveau du QM (Enabled / Disabled)

Accès au QM en version 7.1 / 7.5

- WMQ 7.5.0.2, Queue Manager : LMD_SEC
- Canal SVRCONN : ADMIN, valeurs par défaut
- Utilisation coté client d'un compte « mqadmin » : KO



Accès au QM en version 7.1 / 7.5

- AMQERR01.LOG :

AMQ9776: Le canal a été bloqué par l'ID utilisateur.

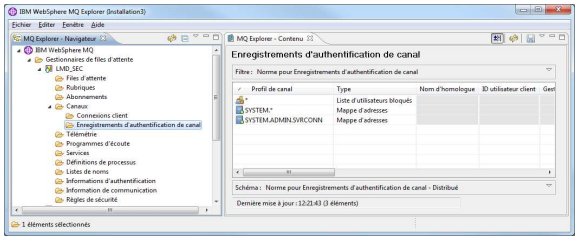
EXPLICATION :

Le canal entrant 'ADMIN' a été bloqué à partir de l'adresse '127.0.0.1' parce que les valeurs actives du canal étaient mappées sur un ID utilisateur qui devrait être bloqué. Les valeurs actives du canal étaient 'MCAUSER(lmd) CLNTUSER(lmd)'.

ACTION :

Prenez contact avec l'administrateur système qui examinera les enregistrements d'authentification de canal pour s'assurer que les paramètres corrects ont été configurés. Le commutateur ALTER QMGR CHLAUTH permet de contrôler si les enregistrements d'authentification de canal sont utilisés. La commande DISPLAY CHLAUTH peut être utilisée pour interroger les enregistrements d'authentification de canal.

Accès au QM en version 7.1 / 7.5



Trois règles appliquées par défaut pour les QM crées depuis MQ 7.1 :

dis chlauth(*)

CHLAUTH(SYSTEM.ADMIN.SVRCONN) TYPE(ADDRESSMAP) ADDRESS(*) USERSRC(CHANNEL)

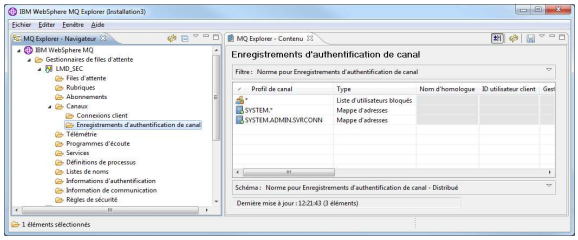
CHLAUTH(SYSTEM.*) TYPE(ADDRESSMAP) ADDRESS(*) USERSRC(NOACCESS)

CHLAUTH(*) TYPE(BLOCKUSER) USERLIST(*MQADMIN)

Pour le canal ADMIN, en l'absence de règle plus spécifique, la 3ième s'applique :

USERSRC(CHANNEL) → bloqué

Tentative d'utilisation du canal SYSTEM.ADMIN.SVRCONN



Trois règles appliquées par défaut pour les QM crées depuis MQ 7.1 :

dis chlauth(*)

CHLAUTH(SYSTEM.ADMIN.SVRCONN) TYPE(ADDRESSMAP) ADDRESS(*) USERSRC(CHANNEL)

CHLAUTH(SYSTEM.*) TYPE(ADDRESSMAP) ADDRESS(*) USERSRC(NOACCESS)

CHLAUTH(*) TYPE(BLOCKUSER) USERLIST(*MQADMIN)

Pour le canal SYSTEM.ADMIN.SVRCONN, la 1ère règle s'applique : USERSRC(CHANNEL),

puis la 3ième : TYPE(BLOCKUSER) USERLIST(*MQADMIN) → bloqué

Accès au QM en version 7.1 / 7.5

- Solution 1 :
  - Casser la sécurité CHLAUTH :

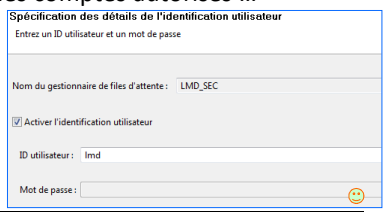
  ALTER QMGR CHLAUTH(DISABLED)
  - Retour au fonctionnement type 7.0
  - Impossible d'utiliser les CHLAUTH pour protéger les (autres) canaux

Accès au QM en version 7.1 / 7.5

- Solution 2 :
  - Pour le canal ADMIN , créer une règle « plus spécifique » que CHLAUTH(*) TYPE(BLOCKUSER) USERLIST(*MQADMIN)
  - Par exemple :
    SET CHLAUTH(ADMIN) TYPE(BLOCKUSER) USERLIST(toto)
- Résultat OK, mais :
  - Situation équivalente à MQ 7.0 et MCAUSER(‘ ‘) pour ce canal
  - Utilisation des CHLAUTH possible pour les autres canaux

Accès au QM en version 7.1 / 7.5

- Solution 3 :
  - Ajout d’une règle autorisant spécifiquement certains compte
- SET CHLAUTH('ADMIN') TYPE(USERMAP) CLNTUSER('lmd') + USERSRC(CHANNEL) ACTION(ADD)
- Résultat OK, mais :
  - Sécurité faible : si on spécifie un des comptes autorisés …
  - Mieux que les solutions 1 & 2



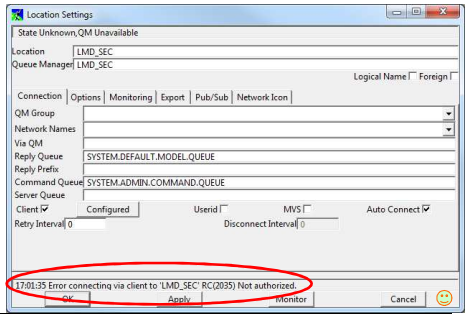
Accès au QM en version 7.1 / 7.5

- Solution 4 :
  - Affecter à chaque administrateur MQ une identité à travers un certificat SSL
  - Utiliser CHLAUTH pour contrôler l'accès au QM via un canal spécifique
  - Exemple :

```
SET CHLAUTH('ADMIN') TYPE(SSLPEERMAP) +
SSLPEER('OU="Admin MQ"') USERSRC(CHANNEL) ACTION(ADD)
```


Accès au QM en version 8.0

- Configuration identique à WMQ 7.5 :
  - DEFINE CHANNEL(ADMIN) CHLTYPE(SVRCONN) REPLACE
  - SET CHLAUTH('ADMIN') TYPE(BLOCKUSER) + USERLIST('toto') WARN(NO) ACTION(ADD)
- Résultat : KO



Analyse du AMQERR01.LOG

AMQ5540: L'application mqmonntp.exe n'a pas fourni d'ID utilisateur et de mot de passe

EXPLICATION :

Le gestionnaire de files d'attente est configuré pour nécessiter un ID utilisateur et un mot de passe, mais ni l'un ni l'autre n'a été fourni.

ACTION :

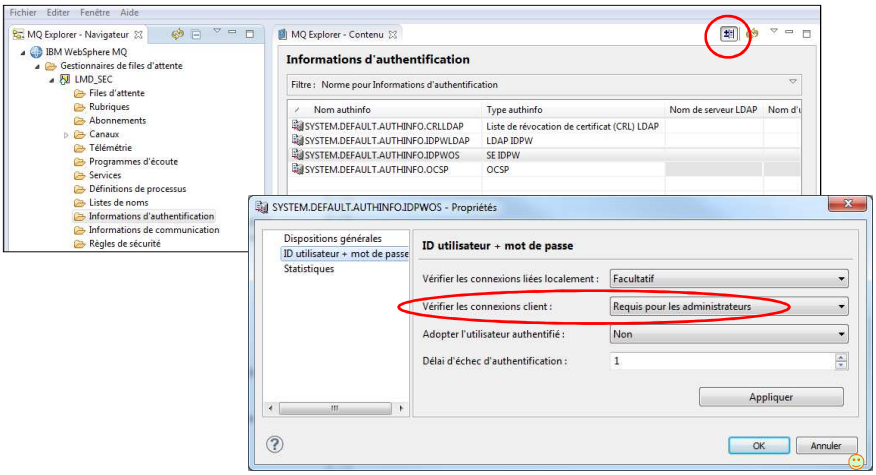
Assurez-vous que l'application fournit un ID utilisateur et un mot de passe valides ou spécifiez FACULTATIF pour la configuration du gestionnaire de files d'attente afin de permettre aux applications n'ayant pas fourni d'ID utilisateur et de mot de passe de se connecter.

AMQ5541: L'échec de la vérification de l'authentification a été provoqué par la configuration CONNAUTH CHCKCLNT(REQDADM) du gestionnaire de files d'attente.

EXPLICATION :

L'ID utilisateur 'lmd' et son mot de passe ont été vérifiés car l'ID utilisateur est privilégié et la configuration de l'autorité de connexion du gestionnaire de files d'attente (CONNAUTH) fait référence à un objet d'informations d'authentification (AUTHINFO) nommé 'SYSTEM.DEFAULT.AUTHINFO.IDPWOS' avec CHCKCLNT(REQDADM).

Informations d'authentification en V8



Accès au QM en version 8.0

- Solution 1 :
  - ALTER QMGR CONNAUTH(‘ ‘)
    - Retour au fonctionnement MQ 7.1/7.5
- Solution 2 :
  - ALTER AUTHINFO(SYSTEM.DEFAULT.AUTHINFO.IDPWOS) + AUTHTYPE(IDPWOS) CHCKCLNT(OPTIONAL)
  - REFRESH SECURITY TYPE(CONNAUTH)
    - Retour au fonctionnement MQ 7.1/7.5
    - Permet de spécifier un user / pass quand nécessaire

Accès au QM en version 8.0

- Solution 2 complète :
  - SET CHLAUTH('ADMIN') TYPE(BLOCKUSER) USERLIST('toto') WARN(NO) + ACTION(ADD)
  - SET CHLAUTH('ADMIN') TYPE(USERMAP) CLNTUSER('lmd') + USERSRC(CHANNEL) ACTION(ADD)
  - ALTER AUTHINFO(SYSTEM.DEFAULT.AUTHINFO.IDPWOS) + AUTHTYPE(IDPWOS) CHCKCLNT(OPTIONAL)
  - REFRESH SECURITY TYPE(CONNAUTH)

Conclusion

- Nouveaux comportements de la sécurité MQ
  - A partir de MQ 7.1
  - Si les QM sont créés / recréés
- Opportunité de mettre en place une vrai sécurité des canaux client :
  - CHLAUTH
  - AUTHINFO en 8.0
- Le SSL reste le moyen le plus simple et le plus fiable pour protéger les canaux

Page blanche intentionnellement