IBM

IBM Software Group

WebSphere MQ Security for QSA's

Or: "What in your network isn't keeping you up at night, but should."

Sponsored by PCIKnowledgebase.com

May 1, 2009

WebSphere software

pci knowledge base

T.Rob Wyatt, WebSphere MQ Security Focused Practice

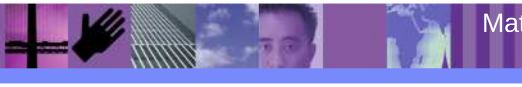
t.rob.wyatt@us.ibm.com
http://ausgsa.ibm.com/~trwyatt/ (internal) or http://t-rob.net (public)
IBM Software Services for WebSphere
http://www.ibm.com/WebSphere/developer/services

e business on demand software

last update: April 15, 2009

WebSphere MQ Security Presentation Series

- This presentation is part of the WebSphere MQ Security Presentation Series led by T.Rob Wyatt with help from so many others
  - Available internally at http://ausgsa.ibm.com/~trwyatt/public/wmqsecurityseries/
- Related presentations
  - We assume you've seen or are familiar with
    - Core Concepts (From the WAS Security Presentation Series)
    - WMQ Security Introduction
    - Authorization Overview
  - You may be interested in
    - WAS Security Presentation Series available internally at http://pokgsa.ibm.com/~keys/documents/securitySeries



Change is the Only Constant

This presentation reflects

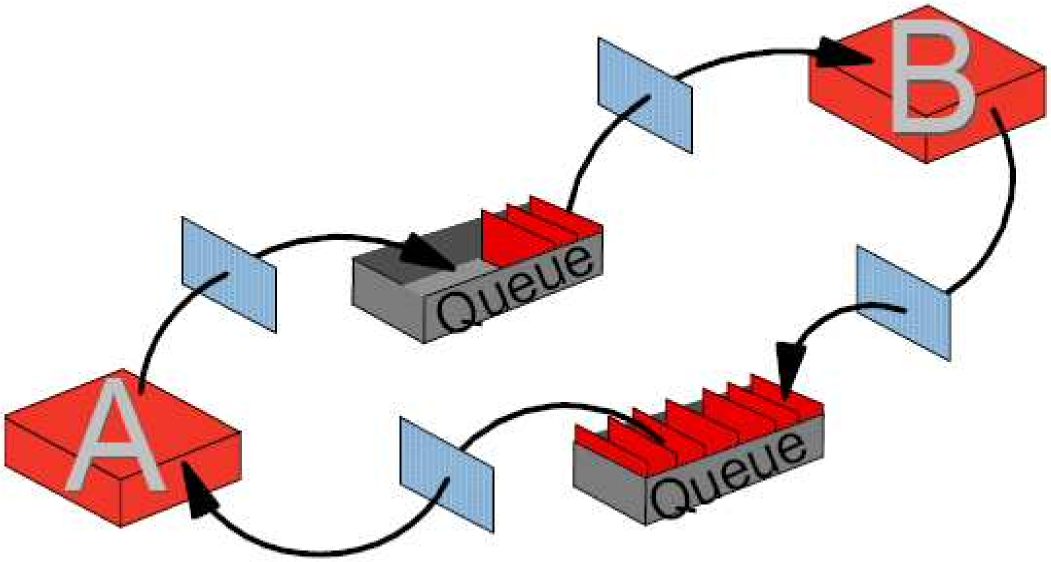
- My current opinions regarding WMQ security
- The product itself continues to evolve (even in PTFs)
  - Presentation is based on V6.0 & V7.0
- This will be revised as we learn more
- Your thoughts and ideas are welcome

Agenda

- What is messaging middleware?
- Who uses WebSphere MQ? Your clients!
- How WebSphere MQ works
- Vulnerabilities of an unsecured queue manager
- Compliance implications
- All the fruit is low hanging fruit
- The 5-minute assessment

Messaging is industrial-strength email

- Communication is based on discrete messages
- Messages are stored and forwarded
- Routing and delivery delegated to messaging provider
- Decouple sender and receiver
  - Temporally – messaging is asynchronous
  - By platform – support of UTF and for code page conversion
- Many qualities of service available
  - Assured once-and-only-once delivery
  - At-least-once delivery
  - Best effort delivery
- Allows for mediation layer
  - Transformation
  - Enrichment
  - Aggregation
  - Policy enforcement



Messaging middleware flavors - JMS

- Specification of an API which includes point-to-point and pub/sub
- Messages are compatible in-memory up to the API
- Behind the API, each transport vendor is free to implement proprietary wire protocols
- Integral part of the JEE framework
- Enterprise Java Beans enhance JMS to include concurrent message consumption as well as JCA transactionality

- Many transport providers support JMS, of which WebSphere MQ has the largest market share

Messaging middleware flavors – WebSphere MQ

- Before there was JMS, there was MQ
- APIs for C, C++, COBOL, REXX, Perl, .Net, Power Shell, Python, RPG
- Platforms include: AIX, HP-UX, Solaris, Linux, OpenVMS, Tandem NSK, z/OS, AS/400, Windows, OS/2, Tru64, z/VSE

Agenda

- What is messaging middleware?
- Who uses WebSphere MQ? Your clients!
- How WebSphere MQ works
- Vulnerabilities of an unsecured queue manager
- Compliance implications
- All the fruit is low hanging fruit
- The 5-minute assessment

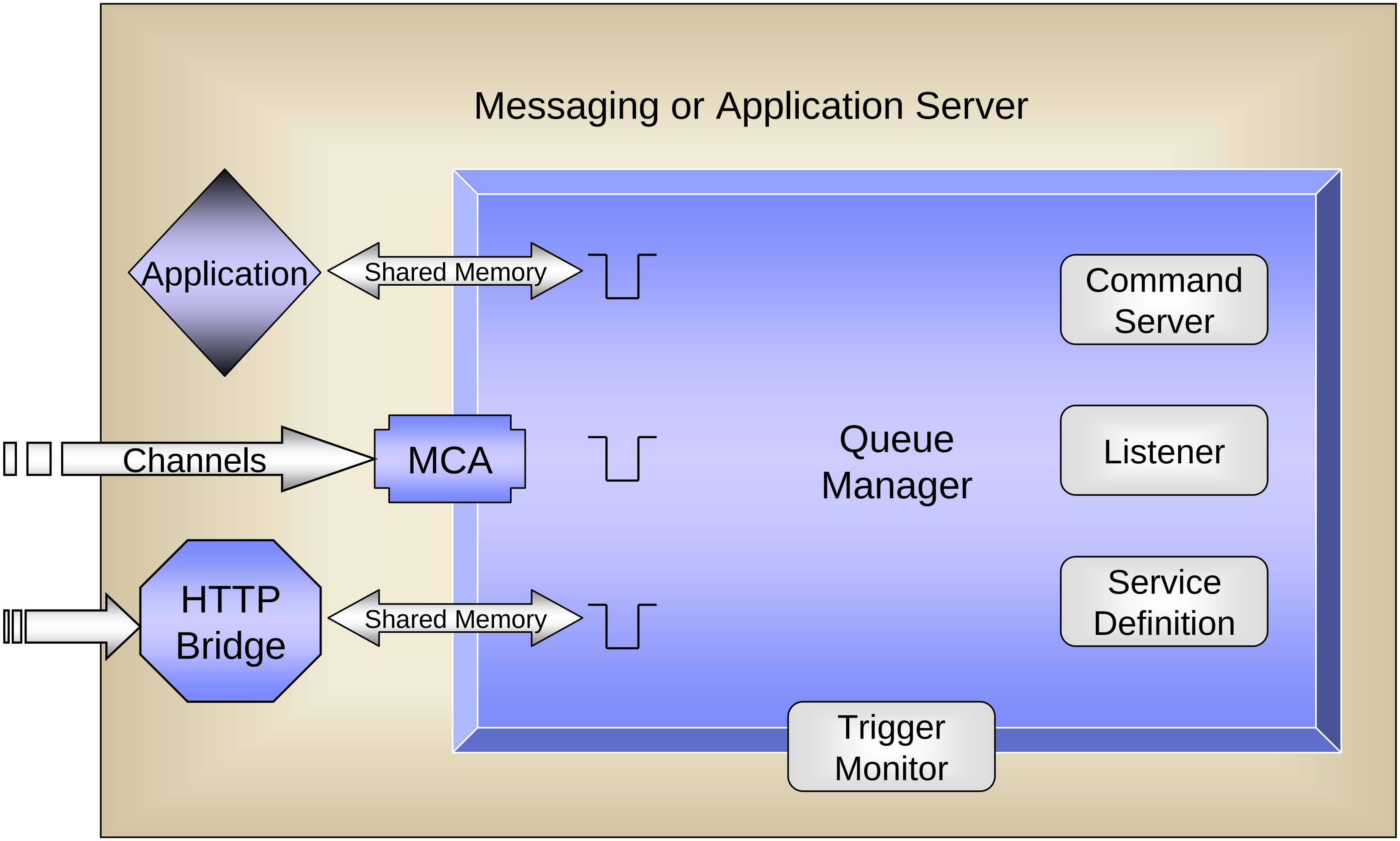
Who uses WebSphere MQ?

- Commerce
  - Brick and mortar and online retail
  - Card payment processors
  - Travel industry
  - Banks, clearing houses and other financial institutions
  - Healthcare, medical, pharmacy
  - Retail, commercial insurers – all lines
- Outsourcing & B2B
  - Customer relationship management – call centers
  - Personnel
  - Supply chain management
  - All of the above

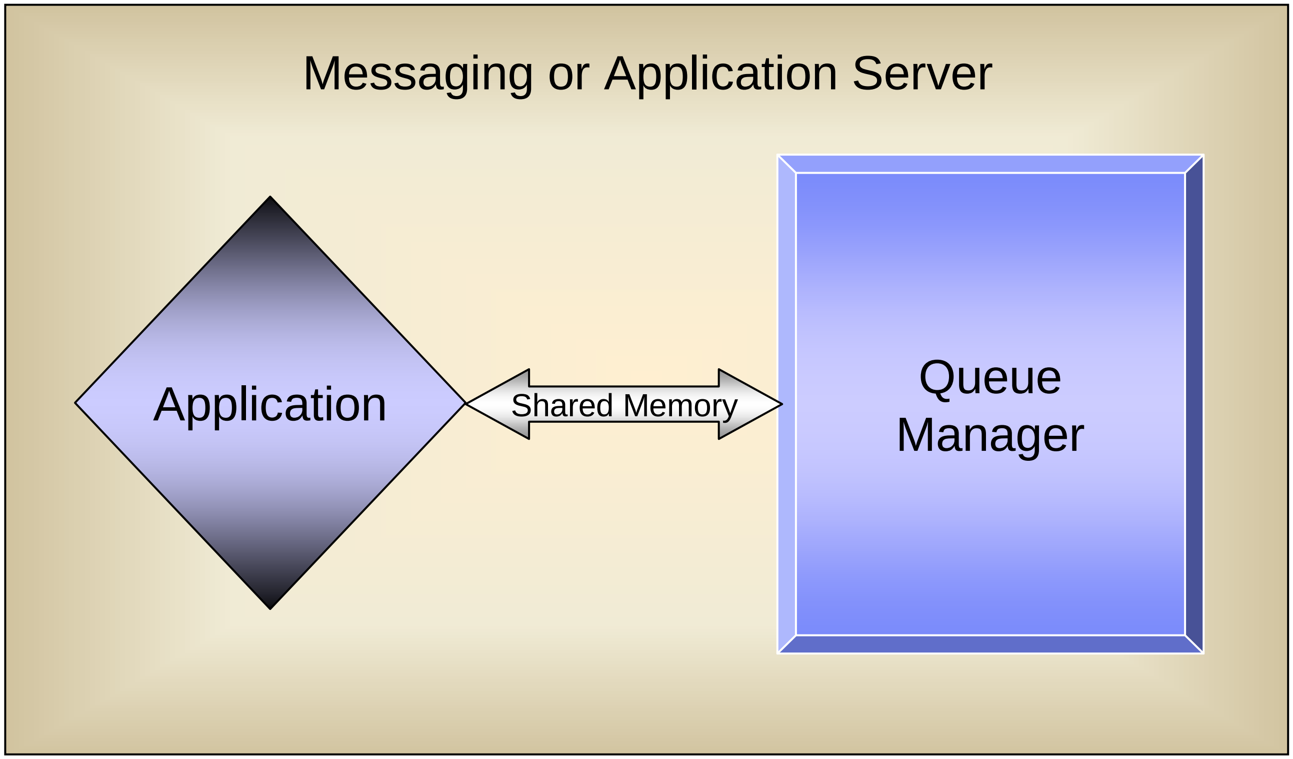
Agenda

- What is messaging middleware?
- Who uses WebSphere MQ? Your clients!
- How WebSphere MQ works
- Vulnerabilities of an unsecured queue manager
- Compliance implications
- All the fruit is low hanging fruit
- The 5-minute assessment

How WebSphere MQ works - Components

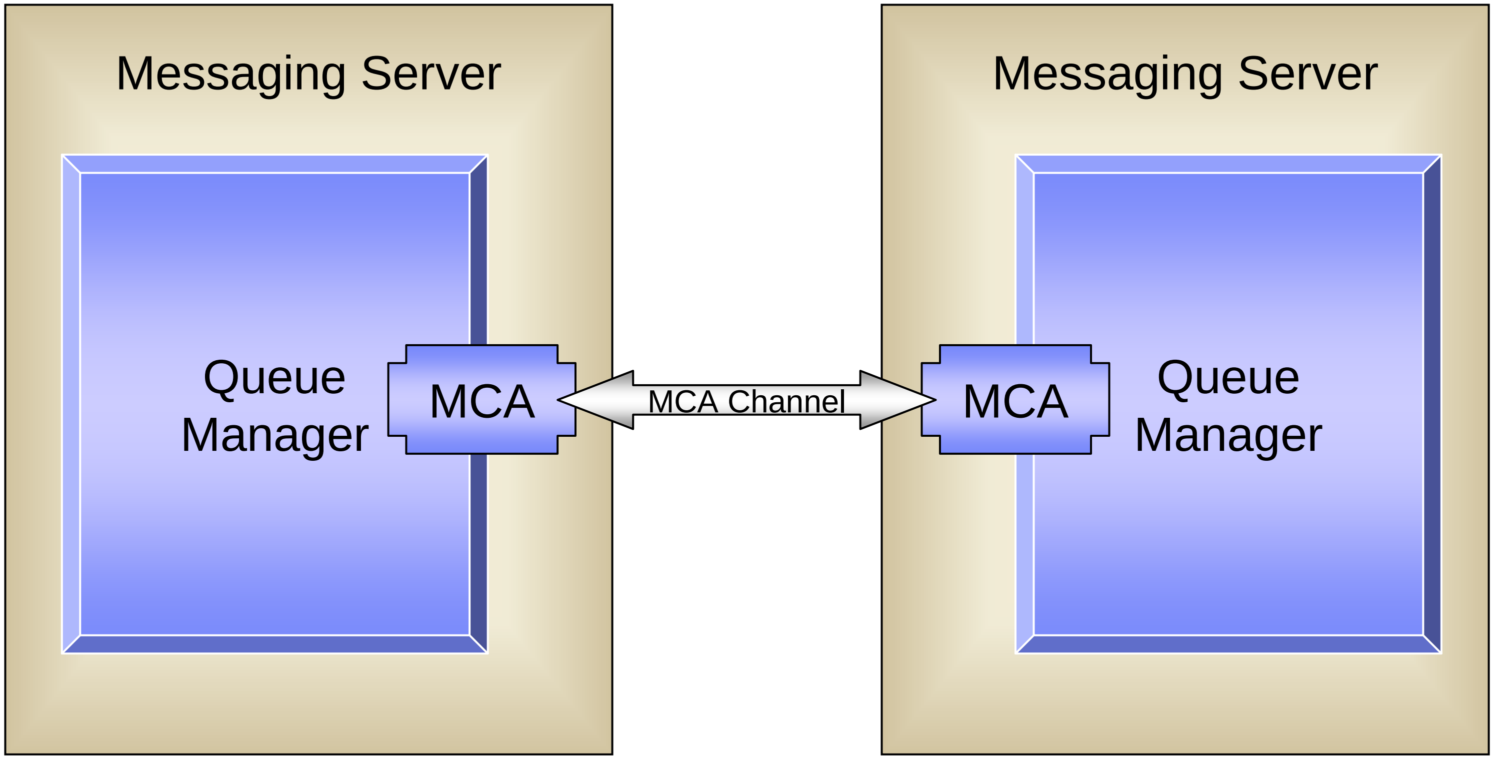


How WebSphere MQ Works – Local applications



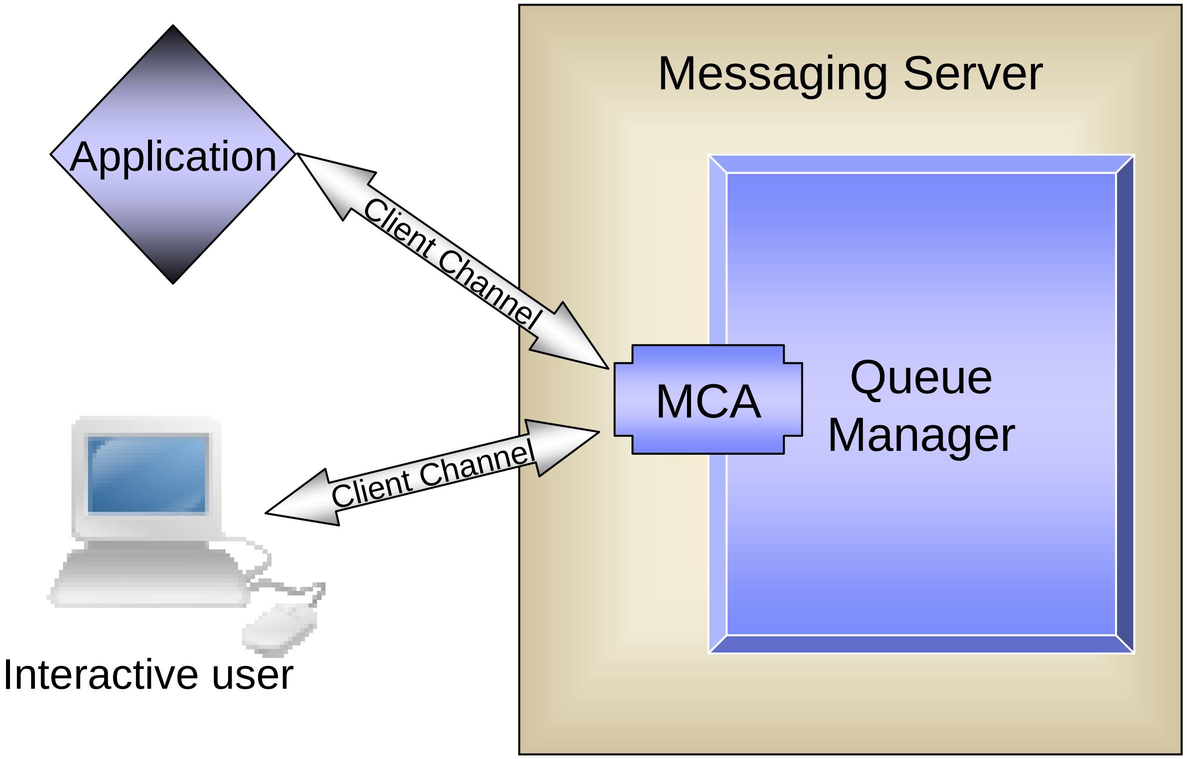
- Authentication is performed by the OS
- WMQ authorizes the ID of the connected process

How WebSphere MQ Works – Remote QMgrs



- Message Channel Agent runs with admin authority
- By default authorized as administrator
- Can put to or get from any queue

How WebSphere MQ Works – Remote clients

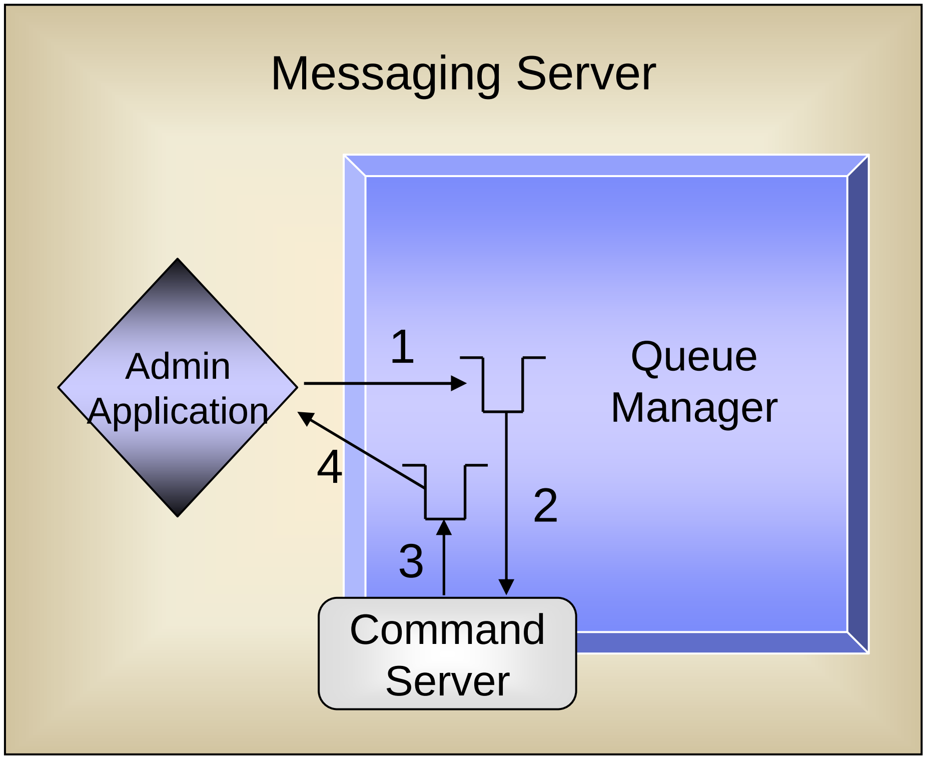


- Message Channel Agent runs with admin authority
- By default authorizes asserted user ID
- No authentication of asserted identity

How WebSphere MQ Works – Command Server

Command Server: Converts command messages into administrative actions such as define, delete, display objects.

1. Msg placed on command queue.
2. Command server reads message and executes command(s)
3. Results reported to reply queue
4. Application consumes reply messages.

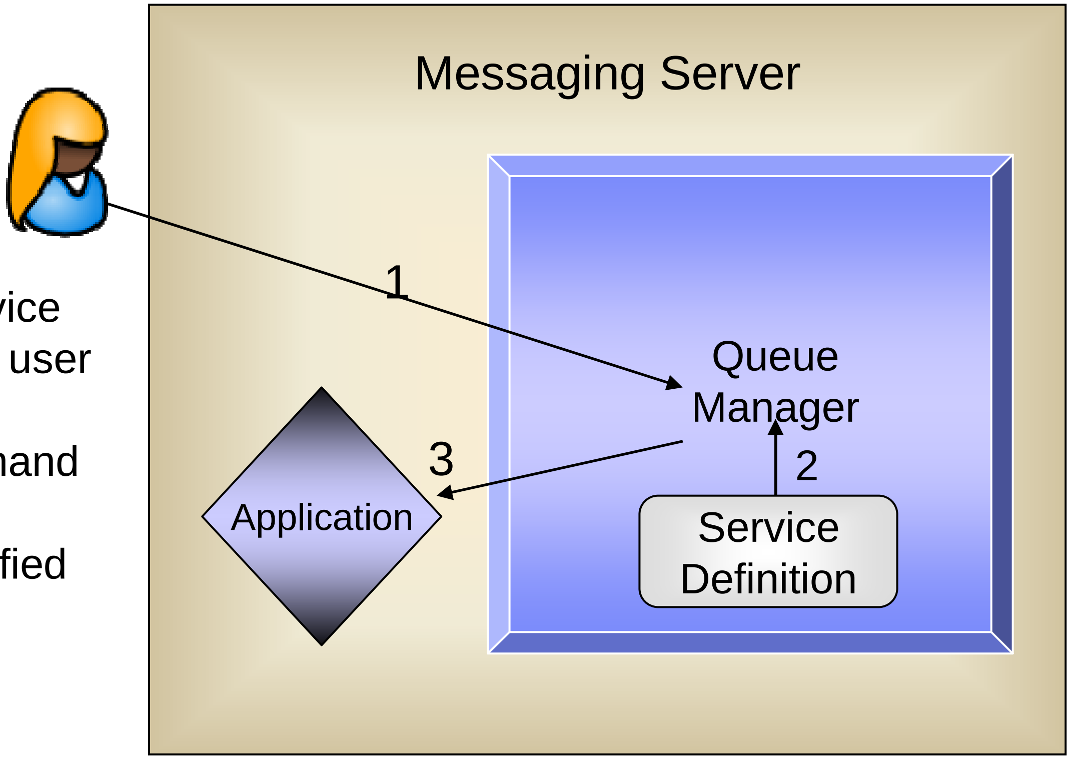


Command server actions are constrained to WebSphere MQ object management and operations such as start/stop of channels. Does not directly execute OS commands or access application messages (except to clear a queue).

How WebSphere MQ Works – Service definition

Service Definition: Pre-defined OS command executed by the queue manager.

1. Command to start or stop a service received from command server, user or automation.
2. Queue manager retrieves command stored in the service definition.
3. Queue manager executes specified command.



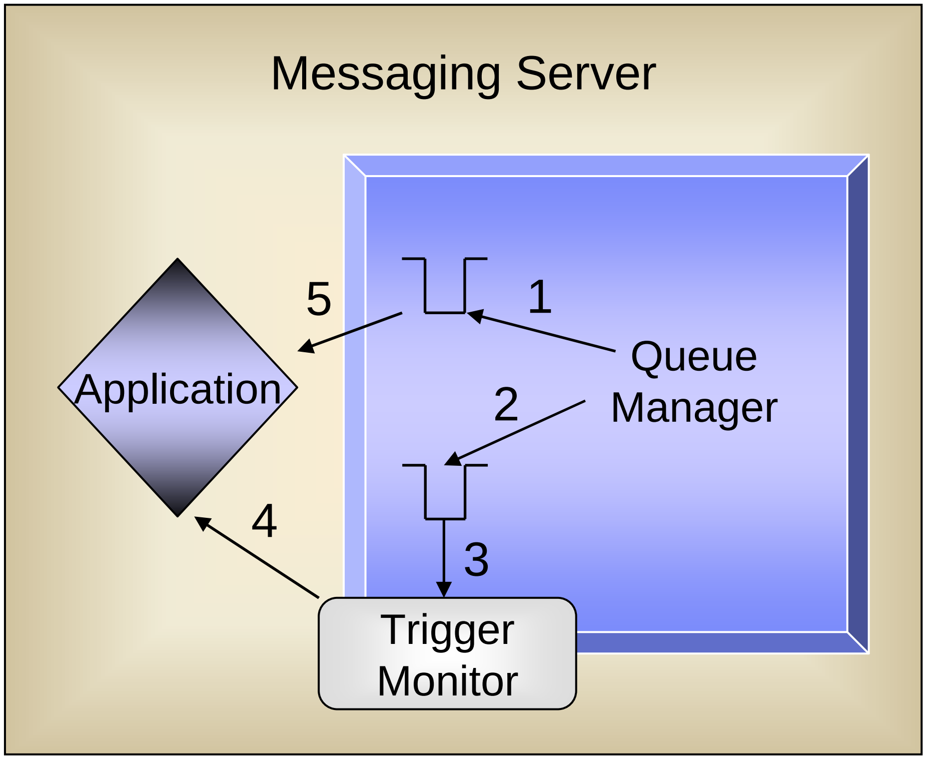
Any arbitrary command may be executed by a service definition. There is no option to disable this behavior. Commands executed as services run under the WMQ administrative account. Service definitions are defined using the command server or command line.

How WebSphere MQ Works – Trigger monitor

Trigger Monitor: Designed to initiate an application based on arrival of a message in a triggered queue.

1. Msg placed on triggered queue.
2. Msg placed on initiation queue.
3. Trigger monitor parses message.
4. Trigger monitor starts application named by and with the options specified by the trigger message.
5. Triggered application services queue.

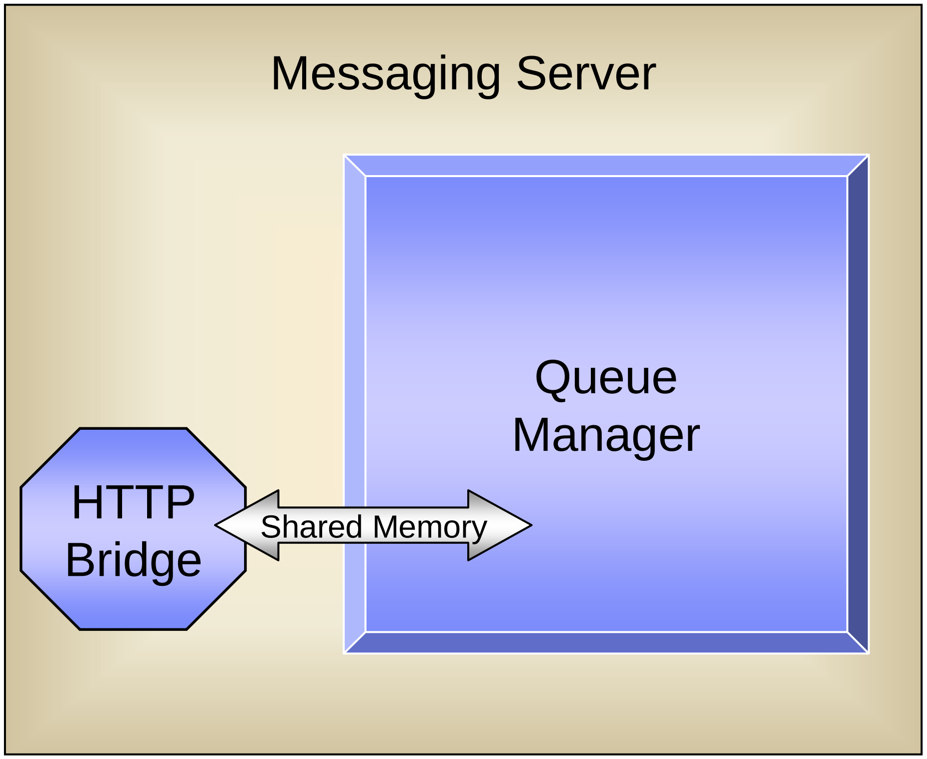
Trigger monitor started as a service runs as the WMQ administrative account.



Alternative definition: process designed to convert queued messages into OS commands.

How WebSphere MQ Works – HTTP Bridge

HTTP Bridge: Converts REST calls to MQ API



- The HTTP bridge converts HTTP calls to enqueue/dequeue calls.
- If the HTTP bridge is running under the WMQ service account, it has access to any queue or message.

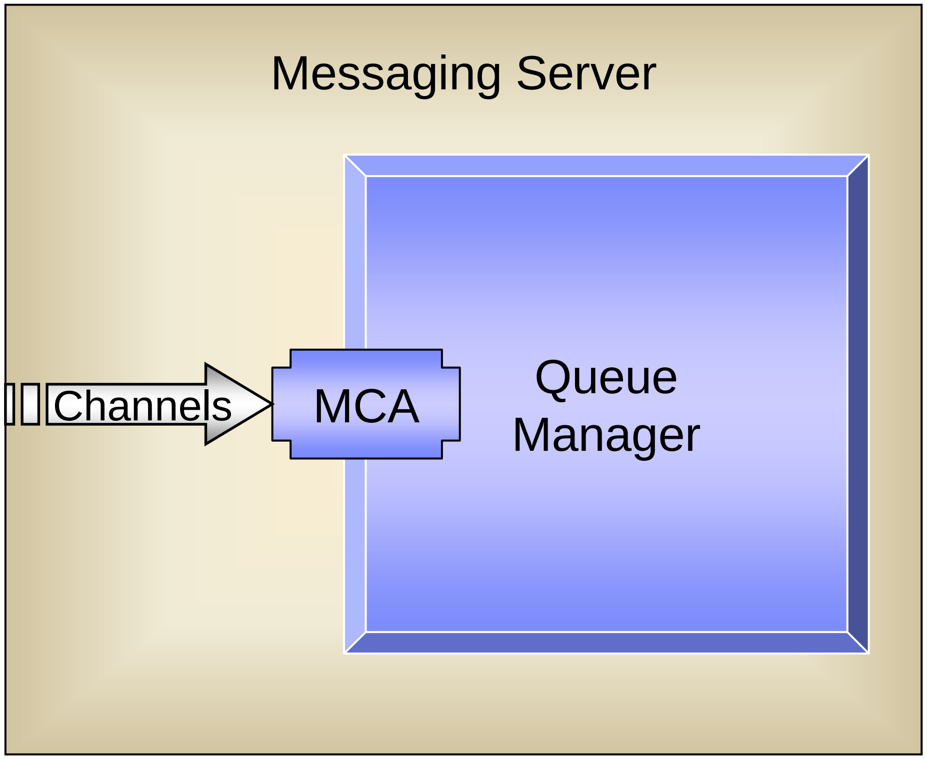
HTTP Bridge started as a service runs as the WMQ administrative account.

If the HTTP Bridge is running under an administrative ID, it has access to any queue.

How WebSphere MQ Works – Message Channel Agent

MCA: Converts network protocols to MQ API calls

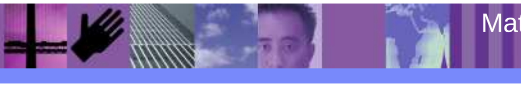
- May be from other QMgrs, interactive users or from applications.
- Channels listen on all interfaces and accept all connection requests.
- Channels run as the WMQ administrator.
- Remote identities not authenticated but authorization is ‘enforced’.
- SSL or exits may be used to provide privacy, integrity or authentication.



The authorization function provided by the channels perpetuates the myth of security in the default configuration. Few administrators realize that THEY are expected to provide the authentication functions using either SSL or exits.

Agenda

- What is messaging middleware?
- Who uses WebSphere MQ? Your clients!
- How WebSphere MQ works
- Vulnerabilities of an unsecured queue manager
- Compliance implications
- All the fruit is low hanging fruit
- The 5-minute assessment



Vulnerabilities – Access to messages

An administrative user can…

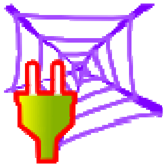
- Browse or read any message on any queue.
  - Undetected collection of sensitive data
- Inject arbitrary messages onto any queue
  - Directly drive services or execute transactions
  - Execute denial of service attack using large or 'poison' messages
- Intercept messages passing through the network
  - Classic man-in-the-middle attack
- Delete messages from queues
  - Denial of service
  - Cover tracks of the intrusion

Vulnerabilities – Execute WMQ commands

An administrative user can…

- Create/delete queues
  - Insert back door access

- Create/delete channels
  - Redefine routing in the network
  - Insert rogue services into message flow
  - Impersonate application or business partner
  - Use your network to attack 3rd party B2B partners



- Create service definitions
  - Run arbitrary OS commands

Vulnerabilities – Arbitrary remote code execution

An administrative user can…

- Execute any command to which the WMQ administrator is authorized.
  - Attack any other queue managers on the same server.
  - Start an X window, telnet or SSH session.
  - Retrieve any keyring(s) of the WebSphere MQ account uses (including the stashed passwords).
  - Bootstrap admin access to adjacent queue managers.
  - Edit or delete log files.
  - Disable security entirely.

Agenda

- What is messaging middleware?
- Who uses WebSphere MQ? Your clients!
- How WebSphere MQ works
- Vulnerabilities of an unsecured queue manager
- Compliance implications
- All the fruit is low hanging fruit
- The 5-minute assessment

WMQ and PCI-DSS

2.1 Always change vendor-supplied defaults **before** installing a system on the network

- Channel template definitions (SYSTEM.* channels) and user-defined channels fo not authenticate or enforce authorization profiles by default.
- Accounts used to run trigger monitors, monitoring, instrumentation or reporting should be run under low-privileged accounts when possible.
- Default behavior of applications started as WebSphere MQ services is to run under an administrative account.

WMQ and PCI-DSS

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.

6.1 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.

- Versions of WebSphere MQ prior to V6.0 are unsupported and will not be patched for newly discovered vulnerabilities.
- Versions 5.3.13 and earlier as well as V6.0 through V6.0.2.1 have channel vulnerabilities that allow bypass of security controls. Acceptable versions are V5.3.1.4 and V6.0.2.2 or higher.
- The exposure due to default channel settings is not just “known” as defined here but *well known* in the WMQ community.

WMQ and PCI-DSS

2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non-console administrative access.

- Administration of WebSphere MQ may be performed entirely at the command line.
- Where remote administration tools are based on the WebSphere MQ client, access should be over dedicated channels with SSL encryption enabled.

WMQ and PCI-DSS

2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data.

- Businesses such as clearinghouse services and card payment processors commonly accept external connections from multiple clients. Exposing administrative access allows the customers complete access to each others' data. Often it allows administrative access to some or all of the queue managers of the third parties.
- Even where administrative access is restricted, improper application isolation where multiple 3rd party connections terminate on the same queue manager may expose them to each other's data.

WMQ and PCI-DSS

3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.
3.6.7 Prevention of unauthorized substitution of cryptographic keys

- Any user with administrative access has access to the queue manager's key store and certificate.
- Where multiple queue managers reside on the same host, administrative access to one equates to administrative access to all.

WMQ and PCI-DSS

6.3.2 Separate development/test and production environments

6.3.3 Separation of duties between development/test and production environments

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

7.2 Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.

- You may find environments with production and non-production queues on the same queue manager or with production and non-production queue managers on the same host.
- Queue managers which leak administrative access cannot enforce separation of duties or enforce access controls.
- Remote access to WebSphere MQ effectively defaults to “allow all”.

WMQ and PCI-DSS

There are currently no widely accepted standards for auditing WebSphere MQ against PCI-DSS or any other security standard. The suggestions provided here are intended to be a starting point from which to discuss and build concensus.

The PCI-DSS was used here because it is likely to set the standard for prevailing practices with regard to WebSphere MQ security.

There are currently no standardized penetration test tools for WebSphere MQ. Early tools seen to date have included a Python toolkit for hacking WebSphere MQ, channel protocol definitions for Wireshark, Java client applications, Eclipse modules and a variety of scripted solutions using Perl, Windows Power Shell, ksh, REXX, etc.

Possible audit findings

A queue manager that exposes anonymous administrative authority…

- Cannot enforce even the most basic of controls
- Allows even casual attackers full access to message data
- Easy to cover tracks of an intrusion
- Provides a platform to attack adjacent nodes

“Yes, but my queue manager authenticates connections!”

A queue manager that over-authorizes legitimate users…

- Cannot provide application isolation
- Cannot enforce separation of duties
- Lacks accountability
- Creates dependencies on elevated access privileges that are difficult to remove later on

Queue managers that expose administrative access to ordinary or anonymous users should always generate an audit finding.

Agenda

- What is messaging middleware?
- Who uses WebSphere MQ? Your clients!
- How WebSphere MQ works
- Vulnerabilities of an unsecured queue manager
- Compliance implications
- All the fruit is low hanging fruit
- The 5-minute assessment

An unscientific sampling

These estimates are based on:

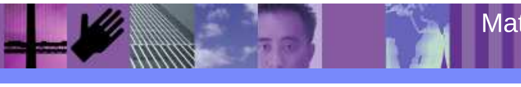
- Anecdotal reports from conference attendees over a 10-year period,
- Discussion in the two main online WebSphere MQ communities
- Pre-sales interviews that did not result in engagements
- Three years of WebSphere MQ consulting engagements within IBM
- Peripheral data collection from non-WMQ consulting engagements

The overwhelming majority of observed implementations have not addressed security at all.

Among those who have tried to address security, most leave at least one “back door” open.

As many as 90% of WMQ shops may be vulnerable. Even assuming a generous error margin, the number of exposed networks is alarming.

There is an extremely high probability that an audit of any WebSphere MQ network will result in a finding requiring remediation.



Agenda

- What is messaging middleware?
- Who uses WebSphere MQ? Your clients!
- How WebSphere MQ works
- Vulnerabilities of an unsecured queue manager
- Compliance implications
- All the fruit is low hanging fruit
- The 5-minute assessment

The 5-minute assessment

Review all inbound WebSphere MQ channels. These are of type Receiver, Requestor, Cluster Receiver and Server Connection.

Look for the following:

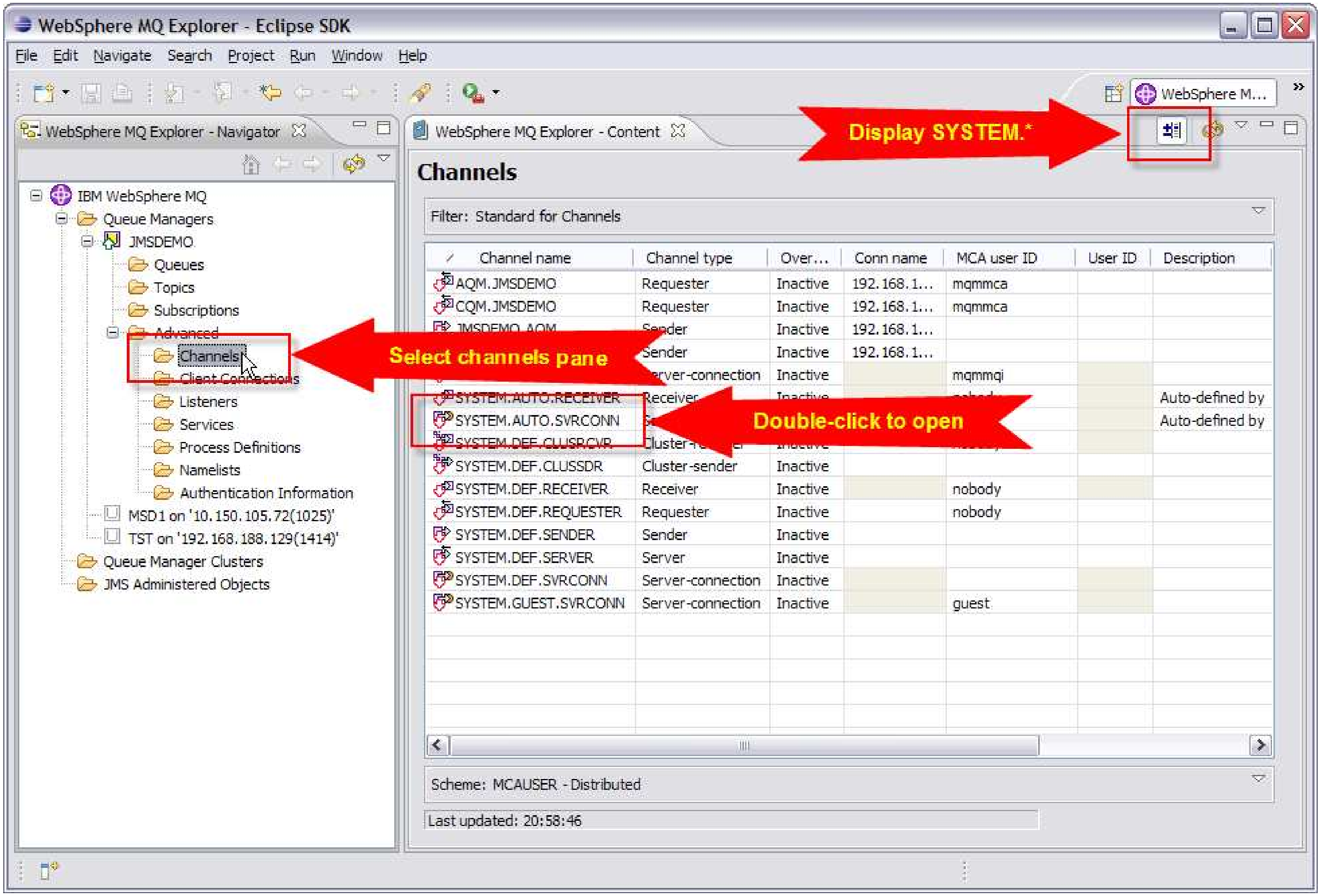
1. MCAUSER attribute is blank (the default) or contains an administrative ID such as mqm on UNIX flavors or MUSR_MQADMIN on Windows.
2. SSLCIPH attribute is blank (the default).
3. SCYEXIT attribute is blank (the default).

   If any single channel (other than those intended for administrative users) has a blank MCAUSER attribute, it exposes administrative access.

   If any inbound channel fails all three of these tests, the queue manager leaks *anonymous* administrative access.

4. In addition, the queue manager must be at V5.3.14 or V6.0.2.2 or higher due to known vulnerabilities in prior versions.

Assessment using WebSphere MQ Explorer


WebSphere MQ Explorer - Eclipse SDK
File Edit Navigate Search Project Run Window Help
WebSphere M...
WebSphere MQ Explorer - Navigator
WebSphere MQ Explorer - Content
IBM WebSphere MQ
Queue Managers
JMSDEMO
Queues
Topics
Subscriptions
Advanced
Channels
Client Connections
Listeners
Services
Process Definitions
Namelists
Authentication Information
MSD1 on '10.150.105.72(1025)'
TST on '192.168.188.129(1414)'
Queue Manager Clusters
JMS Administered Objects

Display SYSTEM.*

Select channels pane

Double-click to open

Channels

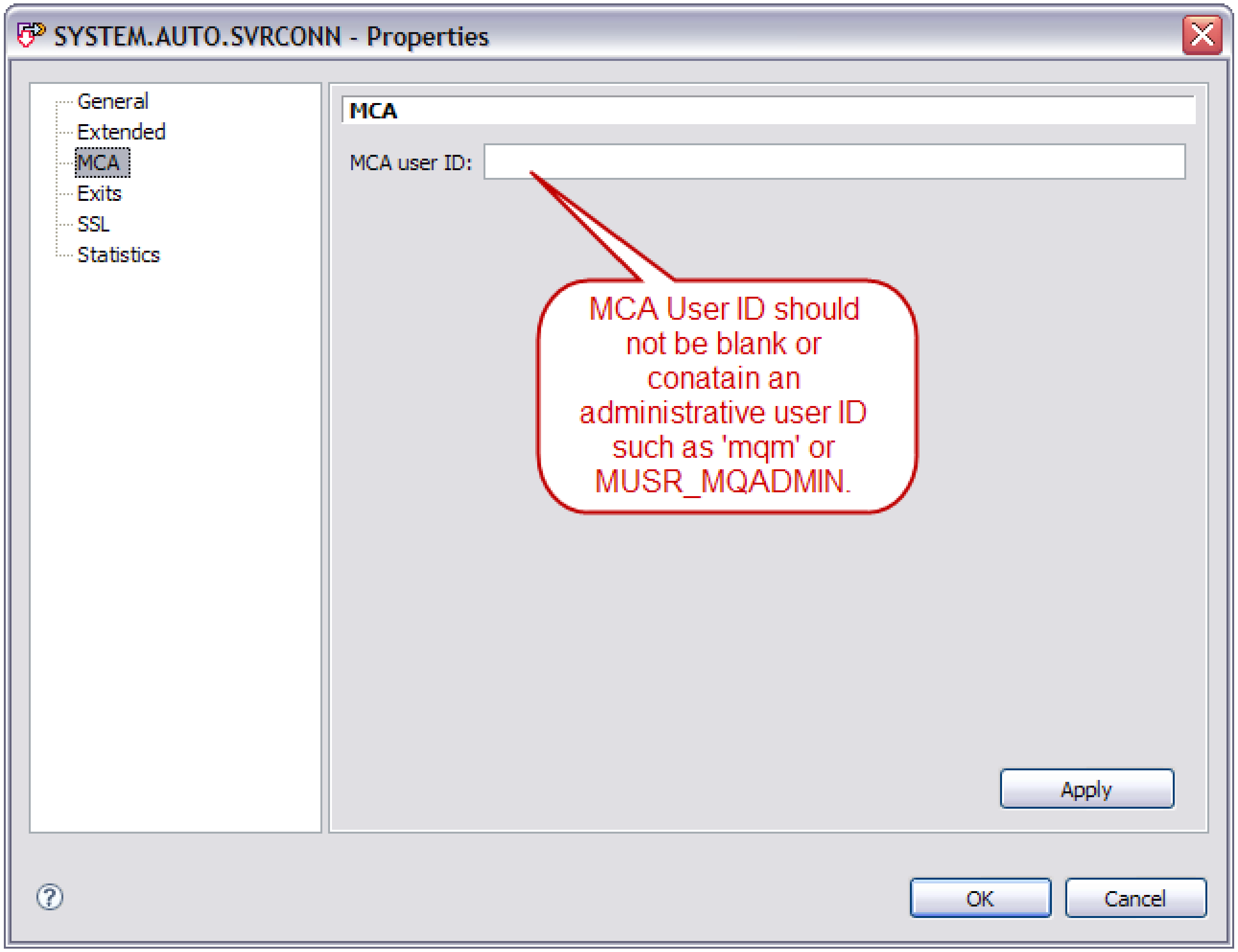
Filter: Standard for Channels

Channel name	Channel type	Over...	Conn name	MCA user ID	User ID	Description
AQM.JMSDEMO	Requester	Inactive	192.168.1...	mqmmca		
CQM.JMSDEMO	Requester	Inactive	192.168.1...	mqmmca		
JMSDEMO.AQM	Sender	Inactive	192.168.1...			
[illegible]	Sender	Inactive	192.168.1...			
[illegible]	Server-connection	Inactive		mqmmqi		
SYSTEM.AUTO.RECEIVER	Receiver	Inactive		nobody		Auto-defined by
SYSTEM.AUTO.SVRCONN	[illegible]	[illegible]		[illegible]		Auto-defined by
SYSTEM.DEF.CLUSRCVR	Cluster-receiver	Inactive		nobody		
SYSTEM.DEF.CLUSSDR	Cluster-sender	Inactive				
SYSTEM.DEF.RECEIVER	Receiver	Inactive		nobody		
SYSTEM.DEF.REQUESTER	Requester	Inactive		nobody		
SYSTEM.DEF.SENDER	Sender	Inactive				
SYSTEM.DEF.SERVER	Server	Inactive				
SYSTEM.DEF.SVRCONN	Server-connection	Inactive				
SYSTEM.GUEST.SVRCONN	Server-connection	Inactive		guest		

Scheme: MCAUSER - Distributed

Last updated: 20:58:46

Assessment using WebSphere MQ Explorer

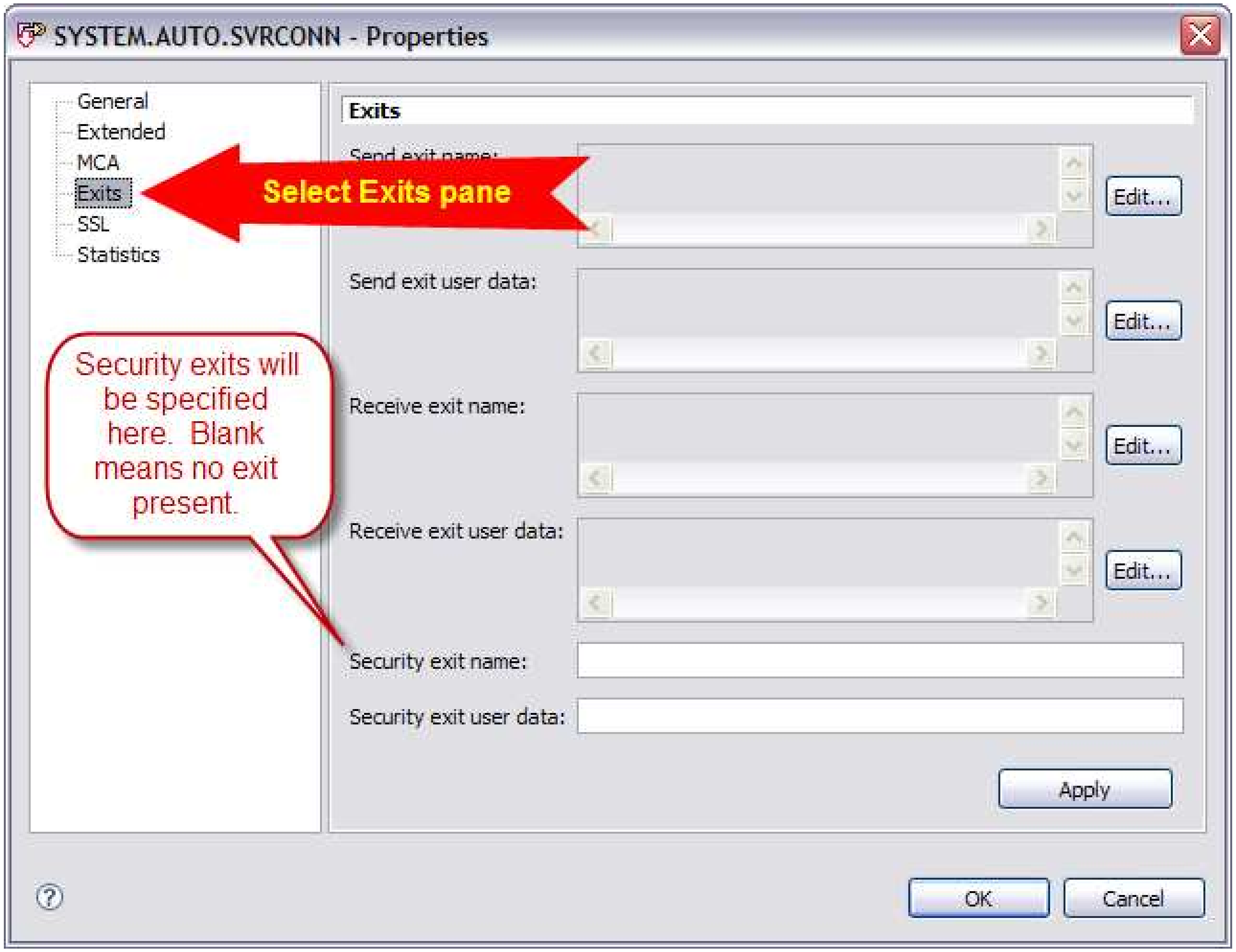


SYSTEM.AUTO.SVRCONN - Properties

MCA user ID:

MCA User ID should not be blank or conatain an administrative user ID such as 'mqm' or MUSR_MQADMIN.

Assessment using WebSphere MQ Explorer



SYSTEM.AUTO.SVRCONN - Properties

Exits

Send exit name:

Send exit user data:

Receive exit name:

Receive exit user data:

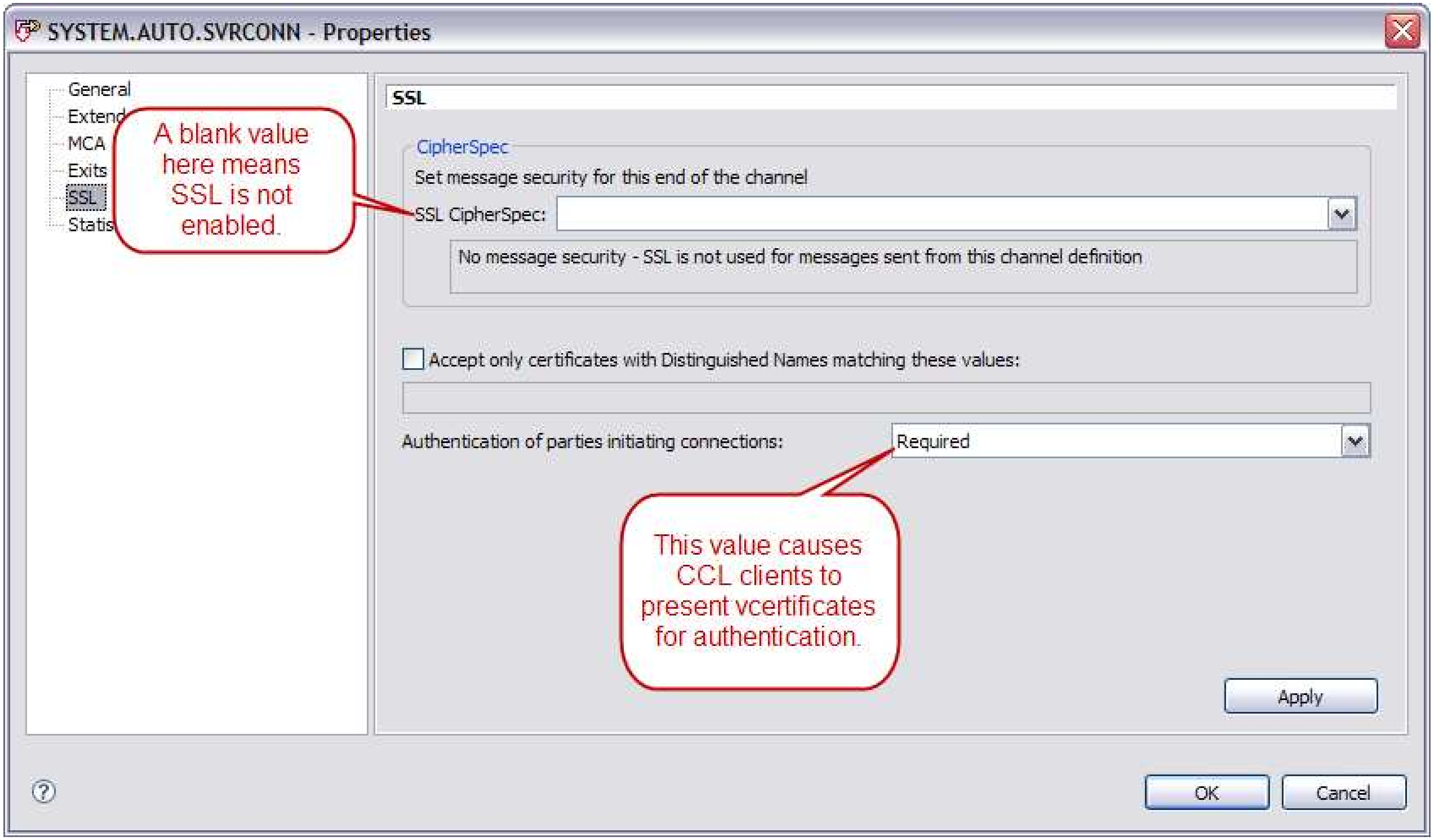
Security exit name:

Security exit user data:

Select Exits pane

Security exits will be specified here. Blank means no exit present.

Assessment using WebSphere MQ Explorer



Set message security for this end of the channel

SSL CipherSpec:

No message security - SSL is not used for messages sent from this channel definition

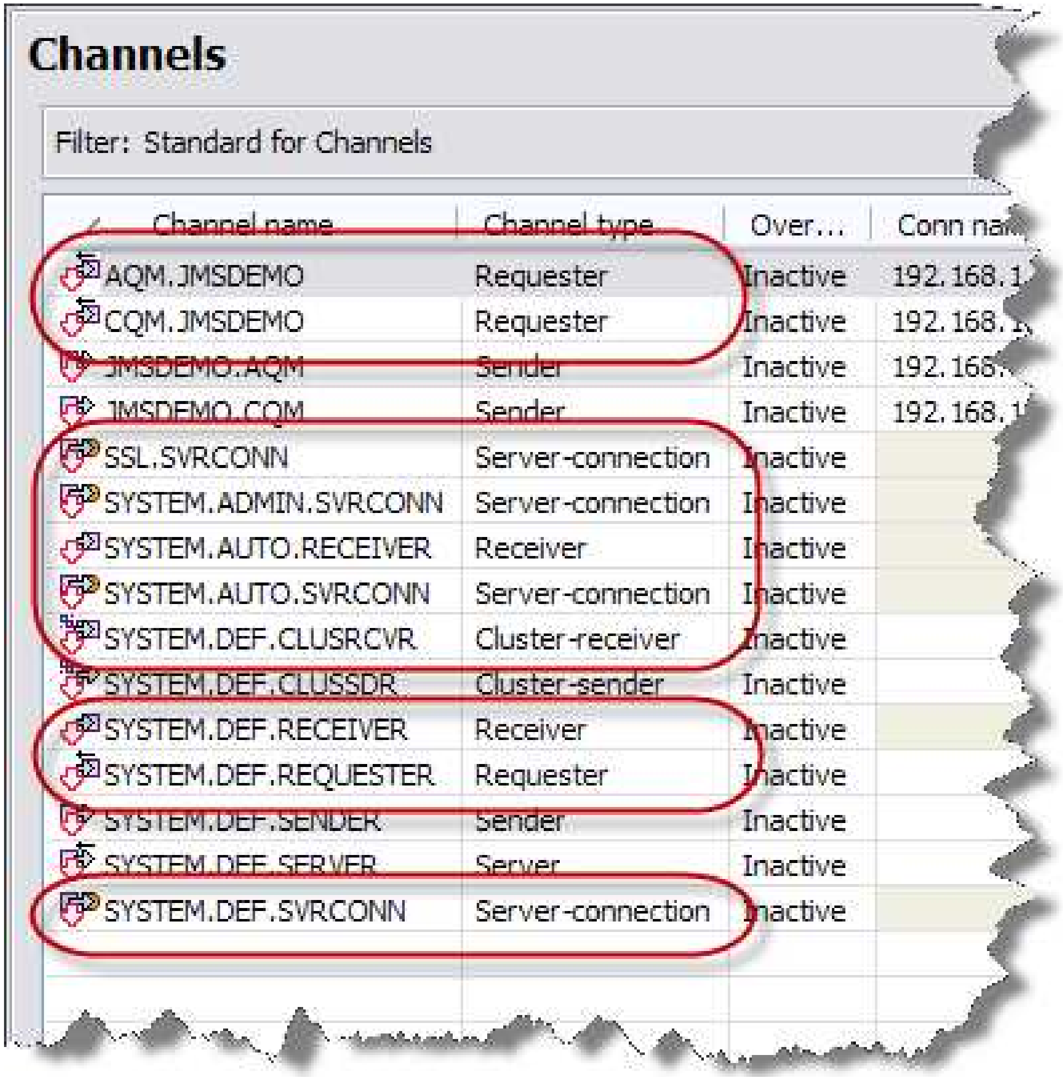
□ Accept only certificates with Distinguished Names matching these values:

Authentication of parties initiating connections: Required

A blank value here means SSL is not enabled.

This value causes CCL clients to present vcertificates for authentication.

Assessment using WebSphere MQ Explorer



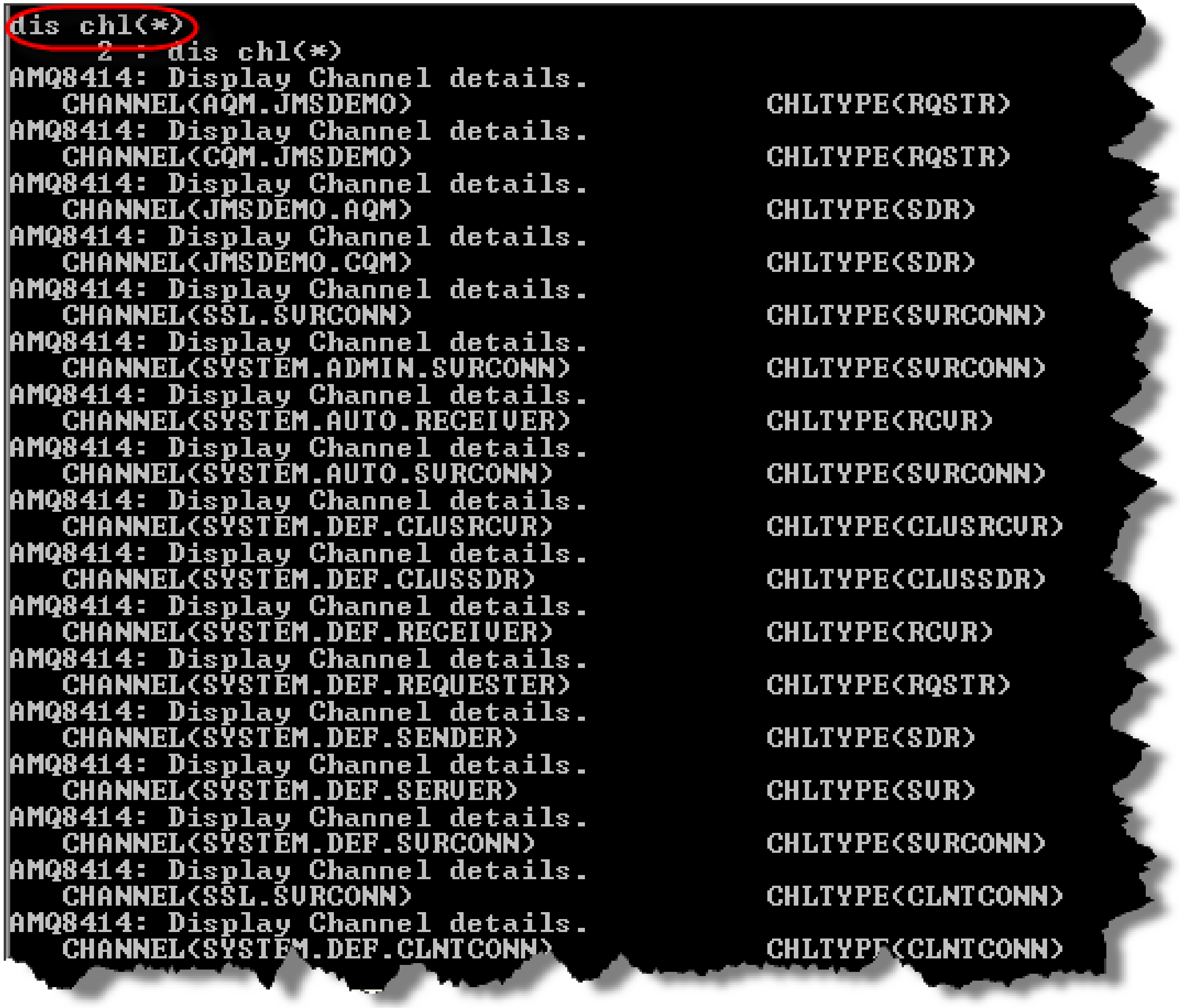
Channels

Filter: Standard for Channels

Channel name	Channel type	Over...	Conn na
AQM.JMSDEMO	Requester	Inactive	192.168.1
CQM.JMSDEMO	Requester	Inactive	192.168.1
JMSDEMO.AQM	Sender	Inactive	192.168.
JMSDEMO.CQM	Sender	Inactive	192.168.1
SSL.SVRCONN	Server-connection	Inactive	
SYSTEM.ADMIN.SVRCONN	Server-connection	Inactive	
SYSTEM.AUTO.RECEIVER	Receiver	Inactive	
SYSTEM.AUTO.SVRCONN	Server-connection	Inactive	
SYSTEM.DEF.CLUSRCVR	Cluster-receiver	Inactive	
SYSTEM.DEF.CLUSSDR	Cluster-sender	Inactive	
SYSTEM.DEF.RECEIVER	Receiver	Inactive	
SYSTEM.DEF.REQUESTER	Requester	Inactive	
SYSTEM.DEF.SENDER	Sender	Inactive	
SYSTEM.DEF.SERVER	Server	Inactive	
SYSTEM.DEF.SVRCONN	Server-connection	Inactive	

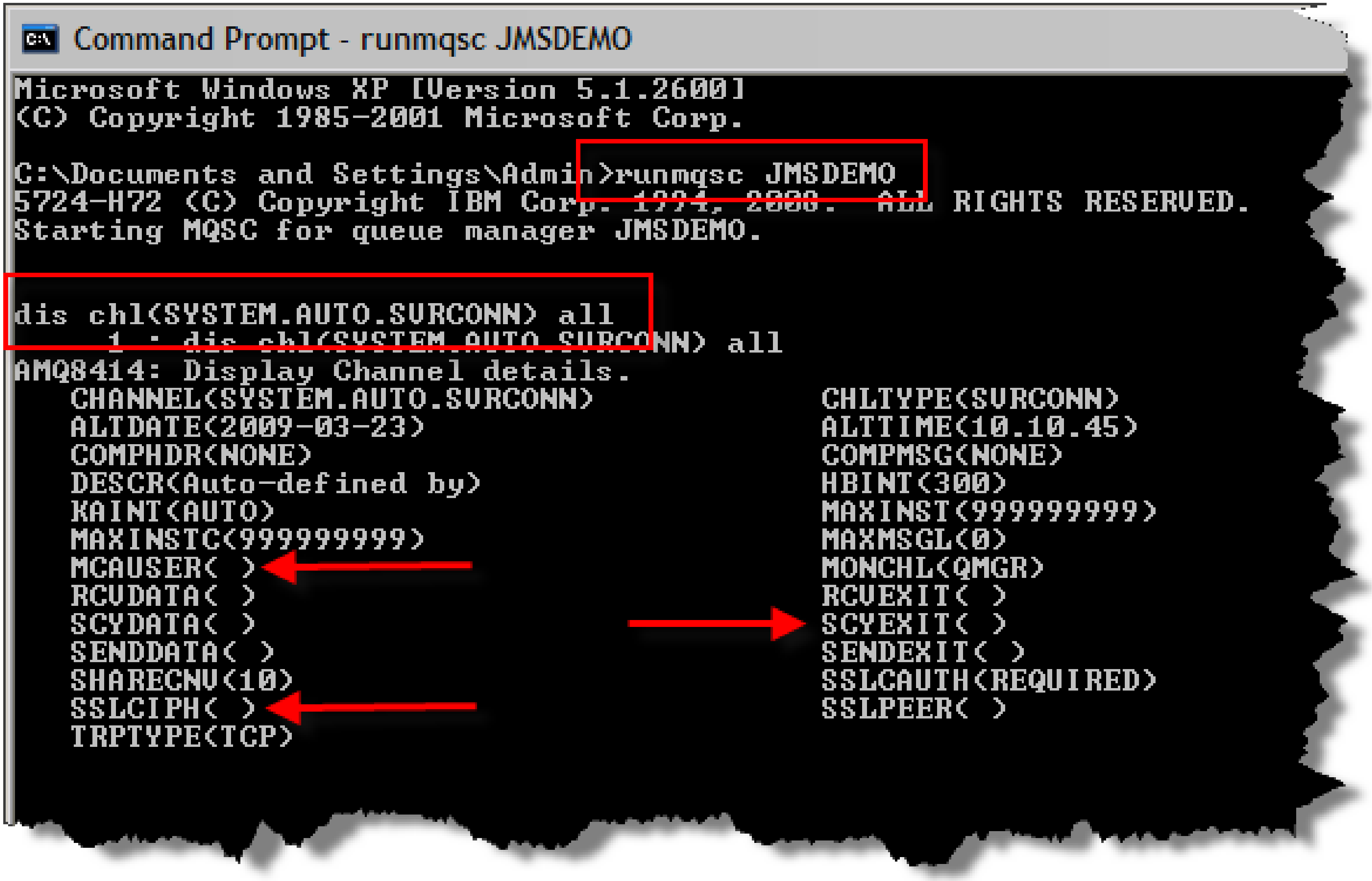
Assessment at the command line

Use the display Channels command **DIS CHL(*)** to list the channels and their types.



```
dis chl(*)
     2 : dis chl(*)
AMQ8414: Display Channel details.
   CHANNEL(AQM.JMSDEMO)                       CHLTYPE(RQSTR)
AMQ8414: Display Channel details.
   CHANNEL(CQM.JMSDEMO)                       CHLTYPE(RQSTR)
AMQ8414: Display Channel details.
   CHANNEL(JMSDEMO.AQM)                       CHLTYPE(SDR)
AMQ8414: Display Channel details.
   CHANNEL(JMSDEMO.CQM)                       CHLTYPE(SDR)
AMQ8414: Display Channel details.
   CHANNEL(SSL.SVRCONN)                       CHLTYPE(SVRCONN)
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.ADMIN.SVRCONN)              CHLTYPE(SVRCONN)
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.AUTO.RECEIVER)              CHLTYPE(RCVR)
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.AUTO.SVRCONN)               CHLTYPE(SVRCONN)
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.DEF.CLUSRCVR)               CHLTYPE(CLUSRCVR)
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.DEF.CLUSSDR)                CHLTYPE(CLUSSDR)
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.DEF.RECEIVER)               CHLTYPE(RCVR)
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.DEF.REQUESTER)              CHLTYPE(RQSTR)
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.DEF.SENDER)                 CHLTYPE(SDR)
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.DEF.SERVER)                 CHLTYPE(SVR)
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.DEF.SVRCONN)                CHLTYPE(SVRCONN)
AMQ8414: Display Channel details.
   CHANNEL(SSL.SVRCONN)                       CHLTYPE(CLNTCONN)
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.DEF.CLNTCONN)               CHLTYPE(CLNTCONN)
```

Assessment at the command line



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Admin>runmqsc JMSDEMO
5724-H72 (C) Copyright IBM Corp. 1994, 2008.  ALL RIGHTS RESERVED.
Starting MQSC for queue manager JMSDEMO.


dis chl(SYSTEM.AUTO.SVRCONN) all
     1 : dis chl(SYSTEM.AUTO.SVRCONN) all
AMQ8414: Display Channel details.
   CHANNEL(SYSTEM.AUTO.SVRCONN)            CHLTYPE(SVRCONN)
   ALTDATE(2009-03-23)                     ALTTIME(10.10.45)
   COMPHDR(NONE)                           COMPMSG(NONE)
   DESCR(Auto-defined by)                  HBINT(300)
   KAINT(AUTO)                             MAXINST(999999999)
   MAXINSTC(999999999)                     MAXMSGL(0)
   MCAUSER( )                              MONCHL(QMGR)
   RCVDATA( )                              RCVEXIT( )
   SCYDATA( )                              SCYEXIT( )
   SENDDATA( )                             SENDEXIT( )
   SHARECNV(10)                            SSLCAUTH(REQUIRED)
   SSLCIPH( )                              SSLPEER( )
   TRPTYPE(TCP)
```

Determining the queue manager version

Use the dspmqver command to display the installed version.

```
C:\Documents and Settings\Admin>dspmqver
Name:          WebSphere MQ
Version:       7.0.0.0
CMVC level:    p000-L080610
BuildType:     IKAP - (Production)
```

Acceptable versions are V5.3.14 (although out of support) and V6.0.2.2 and higher, including all releases of V7.0.x.x.

There can be only one version of WebSphere MQ installed on any server or OS image, LPAR, zone, etc., regardless of how many queue managers are defined there.

For more information

The Deep Queue: A podcast about WebSphere MQ security

- http://feeds2.feedburner.com/t-rob/deepqueue

Store and Forward Messages – WebSphere MQ security blog

- http://t-rob.net

developerWorks WebSphere Technical Journal

- Mission:Messaging column - http://is.gd/2Npo
- WebSphere MQ security heats up - http://is.gd/sgTC

The author’s presentations and papers

- Internal - http://ausgsa.ibm.com/~trwyatt/
- Public – http://www.t-rob.net/links

E-mail: t.rob.wyatt@us.ibm.com
Twitter: http://twitter.com/deepqueue and http://twitter.com/tdotrob
LinkedIn: http://www.linkedin.com/in/tdotrob

Appendix

Legal

IBM, the IBM logo, the e-business logo and other IBM products and services are trademarks or registered trademarks of the International Business Machines Corporation, in the United States, other countries or both. References in this publication to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates.

Product release dates and/or capabilities referenced in this publication may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

Microsoft, Windows, Windows NT and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries or both.

All other trademarks, company, products or service names may be trademarks, registered trademarks or service marks of others.