Channel Authentication Records

Guide MQ France

13/06/2017

Guillaume
GELB

Sommaire

- Concepts
- AUTHINFO
  - Check utilisateur
- Channel Authentication Records
  - Corps du CHLAUTH
  - Display CHLAUTH
  - Securisation SVRCONN
  - Resultat
  - Test de la configuration
  - Securisation channel RCVR
- Références à parcourir

Concepts

- *Authentication*
  - Vérification d'une identité
  - Peu utile sans contrôles d'accès postérieurs
  - CONNAUTH - AUTHINFO
- *Authorization*
  - Mise en place de contrôle d'accès
  - Peu utile sans vérification d'identité préalable
  - CHLAUTH

- En conclusion une association des 2 est primordiale pour sécuriser les accès

AUTHINFO (depuis la v8)

```
   1 : DIS QMGR CONNAUTH CHLAUTH
AMQ8408: Display Queue Manager details.
   QMNAME(CENTRAL)                         CHLAUTH(ENABLED)
   CONNAUTH(IS4F.LDAP)


 1 : DIS AUTHINFO(IS4F.LDAP)
AMQ8566: Display authentication information details.
   AUTHINFO(IS4F.LDAP)                     AUTHTYPE(IDPWLDAP)
   ADOPTCTX(YES)                           DESCR(Auth AD LDAP)
   CONNAME(xxx.xxx.xxx.xxx(389))           CHCKCLNT(REQUIRED)
   CHCKLOCL(OPTIONAL)                      CLASSGRP(group)
   CLASSUSR(user)                          FAILDLAY(1)
   FINDGRP(member)
   BASEDNG(OU=ouGROUPS,DC=xxx,DC=xxx,DC=xxx,DC=xxx)
   BASEDNU(OU=ouUSERS,DC=xxx,DC=xxx,DC=xxx,DC=xxx)
   LDAPUSER(CN=bindUser,OU=xxx,OU=xxx,DC=xxx,DC=xxx,DC=xxx,DC=xxx)
   LDAPPWD(********************************)
   SHORTUSR(sAMAccountName)                GRPFIELD(sAMAccountName)
   USRFIELD(sAMAccountName)                AUTHORMD(SEARCHGRP)
   NESTGRP(YES)                            SECCOMM(NO)
   ALTDATE(2017-01-03)                     ALTTIME(14.26.08)
```

AUTHINFO - suite

- Les nouveaux types
  - IDPWOS
    - Authentification utilisateur basée sur OS
  - IDPWLDAP
    - Authentification utilisateur basée sur annuaire
- Depuis 8.0.0.3 – CMDLEVEL > 802
  - AUTHENMD(OS|PAM) comme attribut de AUTHINFO(IDPWOS)
- Depuis 8.0.0.2 – CMDLEVEL > 801
  - AUTHORMD(OS|SEARCHGRP|SEARCHUSR) comme attribut de AUTHINFO(IDPWLDAP)

Check utilisateur

- CHCKCLNT
  - Authentification utilisateur en connexion client
  - REQUIRED
  - REQDADM
  - OPTIONAL
  - NONE
- CHCKLOCL
  - Authentification utilisateur en connexion bindings
  - REQUIRED
  - REQDADM
  - OPTIONAL
  - NONE

Channel Authentication Records

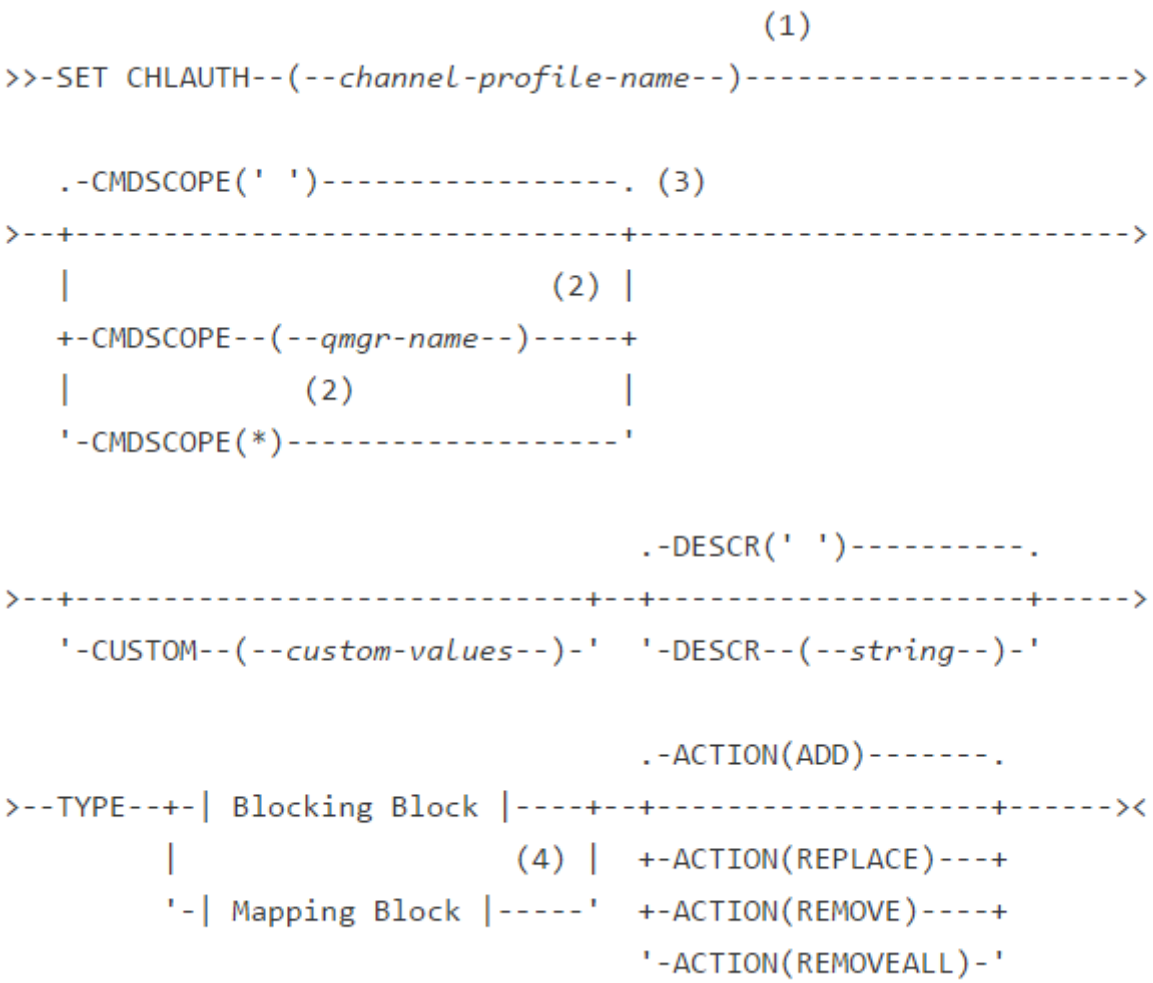
- Définitions par défaut

```
SET CHLAUTH(*) TYPE(BLOCKUSER) USERLIST(*MQADMIN) +
DESCR('Default rule to disallow privileged users')

SET CHLAUTH(SYSTEM.*) TYPE(ADDRESSMAP) USERSRC(NOACCESS) +
DESCR('Default rule to disable all SYSTEM channels')

SET CHLAUTH(SYSTEM.ADMIN.SVRCONN) TYPE(ADDRESSMAP) +
USERSRC(CHANNEL) ADDRESS(*) +
DESCR('Default rule to allow MQ Explorer access')
```

Result of 3 default CHLAUTH rules:
- NO ACCESS to all Channels by any MQ-admin* users
- NO ACCESS to all SYSTEM.* channels by all users
- ALLOW access to SYSTEM.ADMIN.SVRCONN (default channel used by WMQ Explorer)

*MQ-admin = special group which allows MQ adminstrative privileges, (ie: mqm group in Unix)

Corps du CHLAUTH



Display CHLAUTH

- 2 facons simples

dmpmqcfg -x chlauth -o 1line -m CENTRAL

```
********************************************************************************
* Queue manager name: CENTRAL
* Queue manager platform: UNIX
* Queue manager command level: (900/900)
* Command issued: dmpmqcfg -x chlauth -o 1line -m CENTRAL
********************************************************************************
SET CHLAUTH('SYSTEM.ADMIN.SVRCONN') TYPE(ADDRESSMAP) DESCR('Default rule to allow MQ Explorer access')
ADDRESS('*') USERSRC(CHANNEL) ACTION(REPLACE)
SET CHLAUTH('SYSTEM.*') TYPE(ADDRESSMAP) DESCR('Default rule to disable all SYSTEM channels')
ADDRESS('*') USERSRC(NOACCESS) ACTION(REPLACE)
SET CHLAUTH('*') TYPE(BLOCKUSER) DESCR('Default rule to disallow privileged users')
USERLIST('*MQADMIN') ACTION(REPLACE)
********************************************************************************
* Script ended on 2017-06-09   at 09.50.14
* Number of Inquiry commands issued: 3
* Number of Inquiry commands completed: 3
* Number of Inquiry responses processed: 6
* QueueManager count: 1
* ChlAuthRec count: 3
* AuthRec count: 2
* Number of objects/records: 6
********************************************************************************
```

Display CHLAUTH - suite

```
 1 : DIS CHLAUTH(*) ALL
AMQ8878: Display channel authentication record details.
   CHLAUTH(SYSTEM.ADMIN.SVRCONN)           TYPE(ADDRESSMAP)
   DESCR(Default rule to allow MQ Explorer access)
   CUSTOM( )                               ADDRESS(*)
   USERSRC(CHANNEL)                        CHCKCLNT(ASQMGR)
   ALTDATE(2016-12-30)                     ALTTIME(13.20.52)
AMQ8878: Display channel authentication record details.
   CHLAUTH(SYSTEM.*)                       TYPE(ADDRESSMAP)
   DESCR(Default rule to disable all SYSTEM channels)
   CUSTOM( )                               ADDRESS(*)
   USERSRC(NOACCESS)                       WARN(NO)
   ALTDATE(2016-12-30)                     ALTTIME(13.20.52)
AMQ8878: Display channel authentication record details.
   CHLAUTH(*)                              TYPE(BLOCKUSER)
   DESCR(Default rule to disallow privileged users)
   CUSTOM( )                               USERLIST(*MQADMIN)
   WARN(NO)                                ALTDATE(2016-12-30)
   ALTTIME(13.20.51)
```

Securisation SVRCONN

- Config SVRCONN en place

```
********************************************************************************
* Queue manager name: MQSSL1
* Queue manager platform: UNIX
* Queue manager command level: (900/900)
* Command issued: dmpmqcfg -x chlauth -o 1line -m MQSSL1 -n IS4FMID
********************************************************************************
SET CHLAUTH('IS4FMID') TYPE(USERMAP) CLNTUSER('eqm6d') MCAUSER('xqh2y') USERSRC(MAP) CHCKCLNT(REQUIRED)
ACTION(REPLACE)
SET CHLAUTH('IS4FMID') TYPE(USERMAP) CLNTUSER('mqm') MCAUSER('eqm6d') USERSRC(MAP) CHCKCLNT(REQUIRED)
ACTION(REPLACE)
```

- Export de la variable d'environnement

export MQSERVER='IS4FMID/TCP/localhost(1414)'

Resultat

```
[mqm@] /var/mqm > runmqsc -c -u eqm6d MQSSL1
5724-H72 (C) Copyright IBM Corp. 1994, 2016.
Enter password:
********
Starting MQSC for queue manager MQSSL1.


dis chs(IS4FMID) MCAUSER RAPPLTAG
     1 : dis chs(IS4FMID) MCAUSER RAPPLTAG
AMQ8417: Display Channel Status details.
   CHANNEL(IS4FMID)                        CHLTYPE(SVRCONN)
   CONNAME(127.0.0.1)                      CURRENT
   MCAUSER(eqm6d)                          RAPPLTAG(runmqsc)
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
dis chl(IS4FMID) all
     2 : dis chl(IS4FMID) all
AMQ8135: Not authorized.
quit
     3 : quit
3 command responses received.

[mqm@] /var/mqm > echo "dis chl(IS4FMID) MCAUSER" | runmqsc MQSSL1
5724-H72 (C) Copyright IBM Corp. 1994, 2016.
Starting MQSC for queue manager MQSSL1.


     1 : dis chl(IS4FMID) MCAUSER
AMQ8414: Display Channel details.
   CHANNEL(IS4FMID)                        CHLTYPE(SVRCONN)
   MCAUSER(no#body)
One MQSC command read.
No commands have a syntax error.
All valid MQSC commands were processed.
```

```
[mqm@] /var/mqm > dspmqaut -t qmgr -m MQSSL1 -p eqm6d
Entity eqm6d has the following authorizations for object MQSSL1:
        inq
        set
        connect
        altusr
        dlt
        chg
        dsp
        setid
        setall
        ctrl
        system

[mqm@] /var/mqm > dspmqaut -t chl -n 'IS4FMID' -m MQSSL1 -p eqm6d
Entity eqm6d has the following authorizations for object IS4FMID:




[@eqm6d]/globalhome2/eqm6d> runmqsc -c -u eqm6d MQSSL1
5724-H72 (C) Copyright IBM Corp. 1994, 2016.
Enter password:
********
Starting MQSC for queue manager MQSSL1.


dis chs(IS4FMID) MCAUSER RAPPLTAG
     1 : dis chs(IS4FMID) MCAUSER RAPPLTAG
AMQ8417: Display Channel Status details.
   CHANNEL(IS4FMID)                        CHLTYPE(SVRCONN)
   CONNAME(127.0.0.1)                      CURRENT
   MCAUSER(xqh2y)                          RAPPLTAG(runmqsc)
   STATUS(RUNNING)                         SUBSTATE( )
dis chl(IS4FMID) MCAUSER
     2 : dis chl(IS4FMID) MCAUSER
AMQ8414: Display Channel details.
   CHANNEL(IS4FMID)                        CHLTYPE(SVRCONN)
   MCAUSER(no#bdoy)
quit
     3 : quit
```

```
[mqm@] /var/mqm > dspmqaut -t qmgr -m MQSSL1 -p xqh2y
Entity xqh2y has the following authorizations for object MQSSL1:
        inq
        set
        connect
        altusr
        dlt
        chg
        dsp
        setid
        setall
        ctrl
        system

[mqm@] /var/mqm > dspmqaut -t chl -n 'IS4FMID' -m MQSSL1 -p xqh2y
Entity xqh2y has the following authorizations for object IS4FMID:
        dlt
        chg
        dsp
        ctrl
        ctrlx
```

Autre exemple par hostname

```
*SET CHLAUTH('BILWAS') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS) DESCR('Block all
IP for this channel') WARN(NO) ACTION(ADD)

*SET CHLAUTH('BILWAS') TYPE(ADDRESSMAP) ADDRESS('adresse1.is4f.lu') USERSRC(MAP)
MCAUSER('mqadmin') DESCR('Allow connection for adresse1') ACTION(ADD)

*SET CHLAUTH('BILWAS') TYPE(ADDRESSMAP) ADDRESS('adresse1.is4f.lu') USERSRC(MAP)
MCAUSER('mqadmin') DESCR('Allow connection for bilws05d') ACTION(ADD)
```

Test de la configuration

```
[mqm@] /var/mqm > echo "dis CHLAUTH(IS4FMID) MATCH(RUNCHECK) CLNTUSER('eqm6d') ADDRESS('127.0.0.1')" |
runmqsc MQSSL1
5724-H72 (C) Copyright IBM Corp. 1994, 2016.
Starting MQSC for queue manager MQSSL1.


     1 : dis CHLAUTH(IS4FMID) MATCH(RUNCHECK) CLNTUSER('eqm6d') ADDRESS('127.0.0.1')
AMQ8878: Display channel authentication record details.
   CHLAUTH(IS4FMID)                        TYPE(USERMAP)
   ADDRESS( )                              CLNTUSER(eqm6d)
   MCAUSER(xqh2y)                          CHCKCLNT(REQUIRED)
One MQSC command read.
No commands have a syntax error.
All valid MQSC commands were processed.

[mqm@] /var/mqm > echo "dis CHLAUTH(IS4FMID) MATCH(RUNCHECK) CLNTUSER('mqm') ADDRESS('127.0.0.1')" |
runmqsc MQSSL1
5724-H72 (C) Copyright IBM Corp. 1994, 2016.
Starting MQSC for queue manager MQSSL1.


     1 : dis CHLAUTH(IS4FMID) MATCH(RUNCHECK) CLNTUSER('mqm') ADDRESS('127.0.0.1')
AMQ8878: Display channel authentication record details.
   CHLAUTH(IS4FMID)                        TYPE(USERMAP)
   ADDRESS( )                              CLNTUSER(mqm)
   MCAUSER(eqm6d)                          CHCKCLNT(REQUIRED)
One MQSC command read.
No commands have a syntax error.
All valid MQSC commands were processed.
```

Securisation channel RCVR

- Possible mais peu utilisé
- Restriction sur le mapping block
- Restart de channel a effectuer

EXEMPLE :

```
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
DESCR('Back-stop rule')

# Then you could allow this channel to be started
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('192.168.1.134') USERSRC(MAP)
MCAUSER('mqapp') ACTION(ADD)

Another example would be to only allow the connection from a particular queue manager:
# Lock down all access:
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
DESCR('Back-stop rule')

# Then allow access from queue manager MYSVR2 and from a particular ipaddress:
SET CHLAUTH('TO.MYSVR1') TYPE(QMGRMAP) QMNAME('MYSVR2') USERSRC(MAP)
MCAUSER('mqapp') ADDRESS('192.168.1.134') ACTION(ADD)
```

Références à parcourir

- SG24-8069-00 | **Secure Messaging Scenarios with WebSphere MQ**
- IBM Techdoc: 7041997 (rev3) | **CHLAUTH Made Simple**