
VANGUARD
VIPBook:
A Practical Implementation
of IBM MQ on z/OS
Tony Nix, CISSP
Vanguard Professional Services
1

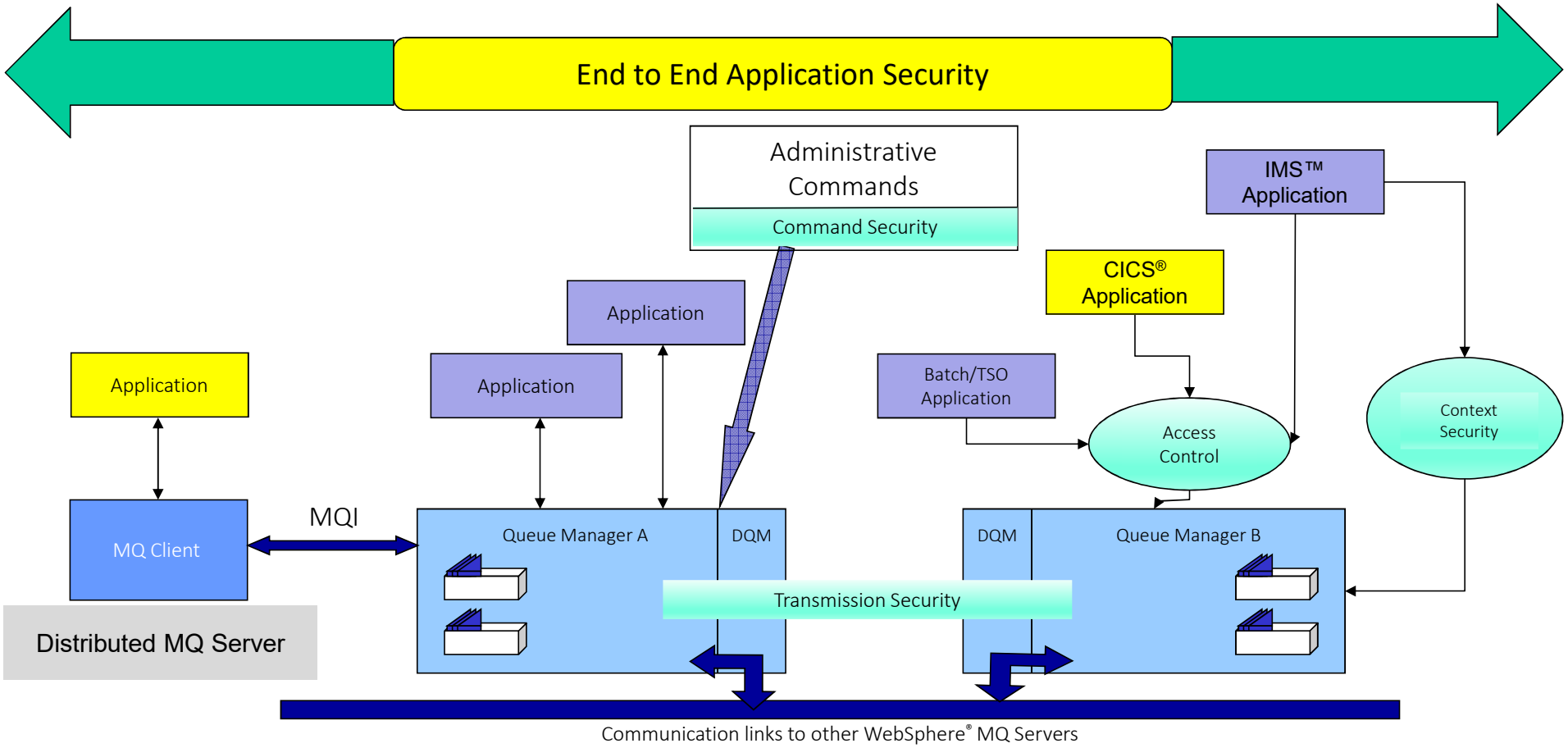
Agenda

- Determine what needs to be implemented
- Determine subjects and MQ objects to be protected
- Build the appropriate RACF® profiles
- Implement security definitions
- Practical example

Assumptions

- z/OS® only
- No distributed systems implemented
- MQSeries® and z/OS system programmers have installed libraries and set up system authorizations (e.g. APF, LINKLIST, etc.)

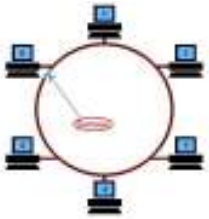
MQ Security – End to End



What do you need MQ to do?

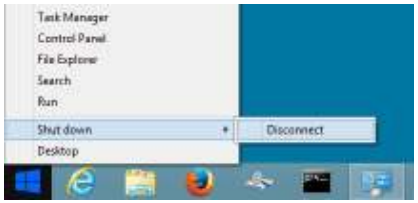
Queue Managers

Distributed Queues



Channels

Command Security



Queue Sharing Groups

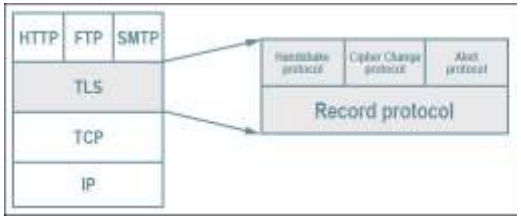
Connection Security

Administration

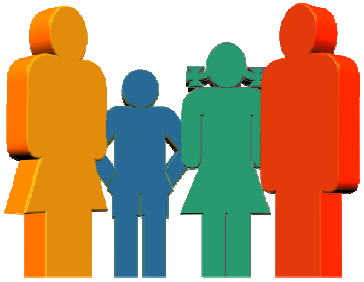
MQ Objects

What do you need MQ to do?

TLS



Alternate user



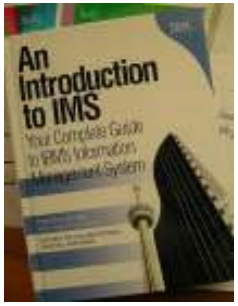
CICS

RESLEVEL

Timeouts

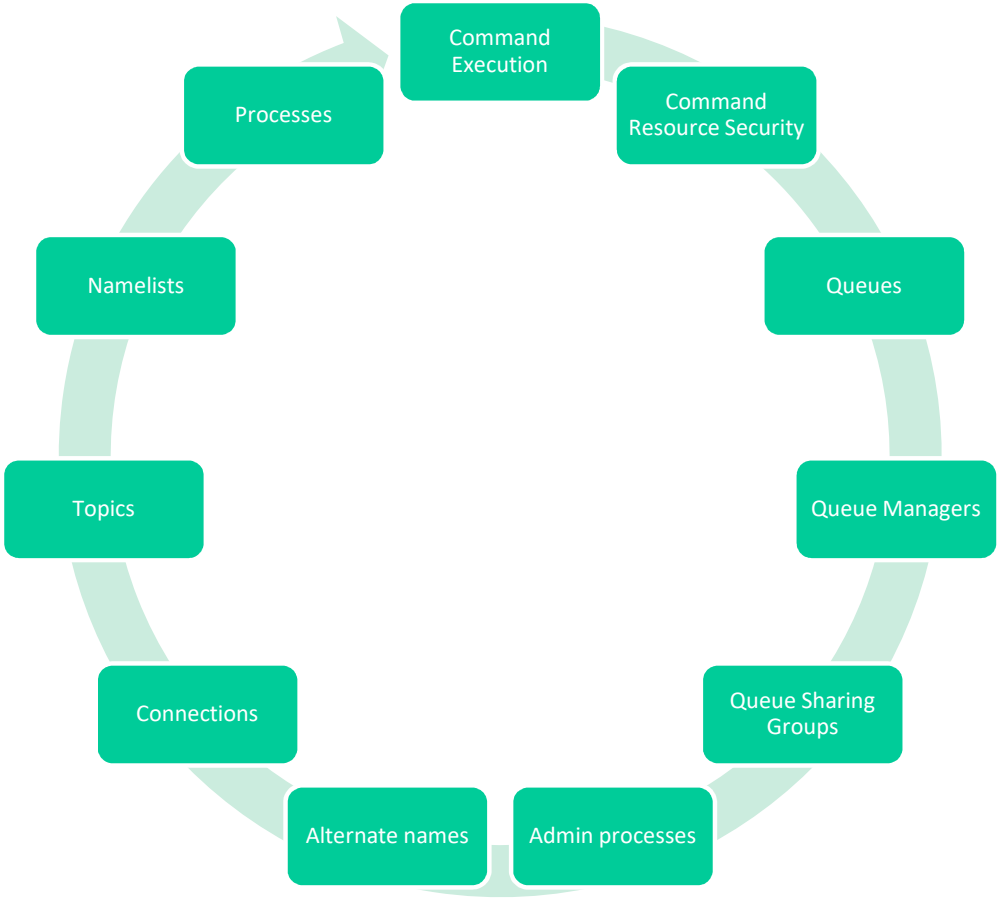
Auditing

IMS



DB2®

What objects need to be protected?



Key dataset libraries

Library Name	Library Purpose
SCSQAUTH	Main loadlib
CSQZPARM	Default system parms (assembled module in SCSQAUTH)
SCSQCICS	Loadlib for CICS DFHRPL concatenation
SCSQCLST	CLISTS
SCSQEXEC	REXX executables
SCSQINST	Install JCL
SCSQLOAD	Non-APF code, user exits, utilities, samples, instatllation verification, adapter stubs
SCSQMVR1	Distributed queuing
SCSQPROC	Sample JCL and default system initialization datasets; PROCLIB
Started Tasks	xxxxMSTR, xxxxCHIN
Custom commands	CSQ4INPX

Members of MQ samples in SCSQPROC

Table 147. Members of thlqual.SCSQPROC

Member name	Description
CSQ4INSG	System object definitions.
CSQ4INSA	System object and default rules for channel authentication.
CSQ4INSX	System object definitions.
CSQ4INSS	Customize and include this member if you are using queue-sharing groups.
CSQ4INSJ	Customize and include this member if you are using publish/subscribe using JMS.
CSQ4INSM	System object definitions for advanced message security.
CSQ4INSR	Customize and include this member if you are using WebSphere Application Server, or the queued publish/subscribe interface supported by the queued publish/subscribe daemon in IBM MQ V7 or later.
CSQ4DISP	CSQINP2 sample for displaying object definitions.
CSQ4INYC	Clustering definitions.
CSQ4INYD	Distributed queuing definitions.
CSQ4INYG	General definitions.
CSQ4INYR	Storage class definitions, using multiple page sets for the major classes of message.
CSQ4INYS	Storage class definitions, using one page set for each class of message.

Source: *Installing IBM MQ,* Version 9 Release 0, IBM® Corporation

Will CICS be connected to MQ?

- No user access to operator transactions CKTI and CKAM
- CICS adapter transaction administration (Category 2):
  - Define each with RESSEC(NO) and CMDSEC(NO)

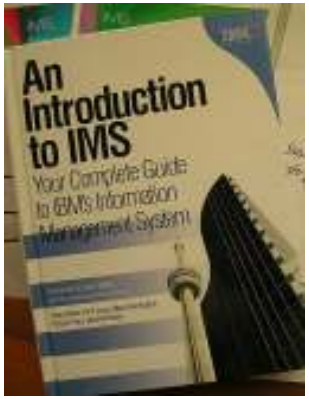
CKBM	CKDP	CKRT
CKCN	CKQC	CKSD
CKDL	CKRS	CKSQ

Will IMS be connected to MQ?

IMS Connection:
FACILITY / IMSXCF.xcfgname.mqxcfmname
QMGR id needs READ

QMGR id:
OPERCMDS for
MODIFY to any region

IMS Region



IMS application access control:
FACILITY / IMSXCF.xcfgname.imsxcfmname
Access depends user ID to check

/SECURE OTMA NON | CHECK | FULL | PROFILE

Do you need to use Queue Sharing Groups?

EXECUTE access required:

- QMGR id = MSTR STC userid
- CHINIT id = CHIN STC userid
- Utilities = whoever needs to submit batch

Do for each DB2 Data Sharing Group (QSG)

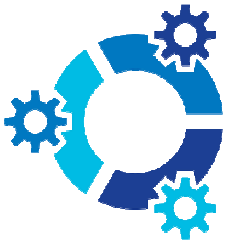
Sample Job Location in SCSQPROC	Job Purpose
CSQ45CSG	Create the storage group that is to be used for the IBM MQ database, table spaces, and tables.
CSQ45CDB	Create the database to be used by all queue managers that are connecting to this DB2 data-sharing group.
CSQ45CTS	Create the table spaces that contain the queue manager and channel initiator tables used for queue-sharing groups
CSQ45CTB	Create the 12 DB2 tables and associated indexes.
CSQ45BPL	Bind the DB2 plans for the queue manager, utilities, and channel initiator.
CSQ45GEX	Grants EXECUTE authority to plans for userids used by QMGR, utilities, and CHINIT.

Who Needs Access to the IBM MQ Objects

Security Administrators

MQ Administrators

Automation Software



Monitoring Software

Application Developers
Programmers

STC's:
xxxxMSTR
xxxxCHIN

Adapter

Operators

MQ Servers
(QMGR)

MQ Clients

Who should be on the project team?

Security Administrators

MQ Administrators

Major Application Developers and Programmers

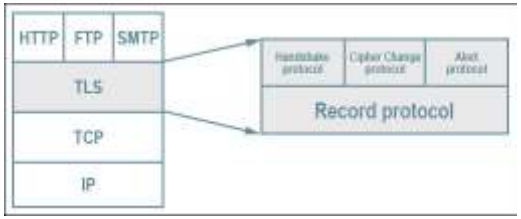
Auditing

Project Manager

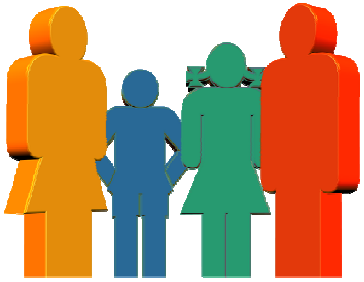
z/OS and MQ System Programmers
DB2 DBA's

What do you need MQ to do? (reminder)

TLS



Alternate user



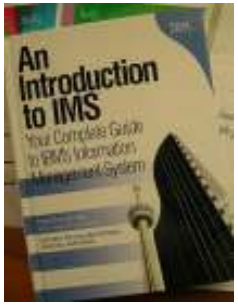
CICS

RESLEVEL

Timeouts

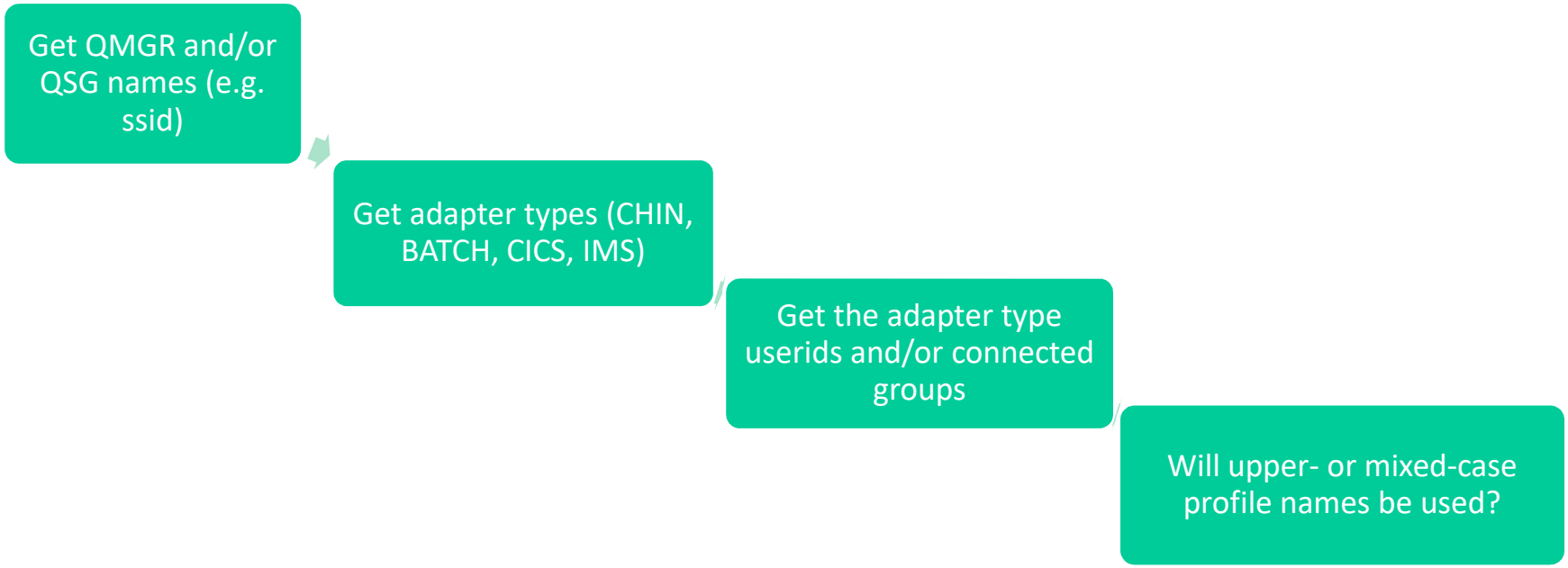
Auditing

IMS

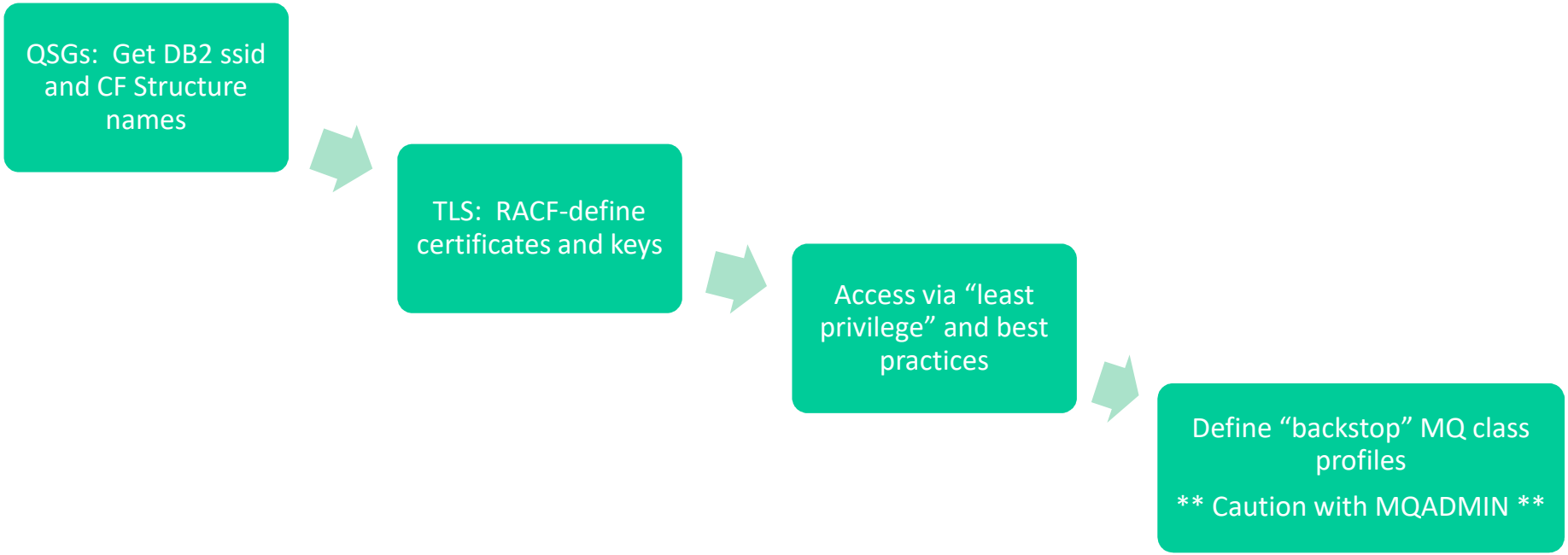


DB2

Before building commands (1/2)



Before building commands (2/2)



Configuration Concerns for Security Staff

Review current setup for CSQZPARM

Review samples in SCSQPROC

Setup data set security

Setup STARTED profiles for xxxxMSTR and xxxxCHIN
- READ: SCSQAUTH, SCSQANLX
- UPDATE: Page dsns, BSDS, CSQOUTX, CSQSNAP
- ALTER: Archives

Coupling Facility (QSGs)
- FACILITY: IXLSTR

Configuration Concerns for Security Staff

Setup resource security

- QMGR
- CHINIT
- MQ Administrators
- Application programmers
- Applications
- Dynamic queues: MQQUEUE: SYSTEM.CSQXCMD.**
- RESLEVEL
- ISPF panels via CSQOREXX and CSQUTIL utility

Define timeout values

- MQSC “ALTER SECURITY” command

Setup TLS

- Digital Certificates for each QMGR
- Key rings

What needs to be defined in RACF?

Activate generic profile checking

Define “backstop” profiles

UACC(NONE)

AUDIT(ALL(READ))

What needs to be defined in RACF?

TCPIP.DATA

TCPPARMS(TCPDATA)

DIGTCERT

CF: FACILITY / IXLSTR.structure

QSG: DB2 DSNR / DB2ssid.RRSAF

What needs to be defined in RACF?

Define local queues (MQ: DEFINE QLOCAL

- MQCMDS / ssid.DEFINE.QLOCAL: ALTER
- MQQUEUE / ssid.QUEUE.qname: ALTER

Delete local queues (MQ: DELETE QLOCAL)

- MQCMDS / ssid.DELETE.QLOCAL: ALTER
- MQQUEUE / ssid.QUEUE.qname: ALTER

Display local queue status (MQ: DISPLAY QLOCAL)

- MQCMDS / ssid.DISPLAY.QLOCAL: READ
- MQQUEUE: no access needed

Refresh internal MQ security environment (MQ: REFRESH SECURITY)

- MQCMDS / ssid.REFRESH.SECURITY: ALTER

Set system parameters (MQ: SET SYSTEM)

- MQCMDS / ssid.SET.SYSTEM: CONTROL

What needs to be defined in RACF?

MQADMIN/MXADMIN

- Resources used in commands
- Queues
- ssid.RESLEVEL
- Switch profiles
- Context security
- Alternate user IDs
- Publish/Subscribe

What needs to be defined in RACF?

MQCONN

- ssid.BATCH
- ssid.CICS
- ssid.IMS
- ssid.CHIN

What needs to be defined in RACF?

- Security checking on commands - all upper case - MQCMDS
- Command resource security
  - ssid.type.resname
- QMGRs:
  - Objects with QSGDISP(GROUP)
    - ALTER
    - DEFINE
    - DELETE
  - Channels with CHLDISP(SHARED)
    - START CHANNEL
    - STOP CHANNEL
- ssid.verb.objecttype
  - (e.g., CSQ1.ALTER.QLOCAL for ALTER QLOCAL command)

MQ Command Security

- Uses MQCMDS/ssid.verb.resource_type profiles

MQCMDS/ssid.verb.resource_type

DISPLAY commands	Require READ access
ARCHIVE, PING, RECOVER, RESET, RESOLVE, RESUME, START, STOP, SUSPEND commands	Require CONTROL access
ALTER, CLEAR, DEFINE, DELETE, REFRESH, RVERIFY commands	Require ALTER access

- Access required depends on the command verb
- Commands can be used as system control or transmitted to another QMGR for execution.

MQ Command Resource Security

- Uses ssid.objtype.local_resource_name profiles in the MQADMIN or MXADMIN classes

ssid.objtype.local_resource_name

PING, RESET, RESOLVE, START, STOP commands	Require CONTROL access
DEFINE, ALTER, DELETE commands	Require ALTER access

- For command object types of:
  - CHANNEL, QUEUE, NAMELIST, PROCESS, TOPIC
- Access required depends on the command verb

Refreshes

- The purpose of the refresh is to discard cached information and force a new RACF check.
- MQ caches previously-made security checks which need to be replaced upon RACF profile changes.
- Refresh needs to be issued by each QMGR

QMGR1

SETR RACLIST(classname) REFRESH
MQ REFRESH SECURITY(*)

QMGR2

SETR RACLIST(classname) REFRESH
MQ REFRESH SECURITY(*)

MQ Refresh Commands

- DISPLAY SECURITY(* | INTERVAL | SWITCHES | TIMEOUT)
  - TIMEOUT: userid signed out of QMGR and security info is discarded
  - INTERVAL: the number of minutes to check MQ to see if the userid can be timed out.

- REFRESH SECURITY(* | MQADMIN | MXADMIN | MQQUEUE | MXQUEUE | MQNLIST | MXNLIST | MQPROC | MXPROC)
  - Discards cached info; force new check against RACF – needs to be issued by each QMGR
  - No refresh required for MQCONN, MQCMDS, MQADMIN, or MXADMIN if RESLEVEL profile changed.

MQ Refresh Commands - continued

- REFRESH SECURITY TYPE(SSL) to refresh cached view of SSL Key Repository (without restarting channel initiator)
- RVERIFY SECURITY(userid1, userid2, …)
  - userid reverification; acts like an ACEE rebuild – re-authenticated
- ALTER SECURITY INTERVAL(nn) TIMEOUT(nn)
  - INTERVAL(nn) – MQ checks every nn minutes for activity
  - TIMEOUT(nn) – MQ active limit for inactivity

Typical process: Granted access to queue and need to refresh:
1. Go to MQ and issue: REFRESH SECURITY(MQQUEUE)
2. Go to RACF and issue: SETR RACLIST(MQQUEUE) REFRESH

Example commands

- %ssid DISPLAY CHANNEL(*) ALL
- %ssid DISPLAY LOG
- %ssid DISPLAY SECURITY ALL
- %ssid DISPLAY SYSTEM
- %ssid DISPLAY USAGE

- %ssid REFRESH SECURITY(*)
- %ssid START LISTENER
- Stopping MQ (stop QMGR last)
  - %ssid STOP CHINIT
  - %ssid STOP QMGR
- Starting MQ (start QMGR first)
  - %ssid START QMGR
  - %ssid START CHINIT

“Interesting” Messages

- CSQO015E - Command issued but no reply received
  - Symptom is that the command timed out for a MQ system reason
  - Problem caused by a “lower case” entry in the ISPF panels
  - All input (except object names if lower-case RACF classes not in use) must be in upper-case
- CSQY220I
  - Beginning with MQ v8, can suppress messages dynamically using SET SYSTEM EXCLMSG(xxxx). For example to suppress CSQY220I, issue SET SYSTEM EXCLMSG(Y220)

Troubleshooting Considerations

- Are switch profiles correctly set?
  - Active classes?
  - DISPLAY SECURITY to display switch status
  - Check MQADMIN switch profiles
  - Issue REFRESH SECURITY(MQADMIN)
- Has the RACF profile changed?
  - Is there a generic profile created during NOGENERIC or NOGENCMD?
  - Issue SETR REFRESH?
  - Issue MQ REFRESH SECURITY?

Troubleshooting Considerations

- Has the userid been changed?
  - New group connections?
  - MQ RVERIFY SECURITY(userid)
- RESLEVEL in use?
  - Check permitted users to bypass access checking
  - CICS: check RESSEC setting to verify userids to be checked.
  - Watch out for “best fit”; go with specific discrete
- QSGs?
  - Check profile consistency across different LPARs, different RACF databases, or whether RACGLIST is active.
  - Are appropriate switch profiles in use or in conflict between QMGR’s?
  - Is DB2 properly setup?
  - Is CF properly setup?

MQ ISPF panels

- Executes the MQ CSQUTIL program
- Functional access needed:
  - MQCONN / ssid.BATCH / READ
  - MQQUEUE / ssid.SYSTEM.COMMAND.INPUT / UPDATE
  - MQQUEUE / ssid.SYSTEM.COMMAND.REPLY.MODEL / UPDATE
  - MQQUEUE / ** / UPDATE (try to define specific MQQUEUE profiles)
  - MQCMDS / ssid.DISPLAY.** / READ
- Refresh security access
  - MQCMDS / ssid.REFRESH.** / ALTER
  - MQQUEUE / ssid.SYSTEM.CSQUTIL.** / UPDATE

STIG Requirements

- Add backstop profiles with UACC(NONE) and AUDIT(ALL(READ))
  - Take caution with MQADMIN
- Define specific resource profiles with UACC(NONE) and AUDIT(ALL(READ))
- Don’t use ID(*) or WARNING

```
ZWMQ0011 V-6958   Channel Definitions
ZWMQ0012 V-6980   Digital Certificates
ZWMQ0014 V-31561  Certified Name Filters
ZWMQ0020 V-3903   MQ Queue Manager Timeout
ZWMQ0030 V-3904   Started Tasks
ZWMQ0040 V-3905   Datasets
ZWMQ0049 V-6959   Related Resource Classes
ZWMQ0051 V-6960   MQ Security Switches
ZWMQ0052 V-6962   MQCONN Profiles
ZWMQ0053 V-6964   Dead Letter Queues
ZWMQ0054 V-6965   MQQUEUE Profiles
ZWMQ0055 V-6966   Process Resources
ZWMQ0056 V-6967   Namelist Resources
ZWMQ0057 V-6969   Alternate User Resources
ZWMQ0058 V-6971   MQADMIN CONTEXT Resources
ZWMQ0059 V-6973   Commands
ZWMQ0060 V-6975   MQADMIN RESLEVEL Resources
```

Practical Example

- Using MQ samples shipped with MQ.
- MQ Explorer or IBM File Manager can also be used.

- Get initial MQ access to define test queue
- Try to PUT a message without authority
  - See violation messages
- Get access; retry PUT
- PUT another message into test queue using File Manager
- GET all messages from test queue

Practical Example - continued

- Use sample COBOL PUT and GET programs and JCL
  - SCSQCOBS (source) and SCSQLOAD (loadlib)
    - CSQ4BVJ1 – GET
    - CSQ4BVK1 – PUT
  - SCSQPROC (proclib)
    - CSQBVJR – JCL to use for both
- Authorizations needed before testing:
  - MQ: DEFINE QLOCAL(TONYN.MAIN)
  - RDEF MQCMDS ssid.DEFINE.*
  - PE ssid.DEFINE.* CL(MQCMDS) ID(TONYN) ACC(A)
  - RDEF MQQUEUE ssid.TONYN.MAIN
  - PE ssid.TONYN.MAIN cl(MQQUEUE) ID(TONYN) ACC(N)
  - Refreshes:
    - SETR RACLIST(MQQUEUE) REFR
    - MQ REFRESH SECURITY(*)

Practical Example - continued

- Sub CSQ4PUT –
  - Not defined – got “MQRC_NOT_AUTHORIZED”, cc2, rc2035
    MQ Reference – says needs authorization for MQGET or MQPUT1
  - Output from CSQ4PUT job:

```
********************************** TOP OF DATA **************
==========================================
PARAMETERS PASSED :
   QMGR         - CSQ7
   QNAME        - TONYN.MAIN
   NUMMSGS      - 000000001
   PADCHAR      - *
   MSGLENGTH    - 000000020
   PERSISTENCE  - N
==========================================
MQCONN SUCCESSFUL
************************************************
* MQOPEN
* COMPLETION CODE : 000000002
* REASON CODE     : 000002035
************************************************
MQDISC SUCCESSFUL
********************************** BOTTOM OF DATA *************
```

Practical Example - continued

- SYSLOG ICH408I “standard” security violation message

```
ICH408I USER(TONYN   ) GROUP(VANGUARD) NAME(TONY NITWIT       )
  CSQ7.TONYN.MAIN CL(MQQUEUE )
  INSUFFICIENT ACCESS AUTHORITY
  ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

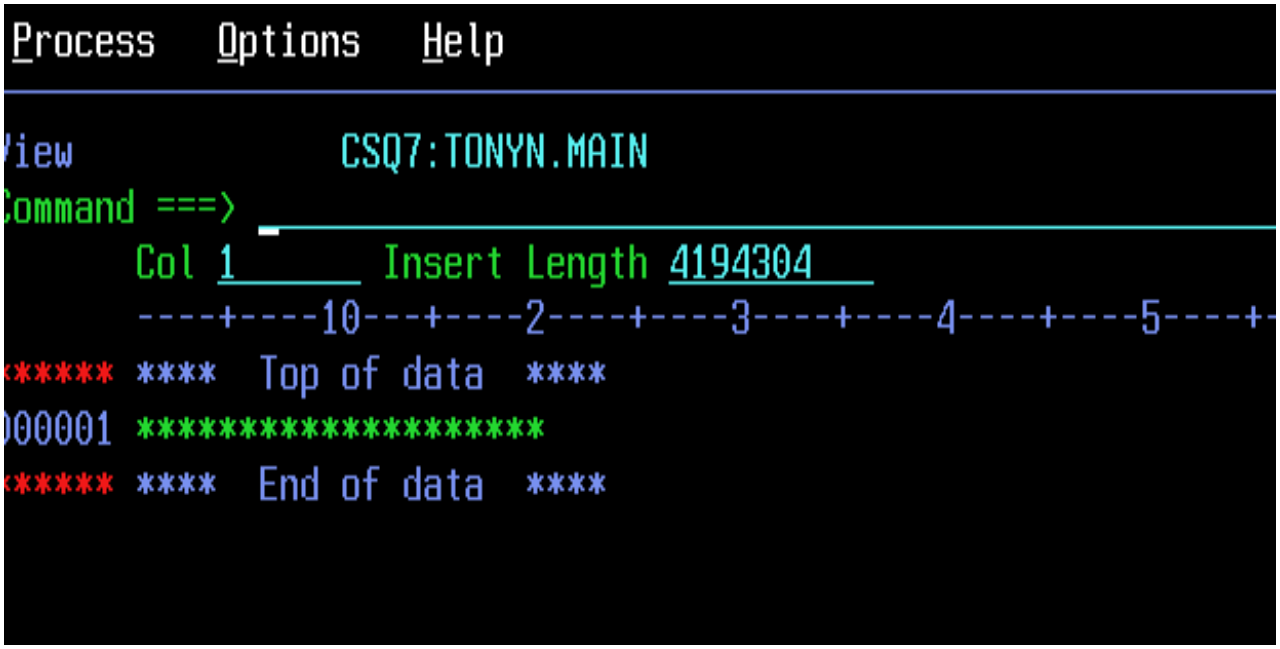
Practical Example - continued

- PE ssid.TONYN.MAIN CL(MQQUEUE) ID(TONYN) ACC(U)
- SETR RACLIST(MQQUEUE) REFR and MQ REFRESH SECURITY(*)
  Resubmit job – rc 0 - ☺
- Output from successful CSQ4PUT job:

```
********************************** TOP OF DATA **********************
==========================================
PARAMETERS PASSED :
   QMGR         - CSQ7
   QNAME        - TONYN.MAIN
   NUMMSGS      - 000000001
   PADCHAR      - *
   MSGLENGTH    - 000000020
   PERSISTENCE  - N
==========================================
MQCONN SUCCESSFUL
MQOPEN SUCCESSFUL
000000001 MESSAGES PUT TO QUEUE
MQCLOSE SUCCESSFUL
MQDISC SUCCESSFUL
********************************* BOTTOM OF DATA ********************
```

- No ICH408 messages like you'd expect for an unauthorized resource access.

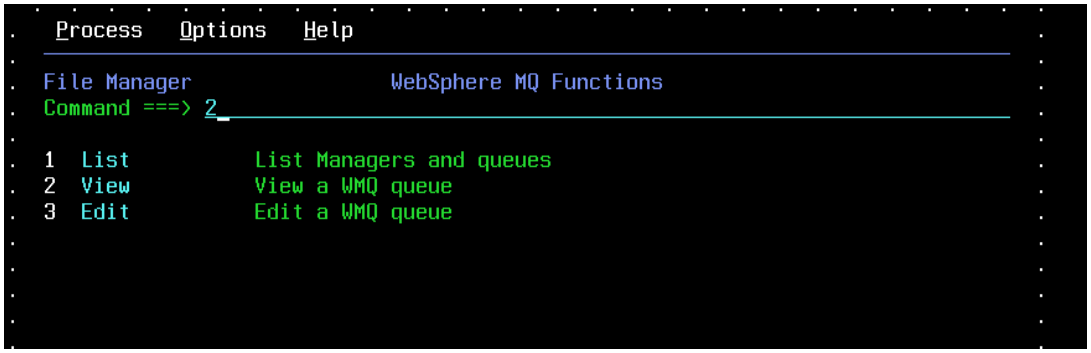
TONYN.MAIN after successful CSQ4PUT

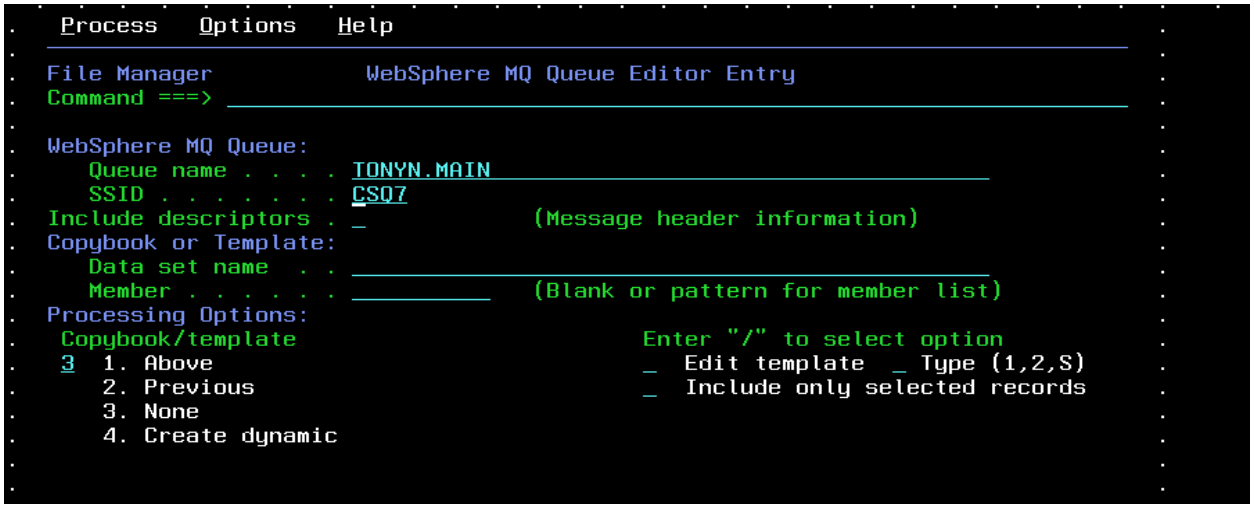


Practical Example - continued

- Put message in TONYN.MAIN using File Manager
  - Needed to change the logon proclib's ISPLLIB concatenation to include SCSQAUTH and SCSQLOAD
    - Test system: USER.PROCLIB(VSS22) to (VSS22TN)
  - RDEF MQADMIN
    - ssid.QUEUE.TONYN.*
      - CONTROL access: ssidCHIN
      - ALTER access: PSTEAM
    - ssid.CONTEXT.TONYN.*
      - CONTROL access: ssidCHIN, PSTEAM
  - RDEF MQQUEUE ssid.QUEUE.TONYN.* (CONTROL access needed)

PUT message in TONYN.MAIN





PUT message into TONYN.MAIN

```
 Process   Options   Help
 ------------------------------------------------------------------------
 File Manager              WebSphere MQ Functions
 Command ===> 3_

 1  List         List Managers and queues
 2  View         View a WMQ queue
 3  Edit         Edit a WMQ queue
```

```
 Process   Options   Help
 ------------------------------------------------------------------------
 File Manager           WebSphere MQ Queue Editor Entry
 Command ===>

 WebSphere MQ Queue:
    Queue name . . . . TONYN.MAIN
    SSID . . . . . . . CSQ7
 Include descriptors . _           (Message header information)
 Copybook or Template:
    Data set name  . . _____________________________________________
    Member . . . . . . ________    (Blank or pattern for member list)
 Processing Options:
  Copybook/template                      Enter "/" to select option
  3  1. Above                            _  Edit template   _ Type (1,2,S)
     2. Previous                         _  Include only selected records
     3. None                             _  Create audit trail
     4. Create dynamic
```

Results of PUT message

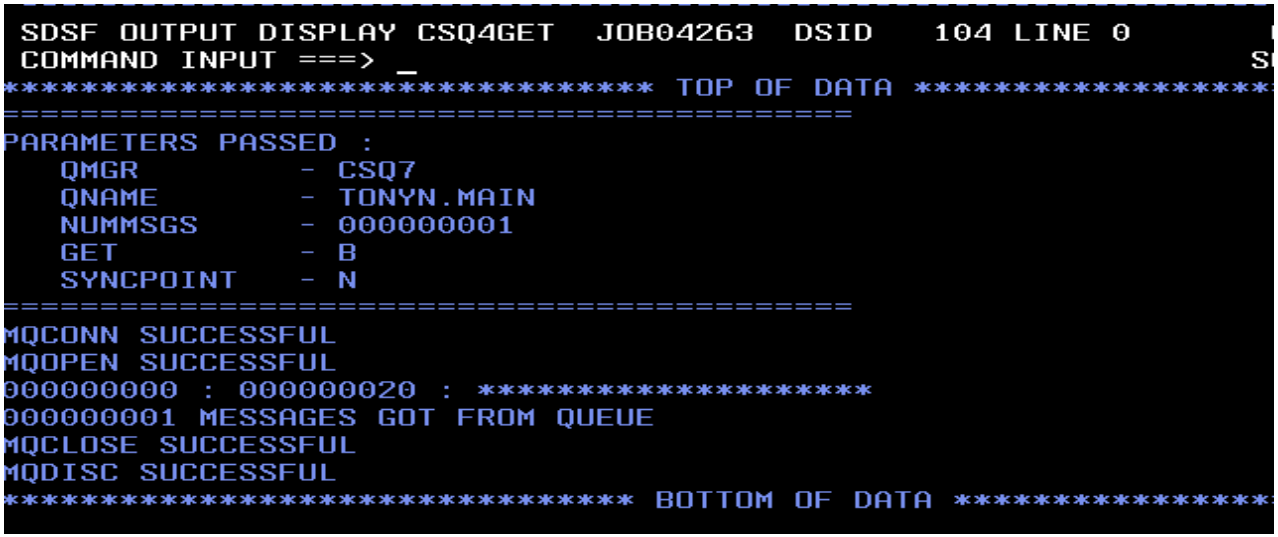
```
Process   Options   Help
Edit            CSQ7:TONYN.MAIN
Command ===>
      Col 1      Insert Length 4194304
      ----+----10---+----2----+----3----+----4----+----5----+----6----+----7----+-
****** ****  Top of data  ****
000001 ********************
000002 Hello World
000003 ** Added by Tony Nix **
****** ****  End of data  ****
```

```
Process   Options   Help
File Manager          WebSphere MQ Queue Editor Entry     2 record(s) updated
Command ===>

WebSphere MQ Queue:
   Queue name . . . . TONYN.MAIN
   SSID . . . . . . . CSQ7
Include descriptors .           (Message header information)
Copybook or Template:
```

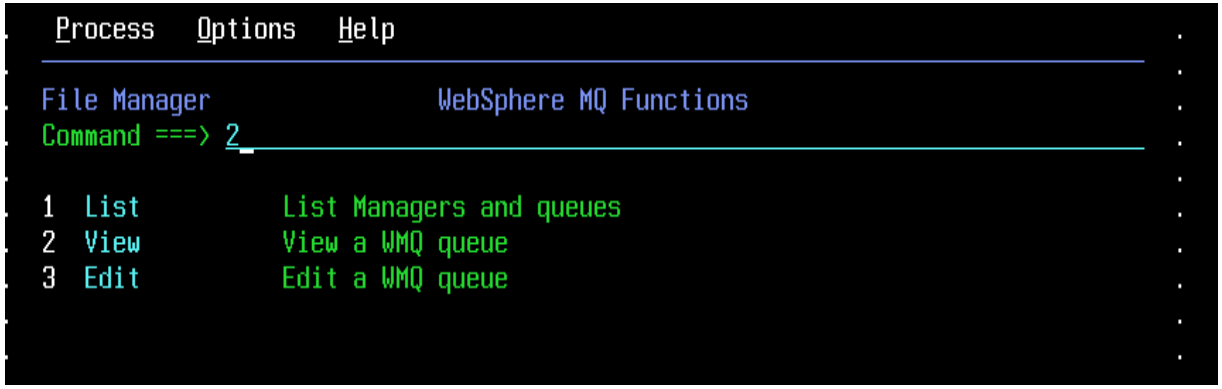
Practical Example - continued

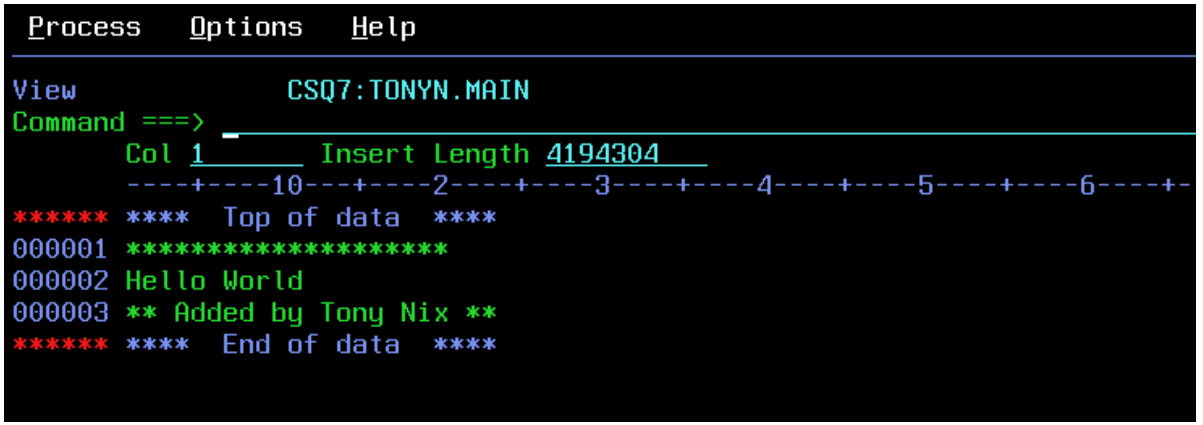
- Use CSQ4GET sample COBOL program to display content of TONYN.MAIN
  - PUT/GET SAMPLE PROGRAMS, CSQ4BVK1/CSQ4BVJ1



  - SCSQPROC(CSQ4BVJ1) proc:
    - //GETMSGS EXEC PGM=CSQ4BVJ1,REGION=1024K,
    - // PARM=('ssid,TONYN.MAIN,1,B,N')

Display the TONYN.MAIN queue





z/OS MQ ISPF options

- MQ Operations (e.g., ISPF option M.11)
  - Use for MQ Administration
  - Object manipulation
  - Commands
- File Manager / WebSphere MQ
  - File context and content
  - List queue managers
  - View a queue
  - Edit a queue
- MQ Explorer (Windows client)
  - Requires SSL/TLS
  - Define MQ objects
    - Local
    - Transmission
    - Channels

References

- SC34-6927-xx : WebSphere MQ for z/OS System Setup Guide
- WebSphere MQ Script (MQSC) Command Reference
- GC34-6926-xx: WebSphere MQ for z/OS, z/OS Concepts and Planning Guide
- IBM WebSphere MQ, Administering IBM WebSphere MQ
- IBM WebSphere MQ, Programming
- IBM WebSphere MQ, Installing IBM WebSphere MQ
- IBM WebSphere MQ, Product Overview
- IBM WebSphere MQ, Reference

Questions

- **How to Contact Us**
- Vanguard Integrity Professionals
- 6625 South Eastern Ave., Suite 100
- Las Vegas, NV 89119-3930

- Direct/International: (702) 794-0014
- Toll Free: (877) 794-0014
- **info@go2vanguard.com**

Legal Notice

Copyright

Trademarks

The following are trademarks of Vanguard Integrity Professionals – Nevada:

Vanguard Administrator
Vanguard Advisor
Vanguard Analyzer
Vanguard SecurityCenter
Vanguard Offline
Vanguard Cleanup
Vanguard PasswordReset
Vanguard Authenticator
Vanguard inCompliance
Vanguard IAM
Vanguard GRC
Vanguard QuickGen
Vanguard Active Alerts
Vanguard Configuration Manager
Vanguard Configuration Manager Enterprise Edition
Vanguard Policy Manager
Vanguard Enforcer
Vanguard ez/Token
Vanguard Tokenless Authenticator
Vanguard ez/PIV Card Authenticator
Vanguard ez/Integrator
Vanguard ez/SignOn
Vanguard ez/Password Synchronization
Vanguard Security Solutions
Vanguard Security & Compliance
Vanguard zSecurity University

Trademarks

The following are trademarks or registered trademarks of the International Business Machines Corporation:

CICS	IMS	S/390	z9
CICSPlex	MQSeries	System z	z10
DB2	MVS	System z9	z13
eServer	NetView	System z10	z/Architecture
IBM	OS/390	System/390	z/OS
IBM z	Parallel Sysplex	VTAM	z/VM
IBM z Systems	RACF	WebSphere	zEnterprise
IBM z13	RMF	z Systems	

Java and all Java-based trademarks are trademarks of Oracle and/or its affiliates.
UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

Other company, product, and service names may be trademarks or service marks of others.