Session Number: 1259

# MQ Security 101: Administrative Hardening

**T.Rob Wyatt (t.rob.wyatt@us.ibm.com)**

**IBM Software Services for WebSphere**

IBM Software

Impact2011

Changing the Way Business and
IT Leaders Work

Optimize for Growth. Deliver Results.

# WebSphere MQ Security: Administrative Hardening

June 2008

WebSphere software

T.Rob Wyatt, WebSphere MQ Security Focused Practice

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

@business on demand software

Last update: 4 April, 2011

# 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/
  - Available externally at https://t-rob.net/links
  - Subscribe to updates at https://t-rob.net/mailman/listinfo/deepqueue_t-rob.net
- Related presentations
  - We assume you've seen or are familiar with
    - Core Concepts (From the WAS Security Presentation Series)
  - You may be interested in
    - WAS Security Presentation Series available internally at http://pokgsa.ibm.com/~keys/documents/securitySeries

Download

Subscribe

# 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 6.0 & 7.0 w/ some future speculation
- This will be revised as we learn more
- Your thoughts and ideas are welcome

# Agenda

- Welcome!
  - Objectives
  - Scope
- Demo
- Some security terms
- Concepts – As applied to WebSphere MQ
- Special considerations
- Checklist
- Resources

# Objectives

"Is my queue manager configured to allow anonymous administrative access?"

This presentation is designed to provide:

- Skills and knowledge to accurately answer the question above and…
- The ability to do something about it if the answer is "yes"!

# Scope

- The presentation covers…
- WebSphere MQ on distributed platforms
- Version 6.x, 7.x
- Messages originating locally
- Messages arriving over a channel, regardless of the originating platform

- Not covered:
  The specifics of securing WebSphere MQ on Z/OS, iSeries and NSK are beyond the scope of this session. Although much of the material is directly applicable, there are additional platform-specific considerations pertaining to security on each of these platforms.

# Agenda

- Welcome!
- Demo
  - Code examples
  - Service and user accounts
  - Channel and MCAUSER
  - Common use cases:
  - Impersonation
- Some security terms
- Concepts – As applied to WebSphere MQ
- Special considerations
- Checklist
- Resources

# Breaking in is easy if the door is open…

What follows are two examples of how to impersonate the mqm User ID using the MQI channel.

Don't blink, you might miss it.

# User Impersonation in Java/JMS

Java code:

```
MQEnvironment.userID = "mqm";
MQEnvironment.password = "any";
```

JMS code:

```
cf.createConnection("mqm", "any");
```

See:
*WebSphere MQ Using Java* in the v6.x or v7.x Information Center

# User impersonation over SSL Channels

Same technique as the previous slide!

SSL begins and ends with the connection handshake. The Message Channel Agent does not directly use any information that is available from the context of the SSL session. SSL does not affect anything at the API layer.

Therefore…

- SSL allows us to authenticate the remote node.
- But we still do not have a trusted identity for API calls.

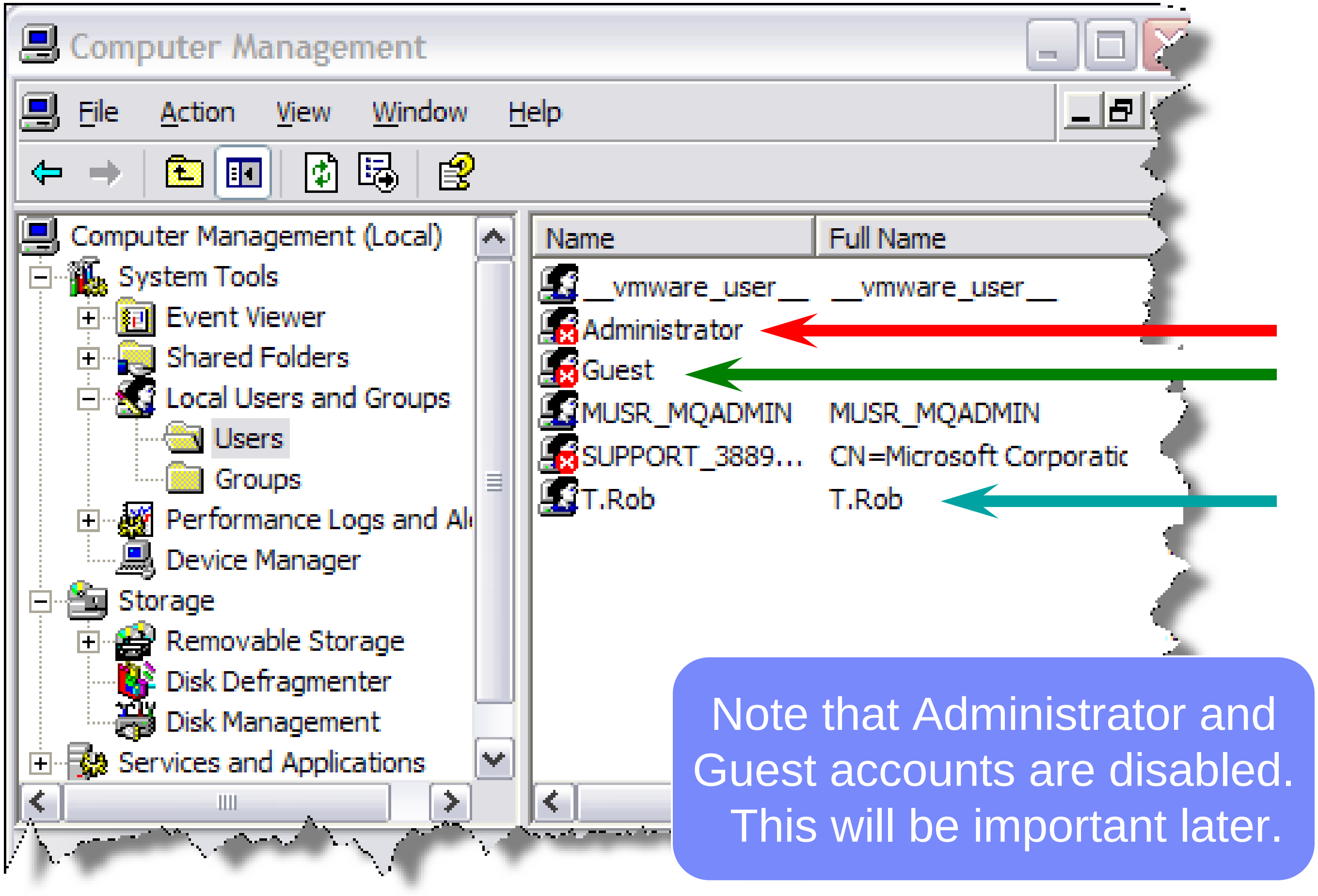
# Demo – Channel and MCAUSER

```
dis chl(SYSTEM.DEF.SVRCONN) MCAUSER
     1 : dis chl(SYSTEM.DEF.SVRCONN) MCAUSER SCYEXIT
AMQ8414: Display Channel details.
  CHANNEL(SYSTEM.DEF.SVRCONN)
  CHLTYPE(SVRCONN)
  MCAUSER( )
  SCYEXIT( )
```

**Any channel without an MCAUSER value allows user impersonation and administrative authority.**

MCAUSER may be set statically or by a security exit. Since neither MCAUSER nor SCYEXIT are set in this example, the channel allows administrative access.

# Demo – Service and user accounts



| Name | Full Name |
|---|---|
| __vmware_user__ | __vmware_user__ |
| Administrator | |
| Guest | |
| MUSR_MQADMIN | MUSR_MQADMIN |
| SUPPORT_3889... | CN=Microsoft Corporatic |
| T.Rob | T.Rob |

Root access!

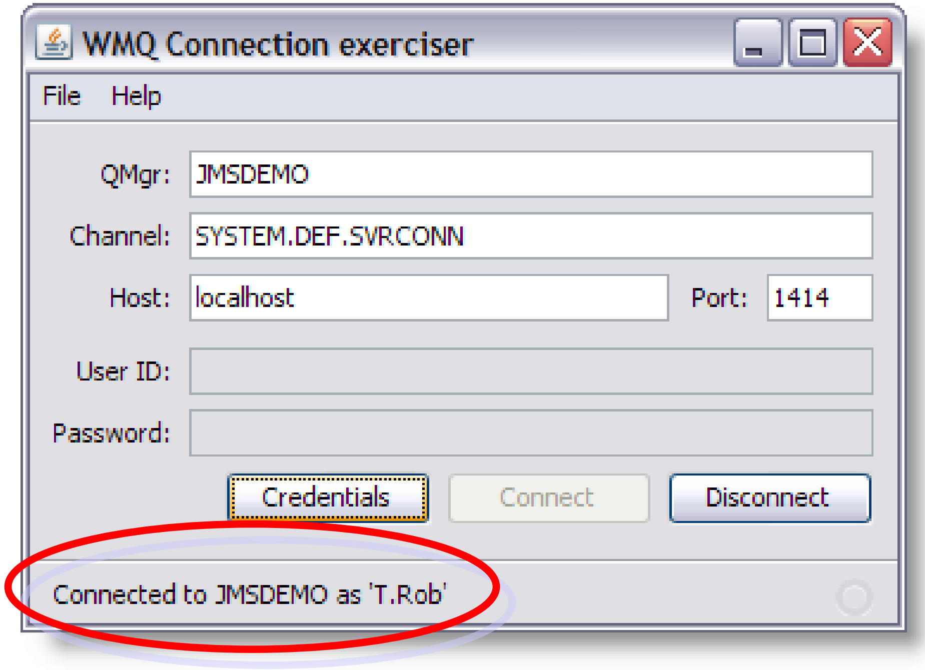
Low-privileged account

My user account

Note that Administrator and Guest accounts are disabled. This will be important later.

# Demo – Common use cases

Intended use:
User ID is passed and authorized to WebSphere MQ



QMgr: JMSDEMO

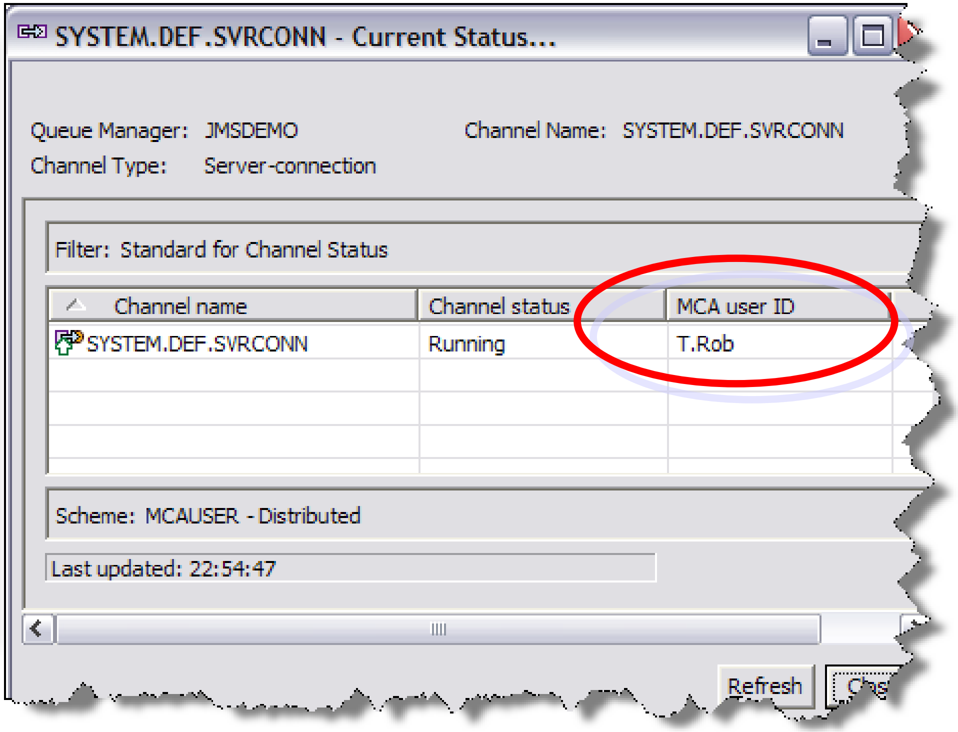
Channel: SYSTEM.DEF.SVRCONN

Host: localhost Port: 1414

User ID:

Password:

Connected to JMSDEMO as 'T.Rob'



Queue Manager: JMSDEMO Channel Name: SYSTEM.DEF.SVRCONN

Channel Type: Server-connection

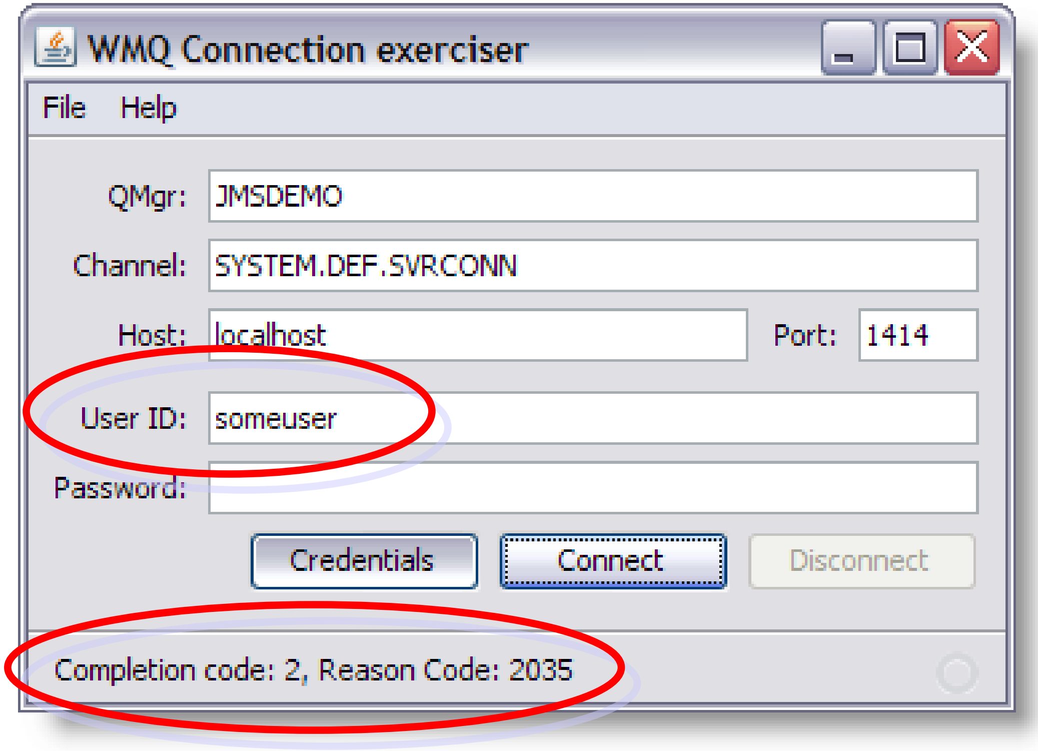
Filter: Standard for Channel Status

| Channel name | Channel status | MCA user ID |
|---|---|---|
| SYSTEM.DEF.SVRCONN | Running | T.Rob |

Scheme: MCAUSER - Distributed

Last updated: 22:54:47

# Demo – Common use cases



QMgr: JMSDEMO

Channel: SYSTEM.DEF.SVRCONN

Host: localhost

Port: 1414

User ID: someuser

Password:

Completion code: 2, Reason Code: 2035

When the user ID is unknown to the WMQ host, the connection fails.

If the ID exists but is not authorized, the connection fails.

Do NOT solve this by placing the user ID in the mqm group!

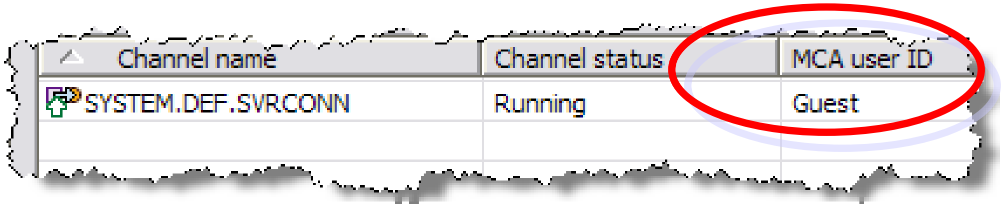
# Demo – Common use cases

User ID is added to host and placed in an authorized group that does NOT have administrative privileges. The group is then authorized to MQ.

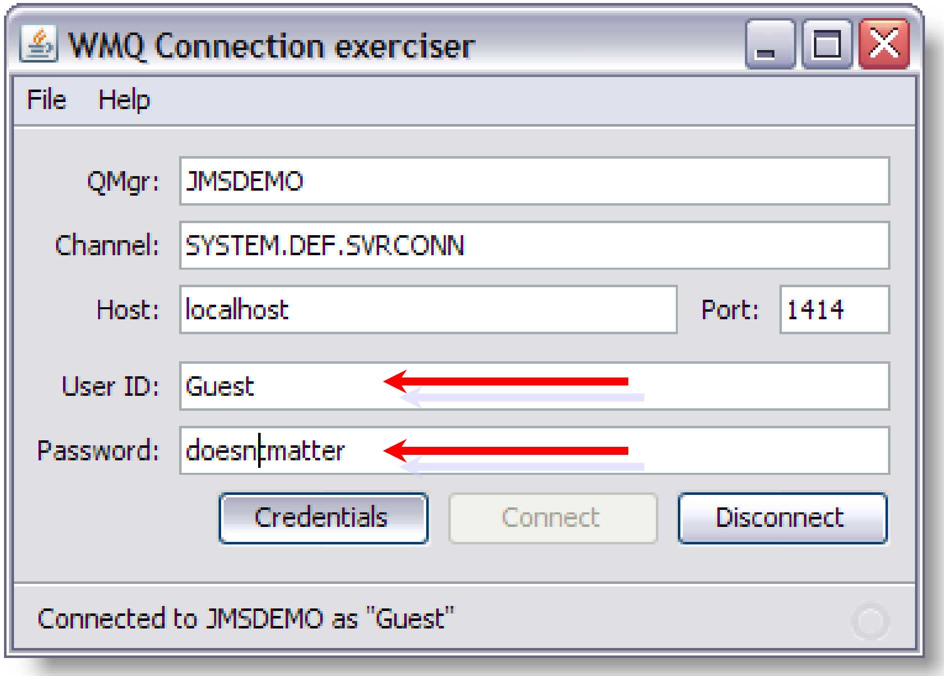
We now connect as “Guest”.

Recall that this account is disabled. Note also that the password literally DOESN’T MATTER since it is not checked. The password field is available for use by an exit but is not used by the MCA.

We can take advantage of this behavior. Service accounts do NOT need to be enabled, they only need to exist in the correct group. This reduces exposure.



| Channel name | Channel status | MCA user ID |
|---|---|---|
| SYSTEM.DEF.SVRCONN | Running | Guest |



WMQ Connection exerciser

QMgr: JMSDEMO
Channel: SYSTEM.DEF.SVRCONN
Host: localhost Port: 1414
User ID: Guest
Password: doesntmatter

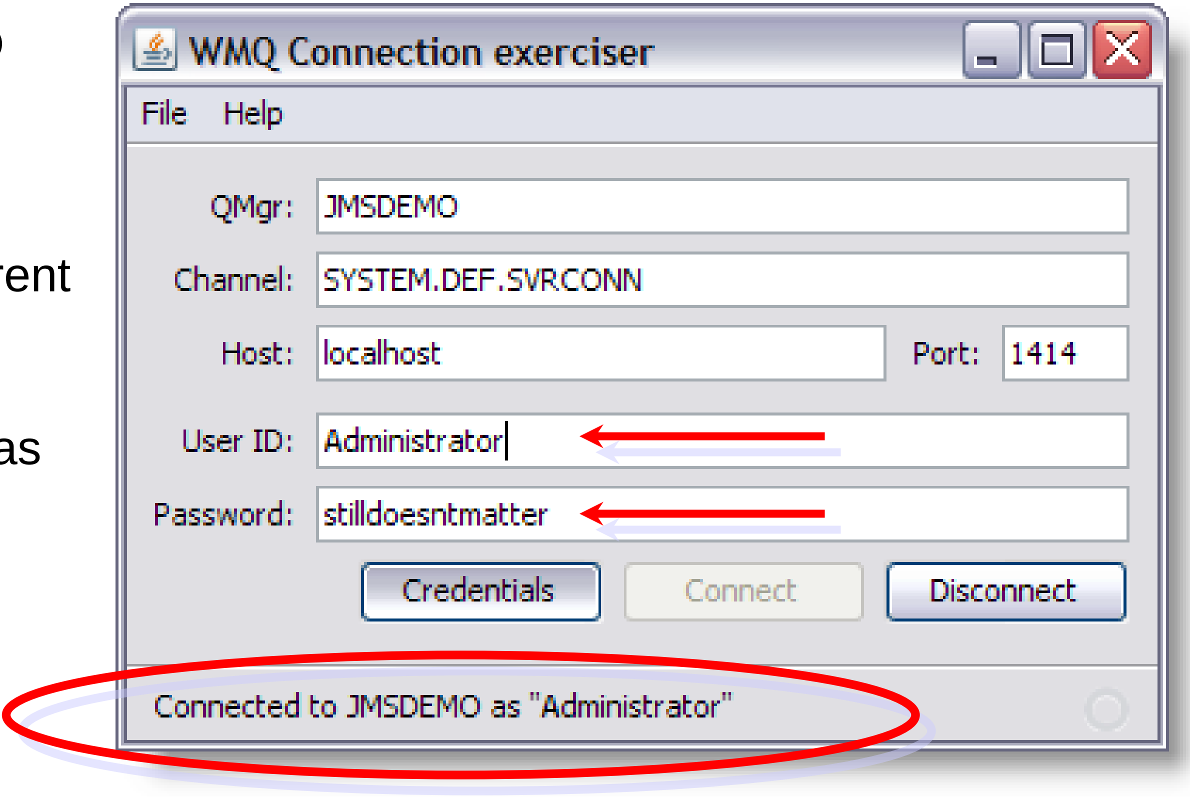
Connected to JMSDEMO as "Guest"

# Impersonation – Assert any arbitrary ID

We've been performing ID assertion throughout the demo!

But what if we pick a different account?

Here we have connected as the local Windows administrator.



QMgr: JMSDEMO

Channel: SYSTEM.DEF.SVRCONN

Host: localhost

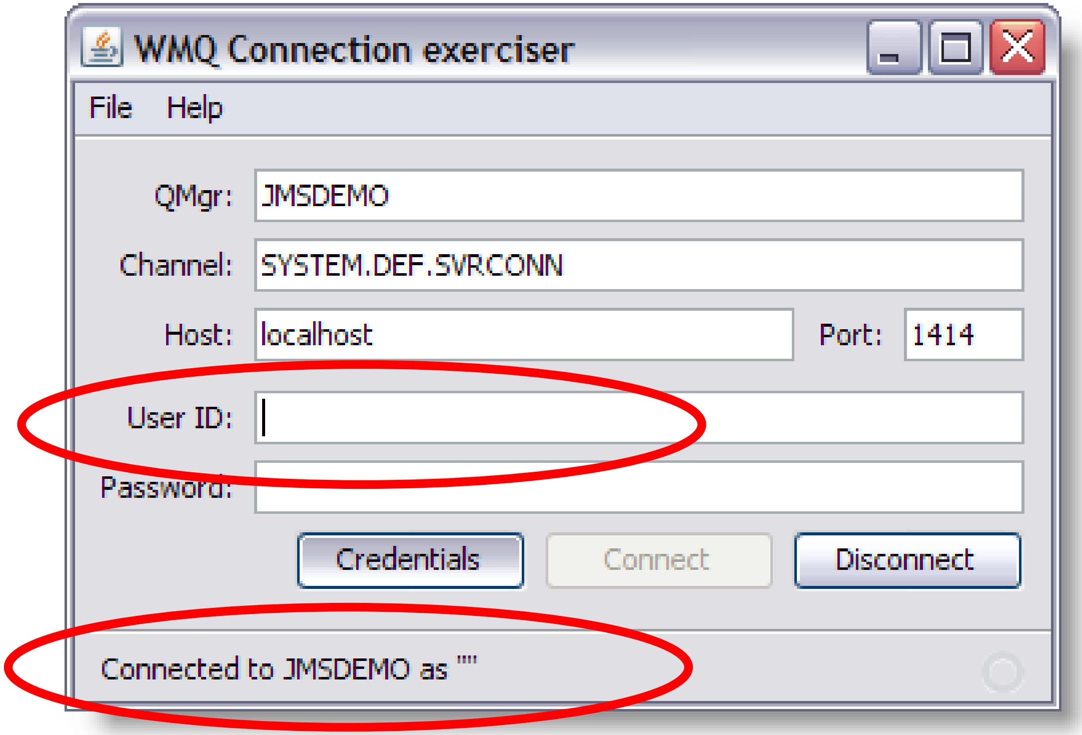
Port: 1414

User ID: Administrator

Password: stilldoesntmatter

Connected to JMSDEMO as "Administrator"

# Impersonation – Assert a blank ID



QMgr: JMSDEMO

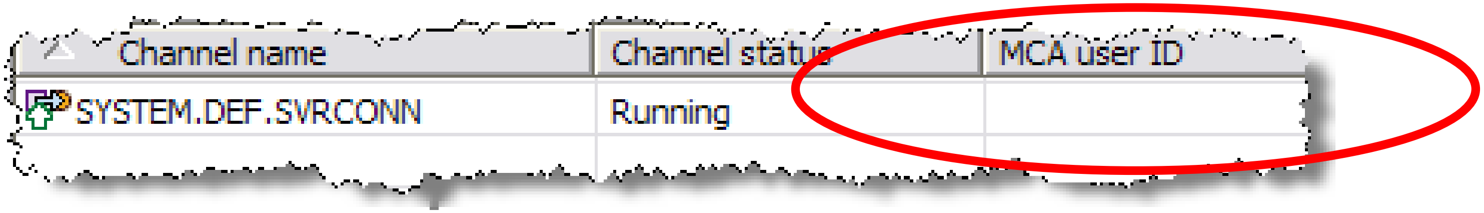
Channel: SYSTEM.DEF.SVRCONN

Host: localhost Port: 1414

User ID:

Password:

Connected to JMSDEMO as ""



| Channel name | Channel status | MCA user ID |
|---|---|---|
| SYSTEM.DEF.SVRCONN | Running | |

What if we specify NO account (blanks or null)?

The channel now runs with the privileges of the MCA process – the same account that MQ is running as!

# How can impersonation be exploited?

- Access any application’s queues
- Access the command server to create, change or delete objects
- Start/stop channels, listeners, processes
- Define and execute services
  - Can run any arbitrary OS command as mqm.
  - Does not depend on a trigger monitor or other external process. This is built in as of WMQ v6.0 and cannot be disabled.
- Can probably gain administrative access to any adjacent queue managers. In the cluster, ALL queue managers are adjacent.

# Call to action!

We are NOT giving away the keys to the castle here. Asserting any ID over a client channel is part of the API. It is documented.

Securing the client channel is also documented.

The people who would use this against you already know it or could easily find it if motivated.

Assume your systems are a target and take action now to protect them!

# Agenda

- Welcome!
- Demo
- Some security terms
  - Authentication
  - Authorization
  - Authorization Domain
  - Cross-domain Authentication
- Concepts – As applied to WebSphere MQ
- Special considerations
- Checklist
- Resources

# Concepts - Authentication

Provides some level of assurance that an identity presented is genuine.

- May be weak such as simple assertion.
- Challenge-response authentication such as the traditional ID and password is better.
- Credentials such as X509 certificates may be used
- Multi-factor authentication combines two or more methods.

# Concepts - Authorization

Access to resources is based on rules and credentials.

- Default access can be "allow all" or "deny all".
- Deny all by default is  best!
- More specific access rules then extend the default policy.
- Local connections default to deny all.
- Remote connections default to allow all!

# Notes

For local bindings-mode connections, the WebSphere MQ security model defaults to “deny all”.

For messages arriving over channels, WebSphere MQ security effectively defaults to “allow all”.  At one point, remote messaging defaulted to “deny all” but customers raised many PMRs and ease of use issues so eventually it was changed.  At that time, the manuals were updated with recommendations to modify the default settings for Production systems or anywhere else where security is a requirement.

Since WMQ will attempt to pass the user’s local ID and can generate an authorization error, the perception is that remote connections are authenticated when in fact they are not.  The ID presented is accepted at face value.

A password field exists in the connection descriptor and is exposed in WMQ Explorer as of v7.  This field makes the password available to exits but is not used by base WMQ.

# Concepts – Authentication Domain

Provides the context within which an identity can be verified.

Examples include:

- Network Information Service (NIS)
- Windows® Active Directory
- Certificate authority
- Tivoli Federated Identity Manager (TFIM)

# Notes

Example: Two Unix queue managers in the same NIS+ domain share a common set of user identities.

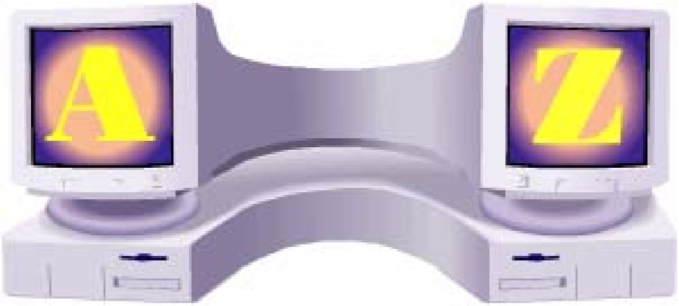
Similarly, two Windows® queue managers in the same Active Directory domain also share a common set of user identities.

If the same ID exists in both the Unix NIS+ domain and the Windows Active Directory domain there is no assurance that both versions of the ID are assigned to the same individual.

Furthermore, without authentication, there is no guarantee that the ID presented even originated in one of those two domains.

# Concepts - Cross Domain Authentication

- Authentication occurs remotely.
- Authorization is performed locally.
- The remote identity is accepted at face value.



The authentication domain must be trusted.

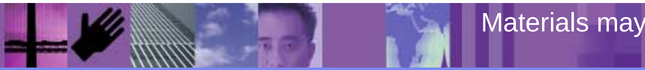
The authentication domain must itself be authenticated.

# Concepts – As applied to WebSphere MQ

The next slides discuss how these concepts are implemented within WebSphere MQ.

# Agenda

- Welcome!
- Demo
- Some security terms
- Concepts – As applied to WebSphere MQ
  - Authentication
    - Bindings mode authentication
    - Authentication of Remote QMgrs
    - Client authentication
    - Remote authentication – SSL
    - Command server
    - Notes on MCAUSER
  - Authorization
- Special considerations
- Checklist
- Resources



# WebSphere MQ Authentication

## WebSphere MQ does not authenticate.

- WebSphere MQ **authorizes** based on the user ID associated with the process that connects to it but does not authenticate that ID in any way.
- In bindings mode, that ID is an application service account (usually) which has been authenticated by the operating system..
- For any remote connection, the ID is that of the Message Channel Agent.
  - The MCA will *attempt* to assert an ID associated with the message or connection.
  - If no such ID is available, the MCA will by default PUT messages with full administrative authority.
- We can improve authentication through system configuration or security exits.

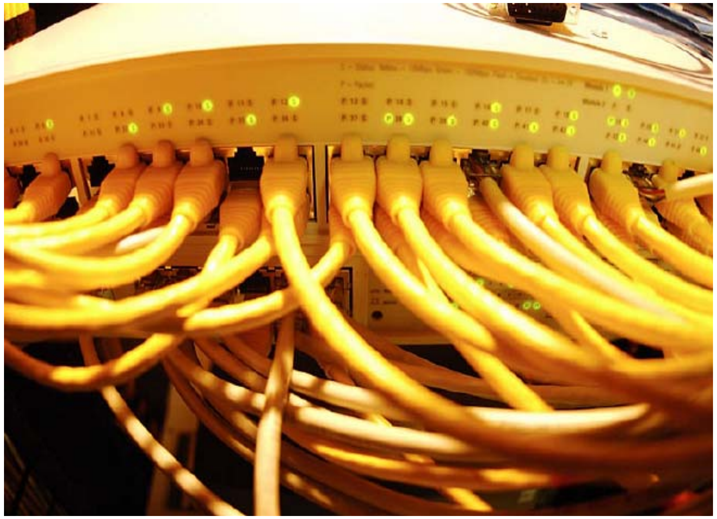
# Bindings-mode Authentication

- Relies on the underlying Operating System.
- Based on the User ID associated with the process that connected to the queue manager.

- Strategies:
- Physical server security
- Restricted root access
- Limit membership to administrative groups

# Authentication of Remote QMgrs

Occurs at the link level.



Strategies:

- MCAUSER
- SSL
- Exits
- LOCLADDR
- Message-level authorization method defined in the channel’s PUTAUT() attribute but does not authenticate in any way.
- WMQ AMS combines link- and message-level authentication.

**Any channel without an MCAUSER value allows user impersonation and administrative authority. If there is no SSL or exit, that authority is granted to anonymous users.**

# Notes

MCAUSER – Forces all messages arriving over a channel to use the same authorization profile.  The ID in MCAUSER should be in a low-privileged group and can be a non-login service account.

SSL – Link-level authentication used to verify that inbound connections originate from authorized systems.  Does not prevent administrative access or guarantee that any specific ID is used for API calls.  MUST set SSLCAUTH and SSLPEER or use an exit to enable authentication!

Security exits – May implement any arbitrary authentication at the link level.  The user ID is then placed by the exit into the MCAUSER field of the channel where it is used for API authorization.

LOCLADDR – Bind a SDR/SVR/CLUSSDR channel to a specific network interface. Use this feature on gateway QMgrs to prevent external connections to internal-facing channels.

API-level authorization method defined in the channel's PUTAUT() attribute.
PUTAUT(DEF) – Messages are put with administrative authority or authority of MCAUSER based on the MQMD.UserID value.  The MQMD.UserID is not authenticated in any way and may be an administrative ID.

PUTAUT(CTX) – ID from the MQMD is used the check authorization during PUT. The ID is accepted at face value.

WMQ AMS combines link- and message-level authentication.

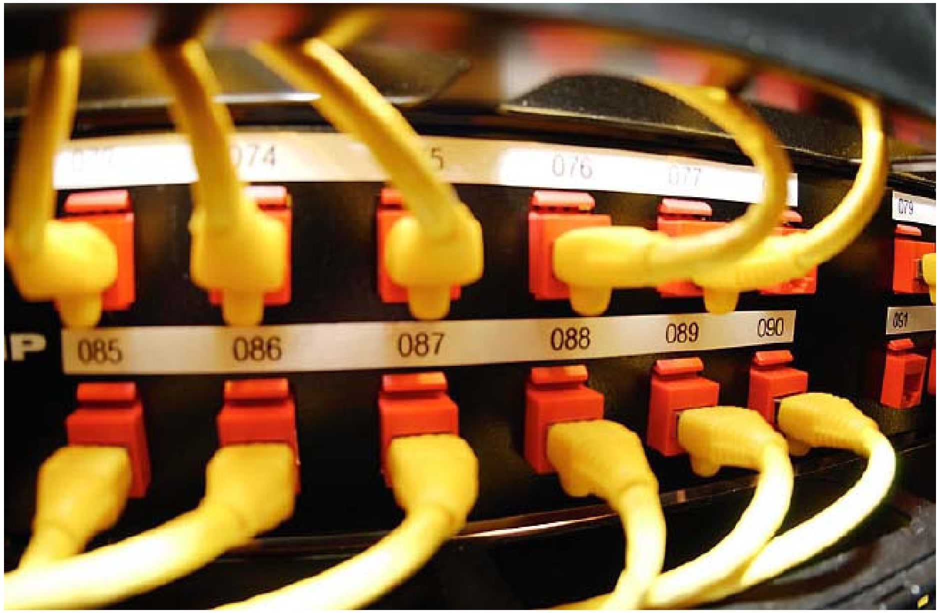
# WebSphere MQ Client Authentication

This page intentionally left blank.

# WMQ Client Authentication – Take 2

Strategies:

- MCAUSER
- SSL
- Exits
- SSL/Exit combo
- WMQ AMS



**Any channel without an MCAUSER value allows user impersonation and administrative authority**

# Remote authentication - SSL

SSL provides assurance that an MQI channel was started by someone who possesses a valid certificate.

SSL does not prevent that user from asserting an arbitrary user ID. Set MCAUSER statically or with a security exit to associate a specific identity with a certificate.

Without SSLPEER, any certificate issued by a trusted signer will be accepted! Set SSLPEER on the channel and delete unneeded certificate authorities from the trust store.

**Any channel without an MCAUSER value allows user impersonation and administrative authority.**

**Even over an SSL-protected channel.**

# Command Server authentication

*The command server does not authenticate!*

It performs authorization checks based on the ID in the message header. But the ID presented is not authenticated in any way. If the ID is privileged, any command requested will be executed.

Strategy – make sure command messages originate from known sources and enforce the MQMD.UserID value.

- Low-privileged MCAUSER on all inbound channels.
- Strongly authenticate administrative IDs.

# Notes on MCAUSER

- Can be set statically in the channel definition.
- Can be set dynamically by an exit. In this case, configure the channel with MCAUSER('\$\!  \&\#') and let the exit override this value.
- Exit can be arbitrarily complex.
  - Filter by IP address
  - Credential exchange
  - Cryptographic tokens
  - Anything you want
- Coding a security exit is not trivial.

# Agenda

- Welcome!
- Demo
- Some security terms
- Concepts – As applied to WebSphere MQ
  - Authentication
  - Authorization
    - Object Authority Manager
    - Interactive users
    - Application service IDs
    - QMgr-to-QMgr
- A Note About Transmit Queues
- Checklist
- Resources

# Object Authority Manager

We know we need to set MCAUSER…now what?

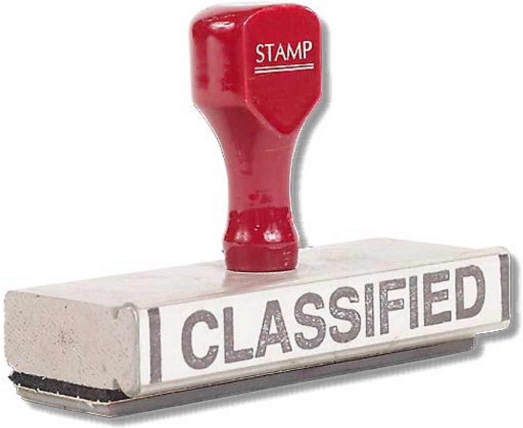
Three different cases to consider…

1. Interactive users
2. Application service accounts
3. QMgr-to-QMgr connections

Each category has different requirements.

# OAM: Interactive users

Make sure the MQI (SVRCONN) channel has a value in the MCAUSER and authorize it appropriately!



Do not routinely grant…

- CREATE
- DELETE
- CHANGE
- CONTROL
- CONTROLX
- Queue Manager SET

These authorizations confer administrative authority to create, delete or change objects, to start or stop channels or services or to manage authorizations.

This population of identities and the associated access policies are very dynamic. Ongoing administration can be expensive. Consider using a central tool for interactive WMQ access to reduce this expense.

# OAM: Application service IDs

- Do not over-authorize with OAM!
- ALTUSR and SETID are administrative privileges. Do not grant these routinely.
  - ALTUSR: Perform API calls with authority of another user - possibly as admin user.
  - SETID: The user ID in the message header may be set to any value.
- SET on the QMgr: Allows administration of authorization profiles.

For this population, the policies are fairly static but the identities tend to be volatile, especially for service oriented applications. Volume of message traffic becomes a consideration as well. Primary costs for this population are the overhead of managing the identities and policies, and the CPU overhead of cryptographic authentication.

# OAM: Application service IDs

Most applications need only PUT or GET/BROWSE and INQUIRE. (JMS applications *always* need INQUIRE.)

Attacks on the command queue can generate orphan reply messages which route to the Dead Letter Queue. Applications should always have PUT access to the DLQ but not GET access since this would allow an attacker to wipe out traces of the attack. Provide application-specific exception queues to eliminate the need for applications to manage messages in the DLQ.

Keep in mind that setmqaut commands are cumulative. For example, after running the following two commands…

```
   setmqaut -m DEMO -n DEMO.QUEUE -t queue -g users +put
   setmqaut -m DEMO -n DEMO.QUEUE -t queue -g users +get
```

…the group ‘users’ has both put and get authority. To insure that the profile contains ONLY the permissions in the command, include `-all` at the beginning:

```
   setmqaut -m DEMO -n DEMO.QUEUE -t queue -g users -all +get
```

As a best practice, authorize groups (-g) rather than principals (-p). On UNIX systems, authorization is always by group even when –p is used. Using the –p setmqaut option can lead to unintended results, especially if the user is in multiple groups and/or the user’s primary group changes.

On Windows systems it is possible to authorize specific principals however these should be fully qualified with the domain. For example, authorize “–p user@domain” rather than “–p user” because the unqualified version is ambiguous.

# OAM: QMgr-to-QMgr

Setting MCAUSER on an inbound MCA channel (RCVR, RQSTR or CLUSRCVR) to a low-privileged ID enables the ability to restrict that channel using setmqaut commands.

To prevent administrative access from another QMgr:

- Do not authorize the channel to the Command Queue.
- Consider restricting access to the any XMit queues as well.
- Consider restricting access to the DLQ if you want the channel to stop when a message is addressed to an unauthorized destination.

QMgr-to-QMgr identities and policies are very stable. The primary cost is a periodic key management and the CPU overhead of cryptographic authentication. Depending on business requirements for privacy and data integrity, weak authentication which does not impose the cryptographic overhead may be acceptable. For example, two queue managers in the same rack on the same VLAN might authenticate by filtering inbound IP addresses.

# Notes

In addition to `+put +inq`, the ID needs `+setall` authority. This is an administrative right but the channel agent part of the queue manager.

Do NOT allow other users to be members of the group used by the MCAUSER ID and DO disable the account!

As of v7.0, the MCA channels apply authorizations when creating scratchpad objects (an internal MQ API call). This is done my checking authorization on SYSTEM.CHANNEL.SYNCQ. Early versions of v7 required +crt authority on S.C.SQ, which makes the MCAUSER administrative. The current version requires only +put so apply the latest Fix Pack! This should revert to v6 behavior (no special access required on S.C.SQ) with 7.0.1.4 according to IZ78326.

# OAM: Using generic Profiles

- SETALL contains SETID.
- ALLMQI grants ALTUSER and SETALL.
- ALLADMIN grants all the non-MQI privileges.
- ALL grants everything.

The generic OAM settings ALL, ALLADM, ALLMQI, SETALL and PASSALL confer administrative privileges and should not be granted routinely – although they often are!

# Notes

We have ALL, ALLADM and ALLMQI but there is no generic grouping that represents “ALL_SAFE_API_COMMANDS”. All of the generic authorizations contain administrative privileges of some kind.

When in doubt, run a simple test. For example, let’s see what is contained in +allmqi:

```
setmqaut -m DEMO -n "DEMO.QUEUE.**" -t queue -g users +allmqi
The setmqaut command completed successfully.
dspmqaut -m DEMO -n "DEMO.QUEUE.**" -t queue -g users
Entity users has the following authorizations for object DEMO.QUEUE.**:
        get
        browse
        put
        inq
        set
        passid
        passall
        setid
        setall
```

Note the quotes around the profile specification. These prevent the shell from expanding the asterisks in the profile into file names. Without the quotes the command works fine until and unless one or more file names in the current directory happens to match the OAM profile specification. At that point the command will fail with unexpected and strange results.

- Welcome!
- Demo
- Some security terms
- Concepts – As applied to WebSphere MQ
- Special considerations
  - A Note About Transmit Queues
  - PUTAUT – Put Authority for channels
  - Clustered topics in v7.0
- Checklist
- Resources

# A Note About Transmit Queues

Authorization to a transmit queue enables the user to PUT to *any* queue accessible from that transmit queue.

In the case of the cluster transmit queue that means the user can PUT to any queue in the cluster, whether it is advertised to the cluster or not.

Restrict at the sender side with aliases or QRemotes.  Restrict at the receiver side with MCAUSER.

# PUTAUT – Put Authority for channels

The exception to the previous slide is when PUTAUT(CTX) is enabled. In this case, messages are PUT on the receiving side with the authority of the ID in the MQMD. Because PUTAUT(CTX) requires all QMgrs to be in the same authentication domain, it is not usually practical in a mixed platform environment and therefore is seldom used.

The alternative to authorizing the XMitQ is that a QRemote or QAlias is required for EVERY authorized remote destination. The OAM privileges are then granted on the locally defined QRemote and QAlias objects.

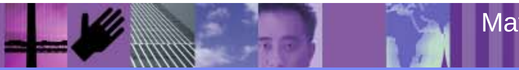
# Clustered Topics in WMQ v7.0

The exception to the rule about authorizing only locally defined objects is clustered topics. Topics became full-fledged WebSphere MQ objects as of v7.0. In addition, authorization profiles may be enforced on topics that are advertised in a cluster, regardless of where they are defined.

For example, consider a cluster with three queue managers A, B and C. If a topic is defined on QMGRA and advertised to the cluster, it is visible on QMGRB and QMGRC. Furthermore, SETMQAUT commands on QMGRB and QMGRC will be enforced against local publications or subscriptions to that clustered topic.

# Agenda

- Welcome!
- Demo
- Some security terms
- Concepts – As applied to WebSphere MQ
- Special considerations
- Checklist
- Resources



# Security Assessment Checklist

1. Verify that the OAM is enabled in the ini files or registry when creating the QMgr.  Check for amqzfuma to be running.
2. Check to see who's in the mqm group (or the Windows equivalent - domain mqm, local mqm or administrators).
3. Verify that non-privileged users have not been granted +all, +allmqi, +alladm, +setid, +setall or, on the queue manager, +set.
4. Verify SVRCONN channels are effectively locked down with a low-privileged MCAUSER or strong authentication for admin users.

# Security Assessment Checklist

1) An attacker with OS-level access may simply disable the OAM. Verify that it is still active. The amqzfuma process should be running.

2) All IDs in administrative groups should be actual privileged users. Flag any users who should not have privileged access and clean up the group memberships. Watch out for nested groups on Windows. On Unix/Linux check both local files (/etc/group and /etc/passwd) as well as any LDAP, NIS, NIS+ or other distributed authentication domain.

3) Use dspmqaut –m:

```
dspmqaut –m VENUS
```

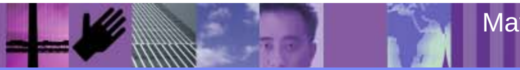
Look for any groups/users that have +all, +allmqi, +alladm, +setid or +setall. Look for +set on the queue manager since this controls the ability to set authorizations using PCF commands.

The +setid and +setall options allow the group/user to put any ID they want into the MQMD. These are also included in +all. Any group/user with +put +setid on the command queue has admin access. If they have +put +setid on any transmit queue, then they have access to whatever is on the other side of that XMit queue or, in the case of the cluster XMitQ, the whole cluster. See the note in Step 6 for exceptions.

The +alladm and its constituent settings as well as +set on the queue manager allow the use of PCF commands. Make sure that these are given with appropriate levels and only to appropriate groups/users.

4) This specifically includes SYSTEM.DEF.SVRCONN and SYSTEM.AUTO.SVRCONN (which is frequently overlooked). Admin access may be restricted by a low-privileged MCAUSER. Otherwise, SVRCONN channels must either use an exit or SSL to authenticate connections. If the channel is to be used by non-administrative users, an exit should be in place to reject connection requests bearing administrative credentials. Alternatively, an exit may dynamically set the MCAUSER based on some credential in the connection request. In this case, the MCAUSER in the channel definition should be set to 'nobody' as the exit will override it if working. Should the exit fail, the default is now ‘no access’ rather than ‘admin access’.

If SVRCONN channels are used for admin access, they may have a blank MCAUSER or some privileged ID in the MCAUSER. In this case, they must be protected so that only administrative users can connect. This usually means SSL with filtering on the certificate DN or it could be an exit or a combination of the two.



# Security Assessment Checklist

5. Do any inbound RQSTR, RCVR, or CLUSRCVR channels have blanks (or an administrative ID) in the MCAUSER? If so, repeat this exercise in its entirety on the adjacent queue manager(s). Better yet – set MCAUSER.
6. Verify that any channel identified in Step #5 authenticates its connections.
7. Verify that any SVR channels authenticate their inbound connection requests.

# Notes

5) In this case, any user of the remote QMgr who has admin access can administer the local queue manager. Similarly, any user with +put +setid privileges on the remote QMgr's XMitQ which leads to this QMgr also has admin access on this QMgr.

Optionally, an exit may be used to filter out messages with administrative IDs or destined for the Command Queue. WebSphere MQ Advanced Message Security may also be used to mitigate this risk.

Note: Any ID set in the MCAUSER of a classic or cluster channel must have some elevated rights. On the QMgr these are +connect, +inq and +setall. The ID must also have +put and +setall for the destination and dead-letter queues. For a CLUSRCVR, the ID requires these rights on the cluster command queue as well. It follows then that the ID must not be a logon ID or used by applications. It should be considered a non-login service ID that is owned by the WMQ admin team exclusively.

6) Does any channel identified in Step 6 allow anonymous connections? An inbound channel with admin privileges must authenticate the incoming connection. This requires an exit or SSL with filtering on the DN.

7) Are there any SVR channels defined (other than SYSTEM.DEF.SERVER)? If so, they must authenticate inbound connection requests. Again, this can be implemented using an exit or SSL with filtering on the DN. The SYSTEM.DEF.SERVER channel has no XMitQ defined and cannot be started by a RQSTR (assuming the QMgr is not compromised). SDR channels started by a RQSTR connect only to whatever is in their CONNAME so do not require the same protection as a SVR channel.

# Agenda

- Welcome!
- Demo
- Some security terms
- Concepts – As applied to WebSphere MQ
- Special considerations
- Checklist
- Resources

# Resources

## WebSphere MQ Advanced Message Security

- Extends the connection-level security described in this presentation to include message-level security.
- Provides a single authentication domain across the messaging network based on a certificate identity.
- Certificate identity is mapped to a locally relevant account even across unlike platforms.
- Does not impact application code.
- Z/OS platform coverage.

http://bit.ly/WMQAMS

# WebSphere MQ Security Lab

- Session #1260 at the 2011 IMPACT Conference
- Lab modules include…
  - Lock down unused channels
  - Set up SSL between two QMgrs
  - Set up SSL to use WMQ Explorer
  - Configure SSLPEER to filter connection requests
  - Configure a channel security exit to filter connection requests
- Contains an extensive lab guide and scripts for each module
- Use the scripts as a starting point for your own implementation

Missed the lab sessions? Download the lab materials any time from: https://t-rob.net/links

# Resources

## SupportPac MH05: WMQ Events Display Tool

This SupportPac provides a simple command line tool (xmqdspev) to display WebSphere MQ events that are generated on the SYSTEM.ADMIN.*.EVENT event queues.

NEW!

MH05 displays events in human-readable form. The output can be optionally re-directed to a file and the tool may be triggered by WebSphere MQ if required. All event message types are supported – including security events.

http://bit.ly/SupportPacMH05

# Resources

## SupportPac MO04: WebSphere MQ SSL Wizard

WebSphere MQ SSL Wizard is an interactive GUI which collects all information needed to configure an SSL connection between two queue managers or over a client channel and then generates all of the necessary commands.  It is great as a learning tool, to provide a starting point for your own scripting, or even to perform all the key management for smaller deployments.

http://bit.ly/SupportPacMO04

# Resources

## SupportPac MO05: WMQ Explorer Security Enhancements

The following WebSphere MQ Explorer plug-ins are included in this SupportPac:

- Authorization Service Infopop Plug-in
- Authorization Service Plug-in
- Authorization Service Tests Plug-in
- Tests Plug-in – Core Test Set
- Explorer documentation Plug-in
- New panel to add role-based authorities for all queue manager objects

http://bit.ly/SupportPacMO05

# Resources

## SupportPac MS81: WebSphere MQ Internet Pass-Thru

WebSphere MQ Internet pass-thru (known as MQIPT) is a WebSphere MQ base product extension that can be used to implement messaging solutions between remote sites across the internet.

It makes the passage of WebSphere MQ channel protocols in to and out of a firewall simpler and more manageable, by tunneling the protocols inside HTTP or by acting as a proxy.

MQIPT has an Administration graphical user interface (GUI) for managing one or more MQIPT servers.

http://bit.ly/SupportPacMS81

# Resources

## SupportPac MS03

- Also known as saveqmgr
- Save WMQ object definitions and authorization settings
- Works locally using bindings mode
- Also works remotely using client channels
- Be sure to authenticate the channels when using MS03 remotely!

http://bit.ly/SupportPacMS03

# Resources

SupportPac MH03

- WebSphere MQ SSL Configuration Checker
- A test tool to look for common configuration mistakes in WebSphere MQ SSL configurations and provides recommendations for resolving problems.
- If also provided with a copy of SSL files used by an WebSphere MQ client, it simulates a connection between the queue manager and client which it can then examine and provide diagnostic feedback on.

http://bit.ly/SupportPacMH03

# Resources

## SupportPac MS0P

- WMQ Explorer Configuration and Display Utilities
- Parses Authorization and other event messages
- API Exit that can be used to log all commands sent to the Command Server on the Distributed platforms

http://bit.ly/SupportPacMS0P

# Resources

## SupportPac IC72: WebSphere BI Brokers - Sample Control Center Security Exits

This SupportPac provides the source code for a pair of exit programs which provide an example of how to code a client and server exit program to verify Control Center users.  The programs are written to implement the MQ security exit interface and also provide examples of using this interface to:

- send and receive data between exits
- set exit response codes
- set the MCAUser field in the MQ Connection
- store and retrieve data in the exit program's own storage area

http://bit.ly/SupportPacIC72

# Resources

## BlockIP2 Security Exit

- Filter inbound connections by IP address.
- Suppress administrative user IDs.
- Dynamically set MCAUSER based on SSL certificate credentials.
- Extensive platform coverage.
- Includes source code - good starting point to write your own custom exit.

http://MrMQ.dk/

# Resources

## IBM developerWorks articles:

*End-to-end security and message protection in a WebSphere MQ client/server environment*

Describes how to use WebSphere MQ Extended Security Edition to secure WebSphere MQ clients. Content applies to AMS as well.
http://ibm.co/hBt98j

*What you didn't know you didn't know about WebSphere MQ Security*

This article clears up some misconceptions about how WebSphere MQ security works.
http://bit.ly/gsVNFH

*WebSphere MQ security heats up*

Article contains some useful setmqaut templates to lock down administrative access to WMQ.
http://ibm.co/17oKEc

# Resources

## IBM developerWorks articles

*From the Mission:Messaging column:*

Planning for SSL on the WebSphere MQ Network
http://ibm.co/3loir

Scripted WebSphere MQ key file management
http://ibm.co/3L1nja

Understanding WebSphere MQ authorization and the setmqaut command
http://ibm.co/aKNTvU

Ten WebSphere MQ SupportPacs I can't live without
http://ibm.co/2DDzjE

# Resources

IBM WebSphere MQ Business Partners

PartnerWorld is the IBM portal for Business Partners and clients looking for Business Partner expertise and solutions.

- Use the Global Solutions directory to search for solutions relating to WebSphere MQ from thousands of IBM and IBM Business Partners
- Use the Software partner directory to search for Business Partners with WebSphere MQ expertise.

http://www-306.ibm.com/software/integration/wmq/partners/

Is your queue manager configured to allow anonymous administrative access?

You should now have the skills and tools to assess the security of your messaging network and answer this question.

# Acknowledgements

Many thanks to the following contributers:

- Paul Faulkner and Joseph Gramig for contributing content, reviewing these slides and testing out the content in a real-world environment.
- Ian Vanstone, author of MO04 SSL Wizard and frequent collaborator.
- Jørgen Pedersen who is the author of BlockIP2.
- Jeff Lowrey, current maintainer of MS03 Save QMgr and collaborator.
- Arjan Van Vught, author of the Connection Exerciser demoed in this presentation and content contributor.
- Oliver Fisse, Long Nguyen, Chris Ahrendt, AJ Aronoff, Scott Munro, Glenn Baddelly, Tom Schneider, Scott Ripley for their contributions to this content and the community.
- Keys Botzum for lighting the path.

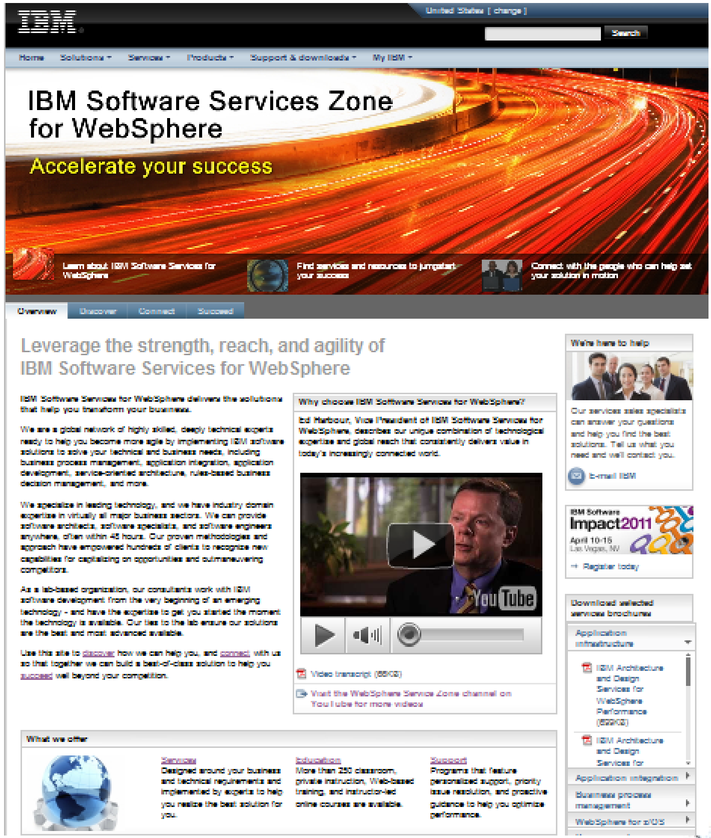
# IBM Software Services Zone for WebSphere

ibm.com/websphere/serviceszone

*The destination for WebSphere **services-related resources**, **offerings**, & **technical skills** to help you on your path to business agility*

## What's New?

- ***BPM-specific resources*** including proven, prescribed, and repeatable assets and offerings to accelerate BPM adoption
- ***Visibility across*** the worldwide skills & capabilities that only IBM Software Services for WebSphere can bring to your project
- ***Access*** to WebSphere practitioners' insight on project trends, best practices & emerging technologies through personal videos, blogs, articles & more
- ***Discover*** defined offerings to get your project started quickly



IBM Software Services Zone for WebSphere

Accelerate your success

Learn about IBM Software Services for WebSphere

Find services and resources to jumpstart your success

Connect with the people who can help set your solution in motion

Leverage the strength, reach, and agility of IBM Software Services for WebSphere

IBM Software Services for WebSphere delivers the solutions that help you transform your business.

We are a global network of highly skilled, deeply technical experts ready to help you become more agile by implementing IBM software solutions to solve your technical and business needs, including business process management, application integration, application development, service-oriented architecture, rules-based business decision management, and more.

We specialize in leading technology, and we have industry domain expertise in virtually all major business sectors. We can provide software architects, software specialists, and software engineers anywhere, often within 48 hours. Our proven methodologies and approach have empowered hundreds of clients to recognize new capabilities for capitalizing on opportunities and outmaneuvering competitors.

As a lab-based organization, our consultants work with IBM software development from the very beginning of an emerging technology - and have the expertise to get you started the moment the technology is available. Our ties to the lab ensure our solutions are the best and most advanced available.

Use this site to discover how we can help you, and connect with us so that together we can build a best-of-class solution to help you succeed well beyond your competition.

Why choose IBM Software Services for WebSphere?

Ed Harbour, Vice President of IBM Software Services for WebSphere, describes our unique combination of technological expertise and global reach that consistently delivers value in today's increasingly connected world.

Video transcript (88KB)

Visit the WebSphere Service Zone channel on YouTube for more videos

We're here to help

Our services sales specialists can answer your questions and help you find the best solutions. Tell us what you need and we'll contact you.

IBM Architecture and Design Services for WebSphere Performance (522KB)

IBM Architecture and Design Services for

What we offer

Services
Designed around your business and technical requirements and implemented by experts to help you realize the best solution for you.

Education
More than 250 classroom, private instruction, Web-based training, and instructor-led online courses are available.

Support
Programs that feature personalized support, priority issue resolution, and proactive guidance to help you optimize performance.

***Visit us in the Solution Center!***

**•Ped SE2:** IBM Software Services for WebSphere

**•Ped BD1:** IBM BPM & BRM Services

# We love your Feedback!

- Don’t forget to submit your Impact session and speaker feedback! Your feedback is very important to us, we use it to improve our conference for you next year.
- Go to impactsmartsite.com from your mobile device
- From the Impact 2011 Online Conference Guide;
  - Select Agenda
  - Navigate to the session you want to give feedback on
  - Select the session or speaker feedback links
  - Submit your feedback

# Copyright and Trademarks