Analyzing MQ security with zSecure 2.1.1

Hans Schoone, Chief Architect zSecure & manager Netherlands Lab
September, 2014
Disclaimer

- IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM’s sole discretion.

- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.
Agenda

- MQ security basics in 6 pages
- CKFCOLL enhancements for MQ
- CARLa enhancements for MQ
- UI RE.Q – zSecure MQ User Interface
- MQ compliance controls
MQ Overview

- MQ Allows applications to store and retrieve messages.
- Messages are kept in Queues.
- Queues are managed by a Queue Manager (QMGR)
- QMGR runs in a subsystem.
- Communication with other MQ systems is managed by Channel Initiator (CHINIT)
MQ Queue Manager and Queue Sharing Group

- MQ Systems can be grouped using a Coupling Facility
- Group is called a Queue Sharing Group (QSG)
- Queues can be Shared or Local
- DB2 is used for backup of shared queues
Security of MQ on z/OS is determined by

- **MQ manager configuration settings** like `SCYCASE(UPPER|MIXED)`
- **Security switches** in SAF class `MQADMIN`
  - By default a security switch is on
  - Presence of *Queue Manager NO* switch profile turns it off
  - Presence of *Queue Sharing Group NO* switch profile turns it off
  - Presence of *Queue Manager YES* switch profile turns it on
- **MQ resource protection** (normal `SAF REQ=(FAST)AUTH use`)
  - SAF class *prefix* MQ or MX, depends on case sensitivity (SCYCASE)
  - SAF class *suffix* by resource type
    - CMD, CONN, PROC, NLIST, QUEUE, TOPIC
  - Class inactive same effect as *NO* switch for the resource type
  - Access level requested depends on command or resource options
  - RACF RACLST merging applies for member/group class pairs
MQ Security switches by SUBSYS

- Switches are defined in MQADMIN class
- Discrete profiles only!
- Shaded tests only if queue manager qmgr-name member of group qsg-name

```
Start

qmgr-name.NO.SUBSYS.SECURITY

<table>
<thead>
<tr>
<th>Present</th>
<th>Absent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absent</td>
<td>Present</td>
</tr>
</tbody>
</table>

No Subsys Security

<table>
<thead>
<tr>
<th>Absent</th>
</tr>
</thead>
</table>

qmgr-name.YES.SUBSYS.SECURITY

<table>
<thead>
<tr>
<th>Present</th>
<th>Absent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absent</td>
<td>Present</td>
</tr>
</tbody>
</table>

Security On

<table>
<thead>
<tr>
<th>Present</th>
<th>Absent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absent</td>
<td>Present</td>
</tr>
</tbody>
</table>
MQ QMGR/QSG-Level Security switches

- Only if queue manager `qmgr-name` is a member of sharing group `qsg-name`.
- Otherwise, use QMGR-level security.
- Determine HLQs of profiles:
  - If both QMGR and QSG level active, QMGR profiles are checked first.
  - Both inactive is invalid → MQ uses both.

![Diagram showing MQ QMGR/QSG-Level Security switches](image-url)
# MQ resource type switches

<table>
<thead>
<tr>
<th>Type of checking</th>
<th>Switch profile name</th>
<th>Override profile for a particular queue manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection security</td>
<td>hlq.NO.CONNECT.CHECKS</td>
<td>qmgr-name.YES.CONNECT.CHECKS</td>
</tr>
<tr>
<td>Queue security</td>
<td>hlq.NO.QUEUE.CHECKS</td>
<td>qmgr-name.YES.QUEUE.CHECKS</td>
</tr>
<tr>
<td>Process security</td>
<td>hlq.NO.PROCESS.CHECKS</td>
<td>qmgr-name.YES.PROCESS.CHECKS</td>
</tr>
<tr>
<td>Namelist security</td>
<td>hlq.NO.NLIST.CHECKS</td>
<td>qmgr-name.YES.NLIST.CHECKS</td>
</tr>
<tr>
<td>Context security</td>
<td>hlq.NO.CONTEXT.CHECKS</td>
<td>qmgr-name.YES.CONTEXT.CHECKS</td>
</tr>
<tr>
<td>Alternate user security</td>
<td>hlq.NO.ALTERNATE.USER.CHECKS</td>
<td>qmgr-name.YES.ALTERNATE.USER.CHECKS</td>
</tr>
<tr>
<td>Command security</td>
<td>hlq.NO.CMD.CHECKS</td>
<td>qmgr-name.YES.CMD.CHECKS</td>
</tr>
<tr>
<td>Command resource security</td>
<td>hlq.NO.CMD.RESC.CHECKS</td>
<td>qmgr-name.YES.CMD.RESC.CHECKS</td>
</tr>
<tr>
<td>Topic security</td>
<td>hlq.NO.TOPIC.CHECKS</td>
<td>qmgr-name.YES.TOPIC.CHECKS</td>
</tr>
</tbody>
</table>

*Note: Generic switch profiles such as hlq.NO.** are ignored*
MQ Data collection and reporting

- MQ QMGR
- In-Storage information
- CMD Input
- CMD Respons

- CKFREEZE Snapshot
- CKFCOLL
- CARLa
- CKRCARLA
- RACF DB
- Displays
- Reports
MQ Data collection – Required authorization

- Display commands to QMGR need **SAF authorization** for each QMGR and/or QSG (*details next page*)
- MQ data collection can be disabled with **MQ=NO**
- If insufficient access, data is not collected.
  - RACF **violation message** in
    - JOBLOG of QMGR
    - SYSLOG
    - Not in CKFCOLL job !!
- MQ connection fails from **reusable** address space.
  - Do not specify **REUSASID=YES** on C2POLICE STC when using Extended Monitoring for MQ
MQ Data collection – Required authorization

- Display commands to QMGR need authorization for each QMGR and/or QSG:

<table>
<thead>
<tr>
<th>Command Type</th>
<th>HLQ</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>MQCONN</td>
<td>&lt;hlq&gt;.BATCH</td>
<td>READ</td>
</tr>
<tr>
<td>MQCMDS</td>
<td>&lt;hlq&gt;.DISPLAY.CHANNEL</td>
<td>READ</td>
</tr>
<tr>
<td>MQCMDS</td>
<td>&lt;hlq&gt;.DISPLAY.CHINIT</td>
<td>READ</td>
</tr>
<tr>
<td>MQCMDS</td>
<td>&lt;hlq&gt;.DISPLAY.CONNPCF</td>
<td>READ</td>
</tr>
<tr>
<td>MQCMDS</td>
<td>&lt;hlq&gt;.DISPLAY.NAMELIST</td>
<td>READ</td>
</tr>
<tr>
<td>MQCMDS</td>
<td>&lt;hlq&gt;.DISPLAY.PROCESS</td>
<td>READ</td>
</tr>
<tr>
<td>MQCMDS</td>
<td>&lt;hlq&gt;.DISPLAY.QMGR</td>
<td>READ</td>
</tr>
<tr>
<td>MQCMDS</td>
<td>&lt;hlq&gt;.DISPLAY.QUEUE</td>
<td>READ</td>
</tr>
<tr>
<td>MQCMDS</td>
<td>&lt;hlq&gt;.DISPLAY.SYSTEM</td>
<td>READ</td>
</tr>
<tr>
<td>MQCMDS</td>
<td>&lt;hlq&gt;.DISPLAY.TOPIC</td>
<td>READ</td>
</tr>
<tr>
<td>MQQUEUE</td>
<td>&lt;hlq&gt;.CKFCOLL.COMMAND.REPLY.*</td>
<td>UPDATE</td>
</tr>
<tr>
<td>MQQUEUE</td>
<td>&lt;hlq&gt;.SYSTEM.COMMAND.INPUT</td>
<td>UPDATE</td>
</tr>
<tr>
<td>MQQUEUE</td>
<td>&lt;hlq&gt;.SYSTEM.COMMAND.REPLY.MODEL</td>
<td>UPDATE</td>
</tr>
</tbody>
</table>
MQ_* newlists with in total > 200 fields

- MQ_REGION 62 fields
- MQ_CHANNEL 21 fields
- MQ_CONNECT 22 fields
- MQ_INIT 12 fields
- MQ_NAMELIST 23 fields
- MQ_PROCESS 24 fields
- MQ_QUEUE 31 fields
- MQ_TOPIC 24 fields
RE.Q.R - MQ region overview display

zSecure Admin+Audit for RACF - MQ - Regions

Command ===>

Show MQ regions that fit all of the following criteria:
Jobname . . . . . . . . . . . . (jobname or filter)
Region userid . . . . . . . . . (userid or filter)
MQ QMGR name/subsystem . . (name or filter)
Complex . . . . . . . . . . . . . (complex or filter)
System . . . . . . . . . . . . . (system or filter)

Output/run options
- Show differences
- Print format
  Customize title
  Send as e-mail
  Background run / Full page form

MQ region display

Command ===>

All MQ region records current settings

<table>
<thead>
<tr>
<th>Jobname</th>
<th>Complex</th>
<th>System</th>
<th>MQID</th>
<th>CMDCCHAR</th>
<th>RegUser</th>
<th>MQ</th>
<th>QSG</th>
<th>Rau</th>
<th>DSG</th>
<th>name</th>
<th>DB2</th>
</tr>
</thead>
<tbody>
<tr>
<td>M71LMSTR</td>
<td>NM84</td>
<td>IP01</td>
<td>M71L</td>
<td>+M71L</td>
<td>MQUSER</td>
<td>710</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q7G1MSTR</td>
<td>LPAR400J</td>
<td>SYS</td>
<td>Q7G1</td>
<td>&gt;Q7G1</td>
<td>DCUSER</td>
<td>701</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q7G2MSTR</td>
<td>LPAR400J</td>
<td>SYS</td>
<td>Q7G2</td>
<td>&gt;Q7G2</td>
<td>DCUSER</td>
<td>701</td>
<td>Q7GG</td>
<td>Yes</td>
<td>D81GRP</td>
<td>D81</td>
<td></td>
</tr>
<tr>
<td>Q7G3MSTR</td>
<td>LPAR400J</td>
<td>SYS</td>
<td>Q7G3</td>
<td>&gt;Q7G3</td>
<td>DCUSER</td>
<td>701</td>
<td>Q7GG</td>
<td>Yes</td>
<td>D81GRP</td>
<td>D81</td>
<td></td>
</tr>
<tr>
<td>Q7G4MSTR</td>
<td>LPAR400J</td>
<td>SYS</td>
<td>Q7G4</td>
<td>&gt;Q7G4</td>
<td>DCUSER</td>
<td>701</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Q7G6MSTR</td>
<td>LPAR400J</td>
<td>SYS</td>
<td>Q7G6</td>
<td>&gt;Q7G6</td>
<td>DCUSER</td>
<td>710</td>
<td>Q7G2</td>
<td>Yes</td>
<td>DA1GRP</td>
<td>DA1</td>
<td></td>
</tr>
</tbody>
</table>

************************************************************************ Bottom of Data **************************************************************************
## RE.Q.R - MQ Region details

### MQ region display

<table>
<thead>
<tr>
<th>Command</th>
<th>All MQ region records</th>
<th>29 Jul 2014 23:45</th>
</tr>
</thead>
<tbody>
<tr>
<td>MQ region display</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Region identification | | |
|------------------------|------------------|
| Complex name           | IDFX             |
| System name            | AHJB             |
| MQ QMGR name/subsystem | CSQ7             |
| Job name               | CSQ7MSTR Job     |
| Step name              | CSQ7MSTR         |
| Command character      | %                |
| MQ region userid       | START2           |
| MQ QMGR release level  | 710              |

### Region settings

| Queue sharing group name      | RESLEVEL         |
| Data sharing group name       | DB2 attach n     |
| Active system zparm module    | CSQZPARM         |
| SMF accounting data           | No               |
| SMF statistics data           | No               |
| Alter date and time           | 2014-06-18 23:16:59 |

### Region security settings

| Security interval | 12 | Security timeout | 54 |
| Mixed case resource profiles | No |
| Subsystem security | Yes | CSQ7.NO.SUBSYS.SECURITY |

- **Empty for non-QSG region**
- **Startup Parameter module**
- **Use MQ/MX classes: Uppercase profiles**
RE.Q.R – MQ Region details, non-QSG

Region settings
Queue sharing group name
Data sharing group name
Active system zparm module
SMF accounting data
SMF status
Alternate user security
Region security
SMF status
Security timeout
Mixed case resource profiles
Subsystem security
Check QSG level security
Check QMGR level security
Queue security
Command security
Command resource security
Context security
Connection security
Alternate user security
Process security
Namelist security
Topic security

Switch profile not found → security active

Empty for non-QSG region

RESLEVEL auditing performed: Yes
DB2 attach name for connect: CSQZPARM
Default coded charset ID: 0
Switch profile not found → security active

Switch profile not found → security active

Switch profile not found → security active

Switch profile not found → security active

Switch profile not found → security active

Switch profile not found → security active

Switch profile not found → security active

Switch profile not found → security active

Switch profile not found → security active

Switch profile not found → security active

Switch profile not found → security active
RE.Q.R – MQ Region details, QSG member

- Switch profile not found → security active
- Invalid combination. MQ ignores them both
- Switch Profile not used if class inactive
RE.Q.R – MQ Region details, No Security

<table>
<thead>
<tr>
<th>Region settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue sharing group name</td>
<td>RESLEVEL auditing performed</td>
</tr>
<tr>
<td>Data sharing group name</td>
<td>DB2 attach name for connect</td>
</tr>
<tr>
<td>Active system zparm module</td>
<td>z parms encoded charset ID</td>
</tr>
<tr>
<td>SMF accounting data</td>
<td></td>
</tr>
<tr>
<td>SMF statistics data</td>
<td></td>
</tr>
<tr>
<td>Alter date and time</td>
<td>2014-07-27 10:36:53</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Region security settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security interval</td>
<td>12</td>
</tr>
<tr>
<td>Mixed case resource profiles</td>
<td>No</td>
</tr>
<tr>
<td>Subsystem security</td>
<td></td>
</tr>
<tr>
<td>Check QSG level security</td>
<td></td>
</tr>
<tr>
<td>Check QMGR level security</td>
<td></td>
</tr>
<tr>
<td>Queue security</td>
<td>Q7G1.NO.SUBSYS.SECURITY</td>
</tr>
<tr>
<td>Command security</td>
<td></td>
</tr>
<tr>
<td>Command resource security</td>
<td></td>
</tr>
<tr>
<td>Context security</td>
<td></td>
</tr>
<tr>
<td>Connection security</td>
<td></td>
</tr>
<tr>
<td>Alternate user security</td>
<td></td>
</tr>
<tr>
<td>Process security</td>
<td></td>
</tr>
<tr>
<td>Namelist security</td>
<td></td>
</tr>
<tr>
<td>Topic security</td>
<td></td>
</tr>
</tbody>
</table>
RE.Q.R - MQ Region detail display

Region user
Dflt userid for cmd security _

Id RI Name DfltGrp InstD
CSQOPR BCSC

Archive log settings
Archive log 1 dsn prefix CSQARC1.CSQ7
Archive log 2 dsn prefix CSQARC2.CSQ7

Default queue names
Dead letter queue name
Command queue
Transmission queue

Event settings
Generate authorization events
Generate bridge events
Generate inhibit events
Generate local events
Generate remote events
Generate start/stop events
Generate performance events
Generate configuration events
Generate command events
Generate channel events
Generate SSL events

SSL Options
SSL Revocation List Name MQключен
SSL Key Ring name MQKEYRING
Suite B-128 compliant crypto
Suite B-192 compliant crypto
SSL key negotiation count 64565

Sensitive queues
CSQ7.DEAD.QUEUE
SYSTEM.COMMAND.INPUT
CSQ7.DEFEXPRMIT.QUEUE

SAF key ring

Audit trail incomplete
incomplete
RE.Q.QU - MQ Queue Selection

Queue Selection Main panel

```
zSecure Admin+Audit for RACF - MQ - Queues

Command ===>

Show MQ queues that fit all of the following criteria:
Queue name ........... 
MQ QMGR name/subsystem _____ (name or filter)
Complex ............ _____ (complex or filter)
System ............. _____ (system or filter)

Advanced selection criteria
  - SAF/RACF settings
  - Further selection

Output/run options
  - 0. No summary
  - 1. Summary by region 2. Summary by queue
  - Show differences
  - Print format Customize title
    Background run / Full page form
```
RE.Q.QU - MQ Queue Selection

- Queue Selection SAF and Further selection panel

```
Show MQ queue records that fit all of the following criteria:
SAF resource class   ________ {class or filter}
SAF resource name...
(operator: <= > >= = <> \- )
```

```
Show MQ queues that fit all of the following criteria:
Remote queue name  
Remote QMGR name...
Creation date ... __ ________ {operator+yy:mm:dd hh:mm:ss}
Alter date ... ... __ ________ {operator+yy:mm:dd hh:mm:ss}
Select flag fields (Y/N/blank)
OR (AND or OR relationship)
  Queue is enabled for PUT
  Queue is enabled for GET

Information flow
Acces control
```
# RE.Q.QU - MQ Queue Overview display

## Overview display

<table>
<thead>
<tr>
<th>Command</th>
<th>MQ queue display</th>
<th>0 s elapsed, 0.0 s CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>MQ queue display</td>
<td>All MQ queue records</td>
<td>29 Jul 2014 23:45</td>
</tr>
</tbody>
</table>

### Queues used by CKFCOLL

- CICSA.INITQ
- CICSO1.INITQ
- CKFCOLL.COMMAND.REPLY.CD244841F90D1041
- CKFCOLL.COMMAND.REPLY.CD4C407EC0AC5B81
- CKFCOLL.COMMAND.REPLY.CD4C410572C21D01
- CKFCOLL.COMMAND.REPLY.CD538CFCC7077080
- CKFCOLL.COMMAND.REPLY.CD87143F83A56B51
- CMQM.REMOTE.QUEUE
- CMQM.XMIT.QUEUE
- CSQ4IVPG.MODEL
- CSQ4IVPG.TRIGGER
- CSQ4IVP1.MODEL
- CSQ4IVP1.MODEL
- CSQ4IVP1.TRIGGER
- CSQ4IVP1.TRIGGER
- CSQ7.DEAD.QUEUE
- CSQ7.DEFXMIT.QUEUE
- FAILURE
- M80E.DEAD.QUEUE
- M80E.DEFXMIT.QUEUE

Queues used by CKFCOLL
RE.Q.QU - MQ Queue detail display

- Detail display (non-QSG member)

**Properties**
- Queue is enabled for PUT: Yes
- Queue is enabled for GET: Yes

**RACF settings**
- Success audit access level: READ
- Failure audit access level: READ
- Warn only (do not protect): No

**Resource information**
**Resource location:**
- AHJB.MQ.CSQ7.QUEUE

**Class/Resource:**
- Used by MQ in RACROUTE
  - Class: MQQUEUE
  - Resource: CSQ7.SYSTEM.ADMIN.ACTIVITY.QUEUE

**Class/Profile:**
- Used by RACF
  - Class: MQQUEUE
  - Profile: CSQ7.SYSTEM.**

**User Access ACL id When**
- START2 ALTER START2

**The RACF ACL**: [Diagram showing RACF ACL details]
RE.Q.QU - MQ Queue detail display

- Detail display (non-QSG member, now with grouping class)

Properties
 Queue is enabled for PUT: Yes
 Queue is enabled for GET: Yes

RACF settings
 Success audit access level
 Failure audit access level
 Warn only (do not protect)

Resource information
 Resource location: AHJB.MQ.CSQ7.QUEUE

Result from RACLthumbnail merge

Class/Resource: Used by MQ in RACROUTE

Class/Profile: Used by RACF

The RACF ACL

<table>
<thead>
<tr>
<th>Class</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>MQQUEUE</td>
<td>CSQ7.SYSTEM.ADMIN.CHANNEL.EVENT</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>MQQUEUE</td>
<td>CSQ7.EVERYTHING</td>
</tr>
<tr>
<td>MQQUEUE</td>
<td>CSQ7.SYSTEM.ADMIN.CHANNEL.EVENT</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User</th>
<th>Access</th>
<th>ACL id</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td>- any -</td>
<td>READ</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>BCSCGB2</td>
<td>READ</td>
<td>BCSCGB2</td>
<td></td>
</tr>
<tr>
<td>START2</td>
<td>ALTER</td>
<td>START2</td>
<td></td>
</tr>
</tbody>
</table>
RE.Q.QU - MQ Queue detail display (3/3)

- Detail display (QSG member, QMGR/QSG level security)

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue is enabled for PUT</td>
<td>Yes</td>
</tr>
<tr>
<td>Queue is enabled for GET</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Create time: 2014-07-22 09.49.31
Alter time: 2014-07-22 09.49.31

RACF settings

- Success audit access level: Used by MQ in RACROUTE.
- Failure audit access level: READ
- Warn only (do not protect): Yes

Class/Profile: Used by MQ in RACROUTE. First match found is used

Class/Resource:

- MQQUEUE: M80E.CICS01.INITQ
- MQQUEUE: MQ1G.CICS01.INITQ

Class/Profile: Used by RACF

Class: MQQUEUE
Profile: M80E.**

User: any
Access: READ
ACL id: *

The RACF ACL
## RE.Q.CH - MQ Channel overview

<table>
<thead>
<tr>
<th>Channel</th>
<th>Type</th>
<th>MQID</th>
<th>Complex</th>
<th>Connect name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLIENT.TO.CSQ7</td>
<td>ClntConn</td>
<td>CSQ7</td>
<td>IDFX</td>
<td>CSQ7</td>
</tr>
<tr>
<td>CLIENT.TO.CSQ7</td>
<td>SrvConn</td>
<td>CSQ7</td>
<td>IDFX</td>
<td></td>
</tr>
<tr>
<td>CMQM.TO.CSQ7</td>
<td>Receiver</td>
<td>CSQ7</td>
<td>IDFX</td>
<td></td>
</tr>
<tr>
<td>CSQ7.TO.CMQM</td>
<td>Sender</td>
<td>CSQ7</td>
<td>IDFX</td>
<td>CMQM</td>
</tr>
<tr>
<td>SYSTEM.ADMIN.SVRCONN</td>
<td>SrvConn</td>
<td>CSQ7</td>
<td>IDFX</td>
<td></td>
</tr>
<tr>
<td>SYSTEM.DEF.CLNTCONN</td>
<td>ClntConn</td>
<td>CSQ7</td>
<td>IDFX</td>
<td></td>
</tr>
<tr>
<td>SYSTEM.DEF.CLUSSDR</td>
<td>ClusSdr</td>
<td>CSQ7</td>
<td>IDFX</td>
<td></td>
</tr>
<tr>
<td>SYSTEM.DEF.RECEIVER</td>
<td>Receiver</td>
<td>CSQ7</td>
<td>IDFX</td>
<td></td>
</tr>
<tr>
<td>SYSTEM.DEF.REQUESTER</td>
<td>Request</td>
<td>CSQ7</td>
<td>IDFX</td>
<td></td>
</tr>
<tr>
<td>SYSTEM.DEF.SENDER</td>
<td>Sender</td>
<td>CSQ7</td>
<td>IDFX</td>
<td></td>
</tr>
<tr>
<td>SYSTEM.DEF.SERVER</td>
<td>Server</td>
<td>CSQ7</td>
<td>IDFX</td>
<td></td>
</tr>
<tr>
<td>SYSTEM.DEF.SVRCONN</td>
<td>SrvConn</td>
<td>CSQ7</td>
<td>IDFX</td>
<td></td>
</tr>
<tr>
<td>TO.CSQ7</td>
<td>Receiver</td>
<td>CSQ7</td>
<td>IDFX</td>
<td></td>
</tr>
<tr>
<td>TO.WRKQM</td>
<td>Sender</td>
<td>CSQ7</td>
<td>IDFX</td>
<td>198.81.193.252(1416)</td>
</tr>
</tbody>
</table>
## RE.Q.CH - MQ Channel detail display

<table>
<thead>
<tr>
<th>Identification section</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System name</td>
<td>AHJB complex IDFX</td>
</tr>
<tr>
<td>QMGR name</td>
<td>CSQ7</td>
</tr>
<tr>
<td>Channel name</td>
<td>CLIENT.TO.CSQ7</td>
</tr>
<tr>
<td>Channel type</td>
<td>SrvConn</td>
</tr>
<tr>
<td>Description</td>
<td>Channel for serving client</td>
</tr>
<tr>
<td>Names of connections</td>
<td></td>
</tr>
<tr>
<td>Local address</td>
<td></td>
</tr>
<tr>
<td>Target QMGR name</td>
<td></td>
</tr>
<tr>
<td>Transmit queue name</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Properties</th>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport type</td>
<td>TCP Alter time</td>
</tr>
<tr>
<td>Userid for channel</td>
<td>2013-04-24 21.11.22</td>
</tr>
<tr>
<td>Password set for channel</td>
<td></td>
</tr>
<tr>
<td>SSL Client auth required</td>
<td>Yes</td>
</tr>
<tr>
<td>Cipher specification</td>
<td></td>
</tr>
<tr>
<td>Peer DN filter</td>
<td></td>
</tr>
</tbody>
</table>
RE.Q.CO - MQ Connection overview

- Connection identifier is too long for display

```
MQ connection display  Line 1 of 69
Command ===>   Scroll==> CSR
All MQ connection records   29 Jul 2014 23:45
  Connect identification     ExtConn in C_ID   Complex M
  C3E2D8C3C3E2D8F740404040404040CD4B26C07D670001 CS0CCS07   IDFX   C
  C3E2D8C3C3E2D8F740404040404040CD4B26C4561B0001 CS0CCS07   IDFX   C
  C3E2D8C3C3E2D8F740404040404040CD4B26C75060001 CS0CCS07   IDFX   C
  C3E2D8C3C3E2D8F740404040404040CD4B26C475150001 CS0CCS07   IDFX   C
  C3E2D8C3C3E2D8F740404040404040CD4B26C475230001 CS0CCS07   IDFX   C
  C3E2D8C3C3E2D8F740404040404040CD4B26C475310001 CS0CCS07   IDFX   C
  C3E2D8C3C3E2D8F740404040404040CD4B26C477140001 CS0CCS07   IDFX   C
  C3E2D8C3C3E2D8F740404040404040CD4B26C477430001 CS0CCS07   IDFX   C
  C3E2D8C3C3E2D8F740404040404040CD4B26C481B90001 CS0CCS07   IDFX   C
```

- Look at the details or use wide screen.

```
MQ connection display
Command ===>   MQ connect display
All MQ connect records
  Conn in C_ID     ExtConn in C_ID     Complex MQID  OType AType Application description
  C0D26C07D670001  CS0CCS07          ADCDPL CS07  Queue QMGR WebSphere MQ Storage Management
  C0D26C4561B0001  CS0CCS07          ADCDPL CS07  Queue QMGR WebSphere MQ Read Ahead Task
  C0D26C475150001  CS0CCS07          ADCDPL CS07  Queue QMGR WebSphere MQ Pageset Space Manager
  C0D26C475230001  CS0CCS07          ADCDPL CS07  Queue QMGR WebSphere MQ Pageset Space Manager
  C0D26C475310001  CS0CCS07          ADCDPL CS07  Queue QMGR WebSphere MQ Pageset Space Manager
  C0D26C477140001  CS0CCS07          ADCDPL CS07  Queue QMGR WebSphere MQ Pageset Space Manager
  C0D26C477430001  CS0CCS07          ADCDPL CS07  Queue QMGR WebSphere MQ Pageset Space Manager
```

- Use selection criteria on the input selection panel.
## RE.Q.CO - MQ Connection detail display

### Identification section
- **System name**: AHJB  
- **QMGR name**: CSQ7  
- **Unique connect identification**: C352D8C393F2D8F7404C9F000  
- **ExtConn part of Connect-ID**: CSQCCS07  
- **Conn part of Connect-ID**: CD539CFCC59F0001  
- **Object type**: QMGR

### Application settings
- **Application type**: Batch  
- **Application description**: CKFCOLL1  
- **Application identification**: CKFCOLL1  
- **Application ASID**: 001B

### Connect settings
- **Channel name**  
- **Connect name**  
- **Destination queue**  
- **Destination QMGR name**  
- **IMS PSB name**  
- **IMS PST region identifier**  
- **CICS transaction name**  
- **Userid for channel**: BCSCGB1

---

The readable part of the connect identifier

The timestamp part of the connect identifier

The Jobname

The RACF userid
### RE.Q.IN - MQ Channel Initiator detail display

![MQ channel init display](image)

**Identification section**

- **System name**: AHJB
- **QMGR name**: CSQ7
- **Complex**: IDFX
- **Channel initiator running**: Yes
- **TCP/IP stack name**: TCPIP

**TCP/IP listeners**

<table>
<thead>
<tr>
<th>Type</th>
<th>Stat</th>
<th>LU name</th>
<th>IPAddress</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>LU62</td>
<td>Stop</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>Run</td>
<td>*</td>
<td>192.168.178.120</td>
<td>1416</td>
</tr>
<tr>
<td>TCP</td>
<td>Run</td>
<td></td>
<td>192.168.178.120</td>
<td>12345</td>
</tr>
<tr>
<td>TCP</td>
<td>Run</td>
<td>IDFX</td>
<td></td>
<td>1010</td>
</tr>
</tbody>
</table>

**SNA listeners**

---

© 2014 IBM Corporation
### RE.Q.NL - MQ Namelist detail display

#### Identification section
- **System name**: AHJB, complex IDFX
- **Namelist name**: SYSTEM.QPUBSUB.QUEUE.NAMELIST
- **Namelist type**: Queue
- **QMGR name**: CSQ7
- **Description**: A list of queues for the queued Pub/Sub interface to monitor

#### Statistics
- **Number of names in list**: 2
- **Alter time**: 2013-04-24 21:11:22

#### Names
- `SYSTEM.BROKER.ADMIN.STREAM`
- `SYSTEM.BROKER.DEFAULT.STREAM`

#### RACF settings
- **Success audit access level**: READ
- **Failure audit access level**: READ
- **Warn only (do not protect)**: No

#### Resource information
- **Resource location**: AHJB.MQ.CSQ7.NAMELIST

#### Class Resource
- `_ MQNLIST` CSQ7.SYSTEM.QPUBSUB.QUEUE.NAMELIST
- **Class Profile**
- `_ MQNLIST` CSQ7.**
### RE.Q.PR - MQ Process overview

<table>
<thead>
<tr>
<th>Command</th>
<th>MQ process display</th>
</tr>
</thead>
<tbody>
<tr>
<td>All MQ process records</td>
<td>Complex</td>
</tr>
<tr>
<td>CQMH.SEND.PROCESS</td>
<td>ADCDPL</td>
</tr>
<tr>
<td>C004IVP1</td>
<td>ADCDPL</td>
</tr>
<tr>
<td>SYSTEM.DEFAULT.PROCESS</td>
<td>ADCDPL</td>
</tr>
</tbody>
</table>
RE.Q.PR - MQ Process detail display

**Process identification**
- **System name**: AHJB
- **QMGR name**: CSQ7
- **Process name**: CMQM.SEND.PROCESS
- **Description**: Process for sending messages to CMQM
- **Application identification**: CSQX START
- **Application type**: z/OS
- **Environment data**: CSQ7.TO.CMQM
- **User data**: CSQ7.TO.CMQM

**Statistics**
- **Alter time**: 2013-04-24 21:11:22

**RACF settings**
- **Success audit access level**: UPDATE
- **Failure audit access level**: READ
- **Warn only (do not protect)**: No

**Resource information**
- **Resource location**: AHJB.MQ.CSQ7.PROCESS
- **Class Resource**
  - MQPROC CSQ7.CMQM.SEND.PROCESS
- **Class Profile**
  - MQPROC CSQ7.CMQM.SEND.**

**User Access ACL id When**
- **Name DfltGrp**
### MQ Topic overview

**Command ==>**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Complex</th>
<th>MQID</th>
<th>Lcl</th>
<th>PEn</th>
<th>SEn</th>
<th>DLQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM.BASE.TOPIC</td>
<td>ADCDPL</td>
<td>CSQ?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SYSTEM.BROKER.ADMIN.STREAM</td>
<td>ADCDPL</td>
<td>CSQ?</td>
<td>Yes</td>
<td>Prn</td>
<td>Prn</td>
<td>Prn</td>
</tr>
<tr>
<td>SYSTEM.BROKER.DEFAULT.STREAM</td>
<td>ADCDPL</td>
<td>CSQ?</td>
<td>Yes</td>
<td>Prn</td>
<td>Prn</td>
<td>Prn</td>
</tr>
<tr>
<td>SYSTEM.BROKER.DEFAULT.SUBPOINT</td>
<td>ADCDPL</td>
<td>CSQ?</td>
<td>Yes</td>
<td>Prn</td>
<td>Prn</td>
<td>Prn</td>
</tr>
<tr>
<td>SYSTEM.DEFAULT.TOPIC</td>
<td>ADCDPL</td>
<td>CSQ?</td>
<td>Yes</td>
<td>Prn</td>
<td>Prn</td>
<td>Prn</td>
</tr>
<tr>
<td>TEST.TOPIC</td>
<td>ADCDPL</td>
<td>CSQ?</td>
<td>Yes</td>
<td>Prn</td>
<td>Prn</td>
<td>Prn</td>
</tr>
</tbody>
</table>

*Bottom of Display*
### RE.Q.TO - MQ Topic detail display

<table>
<thead>
<tr>
<th>Identification section</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System name</td>
<td>AHJB</td>
<td>complex IDFX</td>
</tr>
<tr>
<td>QMGR name</td>
<td>CSQ7</td>
<td></td>
</tr>
<tr>
<td>Topic name</td>
<td>SYSTEM.BASE.TOPIC</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Base topic for resolving attributes</td>
<td></td>
</tr>
</tbody>
</table>

### Settings
- **Topic is local to QMGR**: Yes
- **Publishing enabled**: Yes
- **Subscribing enabled**: Yes
- **Use dead letter queue**: Yes

### Merged security information

**Topic always using MX resource class**

#### Resource information
- **Resource location**: AHJB.MQ.CSQ7.TOPIC
- **Class**: MXTOPIC
- **Resource**: CSQ7.SYSTEM.BASE.TOPIC
- **Profile**: MXTOPIC
- **MX**: CSQ7.*

#### Security levels
- READ
- RACF universal access
- ALTER time
- Warn only (do not protect)

#### RACF ID * access
- RACF universal access
- READ
- ALTER time
- Warn only (do not protect)
MQ STIG compliance controls

- DISA STIG compliance controls about MQ:
  - ZWMQ0011 Channels strong encryption algorithms
  - ZWMQ0012 Channel SSL certificate specifies proper DN, keyring
  - ZWMQ0020 User timeout(15) and interval(5) parameters
  - ZWMQ0030 Started tasks properly defined
  - ZWMQ0049 MQ classes all active
  - ZWMQ0051 Switches must not deactivate security
    - except command resource
  - ZWMQ0052 Connections no blanket access, log all.
  - ZWMQ0053 Protect dead letters from being read by using alias queue
  - ZWMQ0054 Protect sensitive system queues
  - ZWMQ0055 Processes no blanket access
  - ZWMQ0056 Namelists no blanket access
  - ZWMQ0057 No blanket alternate user access
  - ZWMQ0058 No blanket context access
  - ZWMQ0059 Command access appropriate to roles
  - ZWMQ0060 No access for anybody on RESLEVEL resource
Questions