Channel Authentication Records

Bill Newcomb (newcomb@us.ibm.com)
MQSeries distributed support

November 7, 2012

Channel Authentication Records

- Channel authentication records were added to MQSeries version 7.1 to allow you to define rules about how inbound connections should be treated.

- Set rules to control how inbound connections are treated
  - Inbound Clients
  - Inbound QMgr to QMgr channels
  - Other rogue connections causing FDCs

Configuration and Administration

- Create rules using
  - MQSC: SET CHLAUTH
  - PCF
  - MQ Explorer GUI Wizard

Rules

Rules may be created to:

  - Allow a connection
  - Allow a connection and assign MCAUSER
  - Block a connection
  - Ban privileged access
  - Provide multiple positive or negative SSL Peer Name matching

- Rules can use the following identifying characteristics
  - IP Address
  - SSL/TLS Subject's Distinguished Name
  - Client asserted USERID
  - Remote queue manager name

Listener Blocking

- List of IP address patterns

  ```
  SET CHLAUTH(*) TYPE(BLOCKADDR)
  ADDRLIST('100.10.*','192.168.1.0')
  ```

- Not meant as replacement for IP firewall
  - Temporary blocking until firewall is updated
- Blocked before any data is read from the socket
- Avoiding a denial of service attack
- Network Pingers if blocked don't raise an alert

Channel Mapping

- Identifying attributes
    - Channel Name
    - SSL Peer Name pattern
    - Remote queue manager name
    - Client asserted user ID
    - IP address
- Mapping done prior to calling security exit

Out of the Box

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

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

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

- Ban privileged users on inbound channels
- Ban use of all SYSTEM channels except SYSTEM.ADMIN.SVRCONN
- Enabling switch ALTER QMGR CHLAUTH(ENABLED|DISABLED) different for migrated or new queue manager.

- Technote on Not Authorized errors and Channel Authentication Records

  http://www-01.ibm.com/support/docview.wss?uid=swg21577137

What happens if.. Display command

```
DISPLAY CHLAUTH(SYSTEM.ADMIN.SVRCONN)
match(runcheck) CLNTUSER('newcomb')
address(127.0.0.1)
```

```
AMQ8878: Display channel authentication record details.
   CHLAUTH(*)                              TYPE(BLOCKUSER)
   USERLIST(*MQADMIN)
```

How will this be used?

```
SET CHLAUTH(*) TYPE(ADDRESSMAP) ADDRESS(‘*’)
USERSRC(NOACCESS) WARN(YES)

SET CHLAUTH(BPCHL.*) TYPE(SSLPEERMAP) SSLPEER(‘O=Bank
of Shetland’) MCAUSER(BANK123)

SET CHLAUTH(BPCHL.*) TYPE(SSLPEERMAP) SSLPEER(‘O=Bank
of Orkney’) MCAUSER(BANK456)

SET CHLAUTH(SYSTEM.ADMIN.SVRCONN) TYPE(ADDRESSMAP)
ADDRESS(‘9.20.1-30.*’) MCAUSER(ADMUSER)

SET CHLAUTH(TO.CLUS.*) TYPE(QMGRMAP)
QMNAME(CLUSQM*) MCAUSER(CLUSUSR) ADDRESS(‘9.30.*’)
```

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at: http://www.ibm.com/software/websphere/support/supp_tech.html

- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at: http://www.ibm.com/developerworks/websphere/community/

- Join the Global WebSphere Community: http://www.websphereusergroup.org

- Access key product show-me demos and tutorials by visiting IBM® Education Assistant: http://www.ibm.com/software/info/education/assistant

- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically: http://www.ibm.com/software/websphere/support/d2w.html

- Sign up to receive weekly technical My Notifications emails: http://www.ibm.com/software/support/einfo.html

Connect with us!

1. **Get notified on upcoming webcasts**
   Send an e-mail to wsehelp@us.ibm.com with subject line “wste subscribe” to get a list of mailing lists and to subscribe
2. **Tell us what you want to learn**
   Send us suggestions for future topics or improvements about our webcasts to wsehelp@us.ibm.com
3. **Be connected!**
   Connect with us on Facebook
   Connect with us on Twitter

Questions and Answers