Security for IBM MQ on z/OS Using RACF

Tony Nix
Phil Emrich
Vanguard Professional Services

BTB7
Legal Notice

Copyright
©2016 Vanguard Integrity Professionals, Inc. All Rights Reserved. You have a limited license to view these materials for your organization’s internal purposes. Any unauthorized reproduction, distribution, exhibition or use of these copyrighted materials is expressly prohibited.

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
**Legal Notice**

The following are trademarks or registered trademarks of the International Business Machines Corporation in the United States, other countries, or both:

<table>
<thead>
<tr>
<th>CICS</th>
<th>IMS</th>
<th>S/390</th>
<th>z9</th>
</tr>
</thead>
<tbody>
<tr>
<td>CICSPlex</td>
<td>MQSeries</td>
<td>System z</td>
<td>z10</td>
</tr>
<tr>
<td>DB2</td>
<td>MVS</td>
<td>System z9</td>
<td>z13</td>
</tr>
<tr>
<td>eServer</td>
<td>NetView</td>
<td>System z10</td>
<td>z/Architecture</td>
</tr>
<tr>
<td>IBM</td>
<td>OS/390</td>
<td>System/390</td>
<td>z/OS</td>
</tr>
<tr>
<td>IBM z</td>
<td>Parallel Sysplex</td>
<td>VTAM</td>
<td>z/VM</td>
</tr>
<tr>
<td>IBM z Systems</td>
<td>RACF</td>
<td>WebSphere</td>
<td>zEnterprise</td>
</tr>
<tr>
<td>IBM z13</td>
<td>RMF</td>
<td>z Systems</td>
<td></td>
</tr>
</tbody>
</table>

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.

CA ACF2 and CA Top Secret are trademarks or registered trademarks of CA Technologies.

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

• IBM® MQ is the current Product V9 Name formerly known as MQSeries® and WebSphere® MQ

• Messaging and MQ Overview
  – MQ Servers (Queue Managers)
  – MQ Clients
  – MQ Resources and Object Types

• Introduction to MQ Security

• MQ Security for z/OS®
  – Using RACF® as the Security Manager
Messaging Software Overview

• MQ Middleware Links “Islands of Computing”

• Characteristics of Messaging Middleware
  – A common interface across multiple platforms
  – Robust message delivery services
  – Asynchronous, time independent communication between applications
  – Application integration productivity
MQ Characteristics

- Business Process or Program orientation
- Simple common cross-platform API
- Easily imbedded to extend existing applications
- Reliable delivery of data messages
- Provides transactional messaging
  - Coordination of multiple messages
  - Coordination with other Resource Managers
- Support for more than 35 platform types
- (Reasonably) simple to administer
MQ Clients & Servers (Q Managers)

Distributed (non-z/OS) Platform

MQ Client

Application

Distributed MQ Server

MQI

Queue Manager A

DQM

Application

Communication links to other WebSphere MQ servers

z/OS MQ Server

IMS® Application

CICS® Application

Batch/TSO Application

Application

Platform

©2016 Vanguard Integrity Professionals, Inc.
MQ Queue Sharing Group (QSG)

Communication links to other WebSphere MQ servers
MQ Object Types

- Queues
  - Local, Remote, Alias, Model, Cluster, and more
- Queue Managers – WebSphere MQ Servers
- Channels
  - Transport
  - Sending Message Channel Agent (MCA)
  - Receiving Message Channel Agent (MCA)
- Namelists - a list of Queue (or other) names
- Process Definitions - for application triggering
- Topics – Publish / Subscribe Topics (since WMQ 7.0)
Types of Queues in MQ

• Application Queues
  – Local Queues
  – Remote Queues
  – Alias Queues
  – Model Queues

• System Queues
  – Transmission Queues
  – Dead-Letter Queue
  – Initiation Queues
  – Managed Queues
MQ Message: Header + Application Data

- **Header**
  - MQMD
  - Identity Context
    - UserIdentifier
    - AccountingToken
    - ApplIdentityData
  - Origin Context
    - PutApplType
    - PutApplName
    - PutDate
    - PutTime
    - ApplOriginData

Message “metadata”
MQ Application Example

MQ Application

MQOPEN
MQOPEN
MQGET
MQPUT

Application Message

Userid

Input Queue
Local only

Data Context

Output Queue
Local or Remote

Application Message

OBJECT HANDLE

Object Descriptor

Input Queue
Local only

MQOPEN
MQOPEN
Passing MQ Message Context

MQ Application

MQOPEN
MQGET
MQOPEN
MQPUT

MQMD + Application Message

Input Queue
Local only

Data Context

Output Queue
Local or Remote

Userid

MQOPEN
- (input queue): MQOO_SAVE_ALL_CONTEXT
- (output queue): MQOO_PASS.IDENTITY_CONTEXT
MQOO_PASS_ALL_CONTEXT

OBJECT HANDLE
Object Descriptor

©2016 Vanguard Integrity Professionals, Inc.
Publish / Subscribe MQ Message Model

- Publish / Subscribe refers to an application model in which the providers of information need have no awareness of the consumers
  - Providers of information are Publishers
  - Consumers of information are Subscribers
  - Information is Published to a Topic
  - Providers may publish to one or more Topics
  - Consumers may subscribe to one or more Topics
  - Providers and Consumers can be added or deleted dynamically, without disruption
Publish / Subscribe Scenarios

Few Publishers; Many Subscribers:  
Price Quotes, RACF-L, etc.

Many Publishers; Many Subscribers:  
Price Quotes, RACF-L, etc.

Many Publishers; Few Subscribers:  
Order Processing, etc.

Many Publishers; Many Subscribers:  
News, Sports Tickers, etc.
Publish-Subscribe Topic Tree / Topic Strings

Produce

Fruit
- Apples
- Bananas

Vegetables
- Onions
- Potatoes

Produce/Fruit/Apples
Produce/Fruit/Apples/Delicious/Yields
Produce/Fruit/Bananas/Prices
Produce/Vegetables/Onions
Produce/Vegetables/Potatoes
Publish / Subscribe Topic Objects

Topic Objects provide:

- Configuration Attributes
- A Control Point for Security
- Topic Tree Isolation

Starting MQSC for queue manager TST1.

```
DEFINE TOPIC(FRUIT)
    TOPICSTR('Produce/Fruit') DURSUB(NO)

DIS TOPIC(FRUIT)

AMQ8633: Display topic details,
    TOPIC( FRUIT )  TYPE( LOCAL )
    TOPICSTR( Produce/Fruit )
    CLUSTER( )
    PUB(ASPARENT)
    DEFPST(ASPARENT)
    DEFPRES(ASPARENT)
    ALTTIME(15.05.22)
    NPSMSGDLV(ASPARENT)
    SUBSCOPE(ASPARENT)
    WILDCARD(PASSTHRU)
    MNDURMDL()
```
MQ Configuration Controls

Communication links to other WebSphere MQ Servers
Host Operating System Level Controls

• MQ Application Change Control
  – Access Control for the MQ Link Libraries
    • dependent on the native security for the platform
    • resident only on CD for use on some platforms

• MQ Application Usage
  – Access Control for the Compiled/Linked Executable

• MQ commands
  (Commands for Queue Manager configuration and control)
  – Access Control for libraries containing the commands
    • dependent on the native security for the platform
    • resident only on CD for use on some platforms
MQ Security Mechanisms

- MQ Security Mechanisms
- MQ Client
- Application
- MQI
- Queue Manager A
- DQM
- Transmission Security
- Distributed MQ Server
- Queue Manager B
- IMS Application
- Batch/TSO Application
- Access Control
- Context Security
- Administrative Commands
- Command Security
- Communication links to other WebSphere MQ Servers

©2016 Vanguard Integrity Professionals, Inc.
MQ Security Services

- Access control for all MQ resources, except channels
- Provided by two equivalent mechanisms
- z/OS control is more granular than distributed MQ platforms
MQ Security Characteristics

- Controls are imposed by group and/or user
  - Mirroring operating system security services
  - All WebSphere MQ systems use **MQMD.UserIdentifier**
    - an identifier of up to 12 characters
    - first 12 of the 20 character domain-qualified userid for Windows

- Alternate/Surrogate userids may be specified
  - Only by authorized applications

- Access control for queues is imposed only on the application specified name
  - Remote Queues (resolve to Transmission Queues)
  - Alias Queues (resolve to other Queue Names)
Auditing MQ Security

• z/OS Queue Manager
  – Security Server (RACF) messages
  – SMF log records

• Distributed Queue Managers
  – All event messages written to SYSTEM.ADMIN.QMGR.EVENT queue
  – Four ‘Not Authorized’ event types:
    • MQCONN
    • MQOPEN / MQPUT1
    • MQCLOSE - For deletion of dynamic queues
    • MQ PCF commands
MQ Transmission Security Controls (Legacy)

- **Point-to-Point (QMgr MCA-to-QMgr MCA)**
  - Support enabled through exits in the MCA

- **Exits provided:**
  - Security Exit
    - Purpose: Authentication
  - Message Exit
    - Purpose: Message Integrity and Non-Repudiation
  - Send Exit
    - Purpose: Message Compression
  - Receive Exit
    - Purpose: Message Decompression
Transmission Security: Server-Server

1 - Transport security:
   - APPC Session Level Security and IPSEC (IP v6)
   - Transport Layer Security (TLS)

2 - MQSeries security
   - IBM Redbook example - SG24-5306
   - MQSeries Security: Example of using a Channel Security Exit, Encryption and Decryption
   - A MQ Channel Security Exit (search for “Channel security exit programs”)
Transmission Security: Client-Server

1 - Transport security
   • Same as the server to server environment

2 – WebSphere MQ security - security exits
   • Same as the server to server environment

3 – WebSphere MQ security - environment variables
MQ Transmission Security Controls

• SSL/TLS Authentication
  – Client / Server SSL/TLS Authentication
  – Certificate Naming relaxed in V8
  – Certificate Revocation Lists (CRL)
    • LDAP server based protocol
  – Online Certificate Status Protocol (OCSP)
    • Simplifies security certificate management
    • LDAP server not needed
    • Uses details provided in inbound certificate
    • Can be configured within QMGR or application

• CHLAUTH – Channel Authorization
  – Introduced in V7
  – Enhanced in V8 – rules can include subject and issuer DN’s
MQ Transmission Security Controls

• Certificate per Queue manager
  – Certificate Names Fixed by MQ in MQ V7
  – User defined Certificate Name in MQ V8
    • ALTER QMGR CERTLABEL(….)
    • REFRESH SECURITY TYPE(SSL)

• Certificate per Channel – MQ V8
  – A Single QMGR can support Certs from multiple CAs
    • ALTER CHANNEL(…) CHLTYPE(…) CERTLABEL(….)
  – Blank CERTLABEL to use QMGR Cert
  – Non-blank CERTABL required for TLS cypherspec
  – Uses Server Name Indication (SNI)
    • Extension to TLS Protocol
    • Provides Channel Name during Hand-Shake
MQ Security for z/OS

- Identification and authentication of users
  - Performed within the application environment
  - User identity is passed to MQ when MQCONN call used
  - User ID & password passed with MQCONNX call in V8
- MQ issues authorization calls for access to all MQ resources, except channels
  - MQ defines resource naming convention
  - RACF provides a set of resource classes in which profiles are defined to control access
MQ Authorization Processing

• MQ adapter connection authorization
  – Issued for the adapter’s address space User ID

<table>
<thead>
<tr>
<th>CICS region User ID</th>
<th>Batch USER=userid</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMS region User ID</td>
<td>Channel Initiator User ID</td>
</tr>
</tbody>
</table>

• MQ application resource authorization
  – Issues for 0, 1, or 2 User IDs
  – Determined by access to the MQADMIN/ssid.RESLEVEL profile

• MQ command authorization
  – MQ Command Resource Authorization
# RACF MQ Upper Case Profile Classes

<table>
<thead>
<tr>
<th>Member Classes</th>
<th>Group Classes</th>
<th>Contents</th>
<th>Class Posit</th>
</tr>
</thead>
<tbody>
<tr>
<td>MQCONN</td>
<td></td>
<td>Connection Type profiles</td>
<td>(82)</td>
</tr>
<tr>
<td>MQQUEUE</td>
<td>GMQQUEUE</td>
<td>Queue Name profiles</td>
<td>(77)</td>
</tr>
<tr>
<td>MQPROC</td>
<td>GMQPROC</td>
<td>Process Name profiles</td>
<td>(78)</td>
</tr>
<tr>
<td>MQNLIST</td>
<td>GMQNLIST</td>
<td>Namelist profiles</td>
<td>(79)</td>
</tr>
<tr>
<td>MQCMDS</td>
<td></td>
<td>MQ Command profiles</td>
<td>(81)</td>
</tr>
<tr>
<td>MQADMIN</td>
<td>GMQADMIN</td>
<td>Administrative Control profiles</td>
<td>(80)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alternate User profiles</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Context Control profiles</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RESLEVEL profiles</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Switch profiles</td>
<td></td>
</tr>
<tr>
<td>MQCHAN</td>
<td>GMQCHAN</td>
<td>Reserved</td>
<td>(58)</td>
</tr>
</tbody>
</table>
### RACF MQ Mixed Case Profile Classes

<table>
<thead>
<tr>
<th>Member Classes</th>
<th>Group Classes</th>
<th>Contents</th>
<th>Class Posit</th>
</tr>
</thead>
<tbody>
<tr>
<td>MXQUEUE</td>
<td>GMXQUEUE</td>
<td>Queue Name profiles</td>
<td>(583)</td>
</tr>
<tr>
<td>MXPROC</td>
<td>GMXPROC</td>
<td>Process Name profiles</td>
<td>(584)</td>
</tr>
<tr>
<td>MXNLIST</td>
<td>GMXNLIST</td>
<td>Namelist profiles</td>
<td>(585)</td>
</tr>
</tbody>
</table>
| MXADMIN        | GMXADMIN      | Administrative Control profiles    
|                |               | Alternate User profiles    
|                |               | Context Control profiles    
|                |               | RESLEVEL profiles    
|                |               | Switch profiles | (586) |
| MXTOPIC        | GMXTOPIC      | Reserved | (587) |

*Introduced in WebSphere MQ V7 for z/OS*
Selecting MQ Resource Classes

MQ Queue manager Attribute

- SCYCASE( UPPER | MIXED )

For a Queue Manager with SCYCASE(UPPER) will use classes:

- MQCONN, MQCMDS
- G/MQQUEUE, G/MQPROC, G/MQNLIST, G/MQADMIN
- G/MXTOPIC

For a Queue Manager with SCYCASE(MIXED) will use classes:

- MQCONN, MQCMDS
- G/MXQUEUE, G/MXPROC, G/MXNLIST, G/MXADMIN
- G/MXTOPIC
Selecting MQ Resource Classes

MQ Queue manager Attribute

• SCYCASE( UPPER | MIXED )

For a Queue Manager with SCYCASE(UPPER) will use classes:

• G/MQQUEUE, G/MQPROC, G/MQNLIST, G/MQADMIN

For a Queue Manager with SCYCASE(MIXED) will use classes:

• G/MXQUEUE, G/MXPROC, G/MXNLIST, G/MXADMIN

MQCONN, MQCMDS, G/MXTOPIC
MQ Mixed Case Profile Names

• The 'resource_name' portion of the profile name may be “mixed case” with SCYCASE(MIXED)

• MXADMIN
  – ssid.CONTEXT.resource_name
  – ssid.object_type.resource_name
    • Object_types: QUEUE, NAMELIST, PROCESS, TOPIC

• MXQUEUE, MXPROC, and MXNLIST
  – ssid.resource_name

• MXTOPIC
  – ssid.PUBLISH.resource_name
  – ssid.SUBSCRIBE.resource_name
MQ Connection Authorization

When MQCONN / MQCONNX call is issued

• Uses profiles defined in the MQCONN class
• MQ adapter user ID requires READ access
• Profile naming convention is:
  Qmgr_ID.adapter_type (e.g., QM19.CICS)

• Adapter types:
  – BATCH - for Batch or TSO applications
  – CICS - for CICS transactions
  – IMS - for IMS transactions
  – CHIN - for Channel Initiator programs
Authorization for API Resource Security

• MQ adapter user ID access determined by MQADMIN/ssid.RESLEVEL

• Authorization processing may be:
  – bypassed
  – performed only for the MQ adapter user ID
  – performed for more than one userid’s authority

• An ssid.RESLEVEL profile can be used for each Queue manager
  – NONE or no profile: two security checks
  – READ or UPDATE: one security check (generally)
  – CONTROL or ALTER: bypass API security
RESLEVEL Profile Considerations

• Checks against ssid.RESLEVEL profile are performed only at connection
  – Changes in profile access will only become effective on the next connection between an adapter and a Queue Manager

• A generic profile covering ‘ssid.RESLEVEL’ could cause some or all API Security to be bypassed
  – Recommendation: define a ‘discrete’ ssid.RESLEVEL profile for each queue manager

• If the adapter userid is defined as TRUSTED or PRIVILEGED all API Security is bypassed

• If WARNING is in effect for the profile, all API Security is bypassed, with no warning messages
## User IDs for API Resource Security

<table>
<thead>
<tr>
<th>User IDs</th>
<th>Adapter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch</td>
<td>Address space User ID</td>
</tr>
<tr>
<td>TSO</td>
<td>TSO User ID</td>
</tr>
<tr>
<td>CICS</td>
<td>CICS region address space User ID</td>
</tr>
<tr>
<td></td>
<td>Transaction User ID</td>
</tr>
<tr>
<td>IMS</td>
<td>IMS region address space User ID</td>
</tr>
<tr>
<td></td>
<td>“Second” User ID</td>
</tr>
<tr>
<td>Channel Initiator (Mover)</td>
<td>Channel User ID</td>
</tr>
<tr>
<td></td>
<td>MCAUSER</td>
</tr>
<tr>
<td>IGQ</td>
<td>Inter-Group Queueing User ID</td>
</tr>
<tr>
<td></td>
<td>Sending QMGR User ID</td>
</tr>
</tbody>
</table>
MQ API Resource Authorization

• Authorization occurs for MQOPEN, MQPUT1, or MQSUB calls to control access to:
  – Queues or Topics
  – Message Context management
  – Alternate userids
  – Namelists
  – Process definitions

• Authorization also occurs for MQCLOSE calls:
  – For Permanent Dynamic Queues
  – When a Topic subscription is removed
MQ API Queue Authorization

- Uses `ssid.queue_name` profiles in the MQQUEUE or MXQUEUE classes

<table>
<thead>
<tr>
<th>Inquire, Browse…</th>
<th>Require READ access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input, Output, Bind, Context management</td>
<td>Require UPDATE access</td>
</tr>
<tr>
<td>Set</td>
<td>Requires ALTER access</td>
</tr>
</tbody>
</table>

- Access required depends on options requested on the MQOPEN, MQPUT1, or MQSUB calls
- No differentiation between reading and writing messages to a queue
  - OAM for other platforms has multiple permissions
MQ API Queue Authorization

- MQOPEN for dynamic queues checks multiple profiles:
  - Model queue profile name
  - Dynamic queue profile name
- Only the Queue Name specified in the MQOD is checked
  - no check is issued for any resolved Queue Name
- MQOPEN or MQPUT1 for an Alias Queue that resolve to a Topic will also check access to the Topic via MXTOPIC / GMXTOPIC profiles
- No Security Checks are issued for Managed Queues created in response to an MQSUB
  - No users should have access to any Managed Queues
  - Profiles ssid.SYSTEM.MANAGED.DURABLE.* and ssid.SYSTEM.MANAGED.NDURABLE.* should be defined with UACC(NONE) and no access list entries
MQ Message Context Security

- Uses `ssid.CONTEXT.queue_name.profiles` in the MQADMIN or MXADMIN classes

<table>
<thead>
<tr>
<th>Profile</th>
<th>Access Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO_CONTEXT</td>
<td>No check issued</td>
</tr>
<tr>
<td>DEFAULT_CONTEXT</td>
<td></td>
</tr>
<tr>
<td>SAVE_ALL_CONTEXT</td>
<td></td>
</tr>
<tr>
<td>PASS_IDENTITYCONTEXT</td>
<td>Requires READ access</td>
</tr>
<tr>
<td>PASS_ALL_CONTEXT</td>
<td></td>
</tr>
<tr>
<td>SET_IDENTITYCONTEXT</td>
<td>Requires UPDATE access</td>
</tr>
<tr>
<td>SET_ALLCONTEXT</td>
<td></td>
</tr>
<tr>
<td>SAVE_ALL_CONTEXT</td>
<td>Requires CONTROL access</td>
</tr>
</tbody>
</table>

- Access required depends on options requested on the MQOPEN or MQPUT1 calls
- One profile per queue manager per queue qualifier
MQ Alternate User Security

- Uses `ssid.ALTERNATE.USER.altuserid` profiles in the MQADMIN or MXADMIN classes
  - Requires UPDATE access

- Access required depends on options requested on the MQSUB, MQOPEN or MQPUT1 calls based on `ALTERNATE_USER_AUTHORITY(userid)` parameter

- One profile per queue manager, per alternate userid

- Source of Alternate User ID:
  - MQMD UserIdentifier field of the message
  - MQSD AlternateIUserId field on the MQSUB request
MQ Namelist Security

• Uses **ssid.namelist_name** profiles in the MQNLIST or MXNLIST classes
  – Requires READ access

• Access required depends on options requested on the MQOPEN or MQPUT1 calls
  – Namelists are always OPENed for inquiry
MQ Process Security

- Uses `ssid.process_name` profiles in the MQPROC or MXPROC classes
  - Requires READ access

- Access required depends on options requested on the MQOPEN or MQPUT1 calls
  - Process Definitions are always OPENed for inquiry
MQ Topic Security

- Uses `ssid.SUBSCRIBE.resource_name` and `ssid.PUBLISH.resource_name` profiles in the MXTOPIC class and profile members GMXTOPTOPIC class profiles.

<table>
<thead>
<tr>
<th>Action</th>
<th>Access Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESUME</td>
<td>Requires READ access</td>
</tr>
<tr>
<td>CREATE or ALTER</td>
<td>Requires ALTER access</td>
</tr>
</tbody>
</table>

- Access required depends on options requested on the MQSUB call.
- Security Check performed against the nearest Parent Topic Object, for which a profile is defined.
MQ User Roles

Users needing access to MQ commands:

**People**
- MQ Administrators - Typically access to all MQ commands
- Security Administrators – Typically Security Refresh command access
- Operators – Typically access to START / STOP queue manages, CHIN, CHANNELs
- Programmers and Tech Support – Typically only DISPLAY commands

**Processes**
- Channel Initiator User IDs – Access to any commands in CSQINPX concatenation
- Automation User IDs - access to START / STOP queue managers
- Monitoring Software User IDs – DISPLAY commands, possibly others
MQ Command Security

- Uses MQCMDS/ssid.verb.resource_type profiles

<table>
<thead>
<tr>
<th>DISPLAY commands</th>
<th>Require READ access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARCHIVE, PING, RECOVER, RESET, RESOLVE, RESUME, START, STOP, SUSPEND commands</td>
<td>Require CONTROL access</td>
</tr>
<tr>
<td>ALTER, CLEAR, DEFINE, DELETE, REFRESH, RVERIFY commands</td>
<td>Require ALTER access</td>
</tr>
</tbody>
</table>

- Access required depends on the command verb
MQ Command Resource Security

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

| 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

©2016 Vanguard Integrity Professionals, Inc.
MQ Switch Profile Controls

MQADMIN class profiles used to control the types of security checks performed:

<table>
<thead>
<tr>
<th>MQ API Security</th>
<th>ssid.NO.CONNECT.CHECKS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ssid.NO.QUEUE.CHECKS</td>
</tr>
<tr>
<td></td>
<td>ssid.NO.CONTEXT.CHECKS</td>
</tr>
<tr>
<td></td>
<td>ssid.NO.ALTERNATE.USER.CHECKS</td>
</tr>
<tr>
<td></td>
<td>ssid.NO.NLIST.CHECKS</td>
</tr>
<tr>
<td></td>
<td>ssid.NO.PROCESS.CHECKS</td>
</tr>
<tr>
<td></td>
<td>ssid.NO.TOPIC.CHECKS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MQ Command Security</th>
<th>ssid.NO.COMMAND.CHECKS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ssid.NO.COMMAND.CHECKS</td>
</tr>
<tr>
<td></td>
<td>ssid.NO.CMD.RESC.CHECKS</td>
</tr>
</tbody>
</table>

©2016 Vanguard Integrity Professionals, Inc.
MQ Switch Profile Controls

MQADMIN class profiles are used to control security checking for subsystems and queue sharing groups:

<table>
<thead>
<tr>
<th>MQ Subsystem Security</th>
<th>qmgrid.NO.SUBSYS.SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>qsgid.NO.SUBSYS.SECURITY</td>
</tr>
<tr>
<td></td>
<td>qmgrid.YES.SUBSYS.SECURITY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MQ Queue Manager Level Security</th>
<th>qmgrid.NO.QMGR.CHECKS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>qsgid.NO.QMGR.CHECKS</td>
</tr>
<tr>
<td></td>
<td>qmgrid.YES.QMGR.CHECKS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MQ Queue Sharing Group Level Security</th>
<th>qmgrid.NO.QSG.CHECKS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>qsgid.NO.QSG.CHECKS</td>
</tr>
<tr>
<td></td>
<td>qmgrid.YES.QSG.CHECKS</td>
</tr>
</tbody>
</table>
MQ Switch Profile Controls

• Neither UACC nor access list are used for Switch profiles
• For **full** WebSphere MQ security, ensure that no ssid.NO…profiles exist
  – Use SEARCH command to verify:
    SR CLASS(MQADMIN) MASK(ssid.NO)
• For **selective** WebSphere MQ security
  – Define switch profiles for the security types to be bypassed; for example:
    RDEF MQADMIN ssid.NO.NLIST.CHECKS
    RDEF MQADMIN ssid.NO.PROCESS.CHECKS
    RDEF MQADMIN ssid.NO.CMD.RESC.CHECKS
MQ Security Administration Commands

• RACF Commands
  – SETROPTS GENERIC(classname)
  – Define profiles
  – SETROPTS CLASSACT(classname)
    • MQ Resource Classes are “nasty” - DFLT

• WebSphere MQ Administrative Commands
  – DISPLAY SECURITY
    • ALL | INTERVAL | SWITCHES | TIMEOUT
  – REFRESH SECURITY
    • * | MQADMIN | MQQUEUE | MQNLIST | MQPROC
  – RVERIFY SECURITY
    • USERID1, USERID2, . . .
  – ALTER SECURITY
    • INTERVAL(nn) | TIMEOUT(nn)
MQ QMGR Security Messages

13.35.26 STC01960 CSQH001I !MQ19 CSQHINSQ Security using uppercase classes
13.35.26 STC01960 CSQH024I !MQ19 CSQHINSQ SUBSYSTEM security switch set ON, profile 'SQ05.NO.SUBSYS.SECURITY' not found
13.35.26 STC01960 CSQH022I !MQ19 CSQHINSQ QMGR security switch set ON, profile 'MQ19.YES.QMGR.CHECKS' found
13.35.26 STC01960 CSQH021I !MQ19 CSQHINSQ QSG security switch set OFF, profile 'SQ05.NO.QSG.CHECKS' found
13.35.26 STC01960 CSQH024I !MQ19 CSQHIS1C CONNECTION security switch set OFF, profile 'MQ19.NO.CONNECT.CHECKS' found
13.35.26 STC01960 CSQH024I !MQ19 CSQHIS1C COMMAND security switch set ON, profile 'MQ19.NO.CMD.CHECKS' not found
13.35.26 STC01960 CSQH024I !MQ19 CSQHIS1C COMMAND RESOURCES security switch set OFF, profile 'MQ19.NO.CMD.RESC.CHECKS' found
13.35.26 STC01960 CSQH024I !MQ19 CSQHIS1C ALTERNATE USER security switch set ON, profile 'MQ19.NO.ALTERNATE.USER.CHECKS' not found
13.35.26 STC01960 CSQH024I !MQ19 CSQHIS1C COMMAND RESOURCES security switch set OFF, profile 'MQ19.NO.CMD.RESC.CHECKS' found
13.35.26 STC01960 CSQH024I !MQ19 CSQHIS1C PROCESS security switch set ON, profile 'MQ19.NO.PROCESS.CHECKS' not found
13.35.26 STC01960 CSQH024I !MQ19 CSQHIS1C PROCESS RESOURCES security switch set ON, profile 'MQ19.NO.PROCESS.RESC.CHECKS' not found
13.35.26 STC01960 CSQH024I !MQ19 CSQHIS1C NAMESPACE security switch set ON, profile 'MQ19.NO.NAMESPACE.CHECKS' not found
13.35.26 STC01960 CSQH024I !MQ19 CSQHIS1C QUEUE security switch set ON, profile 'MQ19.NO.QUEUE.CHECKS' not found
13.35.26 STC01960 CSQH024I !MQ19 CSQHIS1C TOPIC security switch set ON, profile 'MQ19.NO.TOPIC.CHECKS' not found
MQ ‘Display Security all’ Messages

Response to ‘display security all’ command:

13.36.06 STC01960 CSQH015I !MQ19 Security timeout = 54 minutes
13.36.06 STC01960 CSQH016I !MQ19 Security interval = 12 minutes
13.36.06 STC01960 CSQH037I !MQ19 Security using uppercase classes
13.36.06 STC01960 CSQH030I !MQ19 Security switches ...
13.36.06 STC01960 CSQH034I !MQ19 SUBSYSTEM: ON, 'SQ05.NO.SUBSYS SECURITY' not found
13.36.06 STC01960 CSQH032I !MQ19 QMGR: ON, 'MQ19.YES.QMGR.CHECKS' found
13.36.06 STC01960 CSQH031I !MQ19 QSG: OFF, 'SQ05.NO.QSG.CHECKS' found
13.36.06 STC01960 CSQH031I !MQ19 CONNECTION: OFF, 'MQ19.NO.CONNECT.CHECKS' found
13.36.06 STC01960 CSQH034I !MQ19 COMMAND: ON, 'MQ19.NO.CMD.CHECKS' not found
13.36.06 STC01960 CSQH031I !MQ19 CONTEXT: OFF, 'MQ19.NO.CONTEXT.CHECKS' found
13.36.06 STC01960 CSQH034I !MQ19 ALTERNATEUSER: ON, 'MQ19.NO.ALTERNATE.USER.CHECKS' not found
13.36.06 STC01960 CSQH034I !MQ19 PROCESS: ON, 'MQ19.NO.PROCESS.CHECKS' not found
13.36.06 STC01960 CSQH034I !MQ19 NAMELIST: ON, 'MQ19.NO.NLIST.CHECKS' not found
13.36.06 STC01960 CSQH034I !MQ19 QUEUE: ON, 'MQ19.NO.QUEUE.CHECKS' not found
13.36.06 STC01960 CSQH034I !MQ19 TOPIC: ON, 'MQ19.NO.TOPIC.CHECKS' not found
13.36.06 STC01960 CSQH031I !MQ19 COMMAND RESOURCES: OFF, 'MQ19.NO.CMD.RESC.CHECKS' found
13.36.06 STC01960 CSQH034I !MQ19 CSQHPDTC 'DISPLAY SECURITY' NORMAL COMPLETION
MQ Security – End to End

End to End Application Security

Administrative Commands

Command Security

Application

Batch/TSO Application

IMS Application

CICS Application

Access Control

Context Security

Transmission Security

MQ Client

MQI

Distributed MQ Server

Queue Manager A

DQM

Queue Manager B

Distributed MQ Server

Communication links to other WebSphere MQ Servers
MQ Advanced Message Security

• MQ Standard Security
  – Message data can be encrypted during transmission via SSL/TLS, but not while residing in queues
  – Authentication is based on operating system identifier of the local process

• MQ Advanced Message Security
  – Provides assurance that messages have not been altered in transit
  – Provides assurance that messages were originated from the expected source
  – Provides assurance that messages can only be viewed by intended recipients
  – Is administered using queue based policies

• MQ AMS incorporated into MQ V8
30,000 foot view of MQ AMS

Sending Application

MQ AMS Exit

TLS and encryption

Sending QM

MQ Channel

Receiving QM

TLS and decryption

MQ AMS exit

Receiving Application

“End to End Security”

Introduced In WMQ V7.01

Rolled into MQ V8.0

©2016 Vanguard Integrity Professionals, Inc.
MQ Advanced Message Security

• MQ Advanced Message Security policy:
  – Policy name
  – Whether signing is required, and signature algorithm
  – Whether encryption is required, and encryption algorithm
  – Which DN identities are can place messages on the queue
  – Which DN identities can retrieve messages from the queue

• Quality of protection Choices
  – None - No data-protection is applicable
  – Integrity - Messages should be signed by the sender
  – Privacy - Messages should be signed and encrypted
Additional MQ Considerations

- **IBM MQ for z/OS V9.0** – Current Release
  - Announced on April 19, 2016
  - Available since June 2, 2016
- **IBM MQ for z/OS V8.0**
  - Available since 13 June 2014
- **WebSphere MQ for z/OS V7.1**
  - Available since 25 November 2011
- **WebSphere MQ AMS for z/OS V7.0.1**
  - End of Service - September 2015
IBM DeveloperWorks References

• Getting started with WebSphere MQ for z/OS security

• WebSphere MQ for z/OS security

• Comparing WebSphere MQ security on distributed platforms and z/OS
Summary

• Messaging & MQ Overview
• Overview of MQ Security
• MQ Security for z/OS
Conclusion

Questions?
Thank you!
Thank You!

For more information, please visit:
http://www.go2vanguard.com
sales@go2vanguard.com