IBM Software Group

Non-SSL Security in WebSphere MQ Open Mic

16 September 2010

WebSphere® Support Technical Exchange

ON DEMAND BUSINESS

Agenda

- Introduce the panel of experts
- Introduce Non-SSL Security in WebSphere MQ
- Answer questions submitted by email (8 questions)
- Open telephone lines for questions
- Summarize highlights

Panel of Experts

Panelist	Role at IBM®
T-Rob Wyatt	Senior Managing Consultant
Tom Schneider	Advisory IT Architect
Morag Hughson	WebSphere MQ Development Product Architect
Paul O'Donnell	Senior Software Engineer

Introduction

- We will discuss non-SSL security configurations for WebSphere MQ versions 6 and 7 on Unix®, Windows® and z/OS platforms.
- Only published materials will be referenced.
- Specific security incidents are out of scope.
- For more information on SSL see the References slide at the end of the presentation.

Question 1

- I put SSL on my application channels, is there anything else I need to do?

Answer to Question 1

- Lock down the channels that do not have SSL on them, set SSLPEER, set MCAUSER and/or SCYEXIT
- See T-Rob's "Hardening WebSphere MQ Security" presentation for more details: https://t-rob.net/links/

Question 2

- How do I apply authorization to a topic?

Answer to Question 2

- Access control on the topic tree can be granted on the whole topic tree with the same access level or with different portions of the topic tree being granted different access levels. The topic tree is a naturally hierarchical structure and so child nodes will inherit behaviours, including security access from their parent nodes if no specific behaviour is defined at that child node. This means that security can be applied to sections of the topic tree without the need to explicitly set security at every node in the topic tree.

- In order to apply security, choose the node in the topic tree that is the top level parent node. By that I mean the highest point in the topic tree where the security is going to apply. It is ideal to choose a layer in your topic tree where all the nodes are siblings and apply security at the same point across the structure. This of course can be the SYSTEM.BASE.TOPIC node at the top, or every child node at the leaves. However, more sensibly it is somewhere in between where your topics logically group into areas requiring the same security definitions.

- Having chosen the nodes in the topic tree to apply security to, you define topic objects to point at those nodes and create security profiles in the usual manner for that 48-character MQ object name. Access is granted to these MQ objects for subscribers and publishers using the appropriate flags or access levels (platform dependant).

Question 3

- What security considerations exist for WebSphere MQ File Transfer Edition (WMQ FTE)?

Answer to Question 3

- FTE is like any other WMQ application. Agents and human users are authenticated when they connect, either by the operating system for bindings mode or by SSL and/or exits when connecting as a client. OAM is used to authorize the authenticated ID to the appropriate FTE queues.

Question 4

- How can I find the cause of a not authorized error on z/OS?

Answer to Question 4

- View the <qmgr>MSTR started task (where <qmgr> is the queue manager name, for example, CSQ1MSTR for queue manager CSQ1)
- Select the JESMSGLG.
- For each 2035 error, assuming RACF is the external security manager being used, there should be an ICH408I RACF message.
- Do a find on the ICH408I message. This message will provide a lot of detail, such as the userid, the fully qualified name of the resource the user is trying to access, the RACF profile for which the user has an insufficient level of access and the access the user currently has versus what the user would need to be successful.

Question 5

- How can I list security profiles used by WebSphere MQ on z/OS?

Answer to Question 5

- Since the security profiles for WMQ on z/OS are not WMQ objects, you will need to list them with a RACF command, or with the command supplied by your external security manager if you are using something other than RACF.
- Use the RACF command RLIST (RL). To use RLIST, you would need to know the name of the RACF CLASS in which the profile is defined, such as MQQUEUE. Then you also need to specify either the exact profile you want to list, or an asterisk (*) to list all of the profiles in the class. If you try to list a series of profiles using a generic string, but there is no profile which exactly matches that string, RLIST will interpret that to mean you want to list that exact profile, and will just return an error message stating that the profile was not found. Multiple profiles can be listed by on RLIST command if you specify them inside of parentheses.

Question 6

- Our customers are planning to move from 1024 bit certificates to 2048 bit certificates. Please let us know what is the required MQ ver/rel Fix pack level to satisfy this requirement.

  This is the platform information - Z/OS, Unix, Windows (RACF, gsk7cmd and IKEYman).

Answer to Question 6

- As of WMQ 6.0.1.0 and GSKit 7.0.3.18 2048 bit keys are supported.
- Key size in RACF depends on the RACF release. For z/OS v1.10 and v1.11 2048 keys are supported except for ICSF RSA keys.
- From MQSC Reference: “when a CipherSpec name includes _EXPORT, the maximum handshake key size is 512 bits.... when a CipherSpec name includes _EXPORT1024, the handshake key size is 1024 bits. Otherwise the handshake key size is the size stored in the certificate.”

Question 7a

- How does MQ Security differentiate between administrative actions on MQ resources and MQ Application use of MQ resources?

Answer to Question 7a

- On z/OS, administrative actions and Application access use different profiles in different classes and therefore are completely segregated.
- On the distributed platforms, for those users that are not privileged users (mqm group for example), there is also a good separation of actions between administrative tasks and application tasks, by having different authorizations required for the different tasks, e.g. +chg (for alteration of a resource) versus +get (to MQOPEN a queue to get messages from it). +dsp crosses the boundaries between administration and application usages but all other authorizations are segregated.

Question 7b

- Is there any sandbox-type of security scheme that can be employed to protect MQ internal objects vs. application specific objects?

Answer to Question 7b

- The Object Authority Manager can be used to control access to SYSTEM.* objects as well as to user-defined objects.
- Be sure to put application and user accounts in a group other than mqm (or platform equivalent).
- A sample script may be downloaded from https://t-rob.net/wmq/ listed as “OAM Templates”.

Question 8

- Since security is such a hot topic, why are the MQ Clients and the new MQ Explorer support pack MS0T freely available to the public? Should these be locked down so only IBM customers licensed for WebSphere MQ can obtain them? Our research with the MQ Explorer indicates it opens additional security risks.

Answer to Question 8

- The answer is that the new version of Explorer does not open any new security exposures, it actually helps to close them. Customers who have gone to the trouble of writing or buying a security exit capable of authenticating ID and password need a way to pass these in. Explorer now allows these customers to utilize such an exit. Tools written in Python capable of emulating the WMQ protocol and which do not depend on IBM code have been available on the Internet for several years. Restricting the client or WMQ Explorer would not in any way hinder an attacker but it would make life more difficult for legitimate users.

Open Lines for Questions

We Want to Hear From You!

Tell us about what you want to learn

Suggestions for future topics
Improvements and comments about our webcasts
We want to hear everything you have to say!

Please send your suggestions and comments to:
wsehelp@us.ibm.com

Summary

References and Useful Links

- Webcast replay: Introduction to Secure Sockets Layer Basic
  http://www-01.ibm.com/support/docview.wss?rs=&uid=swg27016829
- Open Mic Replay: SSL and TLS in WebSphere MQ
  http://www-01.ibm.com/support/docview.wss?rs=&uid=swg27018213
- Webcast replay: Configuration of SSL with WebSphere MQ and Diagnostic Hints and Tips
  http://www-01.ibm.com/support/docview.wss?rs=&uid=swg27016864
- DeveloperWorks
  http://www.ibm.com/developerworks/websphere/community/

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at:
  http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at:
  http://www.ibm.com/developerworks/websphere/community/
- Join the Global WebSphere Community:
  http://www.websphereusergroup.org
- Access key product show-me demos and tutorials by visiting IBM Education Assistant:
  http://www.ibm.com/software/info/education/assistant
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically:
  http://www.ibm.com/software/websphere/support/d2w.html
- Sign up to receive weekly technical My Notifications emails:
  http://www.ibm.com/software/support/einfo.html