Setting context

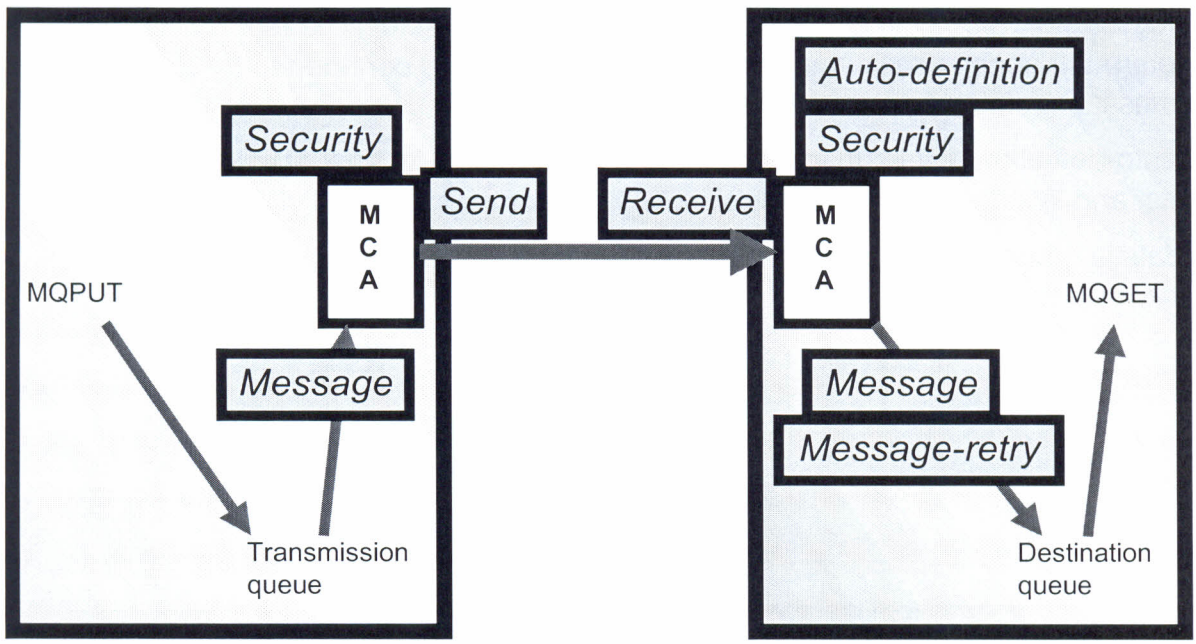
- Two open options that require authority to use
  - MQOO_SET_IDENTITY_CONTEXT
  - MQOO_SET_ALL_CONTEXT
- Two corresponding put message options
  - MQPMO_SET_IDENTITY_CONTEXT
  - MQPMO_SET_ALL_CONTEXT
- Normally used by special programs only
  - Message channel agents
  - System utilities

Figure 12-22. Setting context WM203 / VM2032.0

Notes:

The visual depicts the two remaining context options for use when opening a queue. An application requires authority to use these options. The corresponding put message options are for use when putting a message on a queue once it has been opened.

WebSphere MQ channel exit programs



Significant setup required for user exits
No security ready to use as is

Notes:

The uses of channel exit programs are:

- **Auto-definition exit** can be used to modify the channel definition derived from the model SYSTEM.AUTO.RECEIVER.
- **Security exit** is primarily used by the MCA at each end of a message channel to authenticate its partner.
- **Send and receive exits** can be used for purposes such as data compression/ decompression and data encryption/decryption.
- **Message exit** can be used for any purpose which makes sense at the message level. The following are some examples.
  - Application data conversion
  - Encryption/decryption
  - Journaling
  - Additional security checks such as validating an incoming user identifier

  - Substitution of one user identifier for another as a message enters a new security domain
  - Reference message handling
- **Message-retry exit** is called when an attempt to open a destination queue, or put a message on a destination queue, has been unsuccessful. The exit can be used to determine under what circumstances the MCA should continue to try again, how many times it should retry, and how frequently.

The auto-definition exit is only supported on WebSphere MQ for AIX, HP-UX, iSeries, Solaris, and Windows, and WebSphere MQ for Compaq Tru64 UNIX.

Full details on how to write channel exit programs can be found in *WebSphere MQ Intercommunication manual.*

Channel exit programs on MQI channels

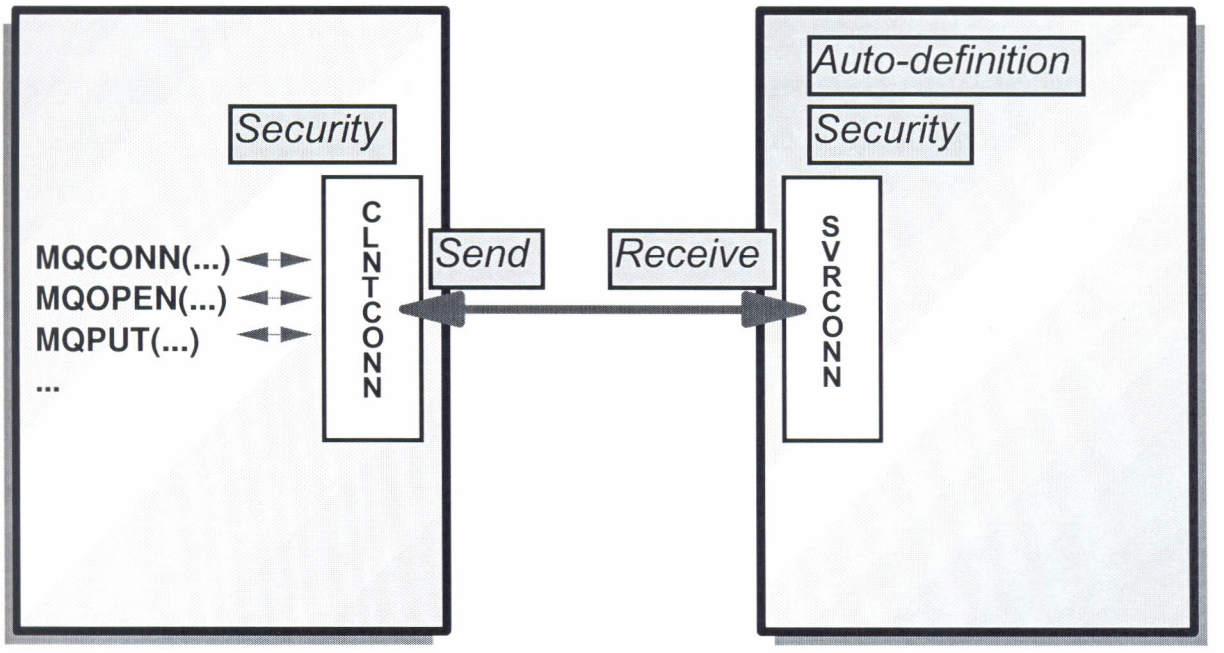


Figure 12-24. Channel exit programs on MQI channels WM203 / VM2032.0

Notes:

No channel exit programs can be called on a client system if the MQSERVER environment variable is used to define a simple client connection.

The auto-definition exit can be used to modify the channel definition derived from the model SYSTEM.AUTO.SVRCONN.

The auto-definition exit is only supported on a Version 6 or 7 queue manager.

Message context topic summary

Having completing this topic, you should be able to:

- Explain how to use the message context information to find out about the originator of the message
- Control the use of this facility

Figure 12-25. Message context topic summary WM203 / VM2032.0

Notes:

Secure sockets layer (SSL)

- Protocol to allow transmission of secure data over an insecure network
- Combines these techniques
  - Symmetric and secret key encryption
  - Asymmetric and public key encryption
  - Digital signature
  - Digital certificates
- Protection
  - Client/server
  - Queue manager and queue manager channels
- To combat security problems

Eavesdropping:	Encryption techniques
Tampering:	Digital signature
Impersonation:	Digital certificates

Notes:

Secure Sockets Layer (SSL) is common across all the Version 6 and later platforms -z/OS, UNIX, Windows, iSeries.

SSL is an industry-standard protocol for secure communications, involving encryption, authentication, and integrity of data. SSL is supported in both client/server and qmgr/qmgr channels (including clusters). There are many flexible capabilities built-in, including the ability to select who are prepared to accept communications from based on their fully-authenticated identity. This feature removes, for many people, the need to set up channel exits, where they were used for security purposes.

SSL, widely accepted in the Internet community, has been subjected to significant testing by the hacker community.

SSL

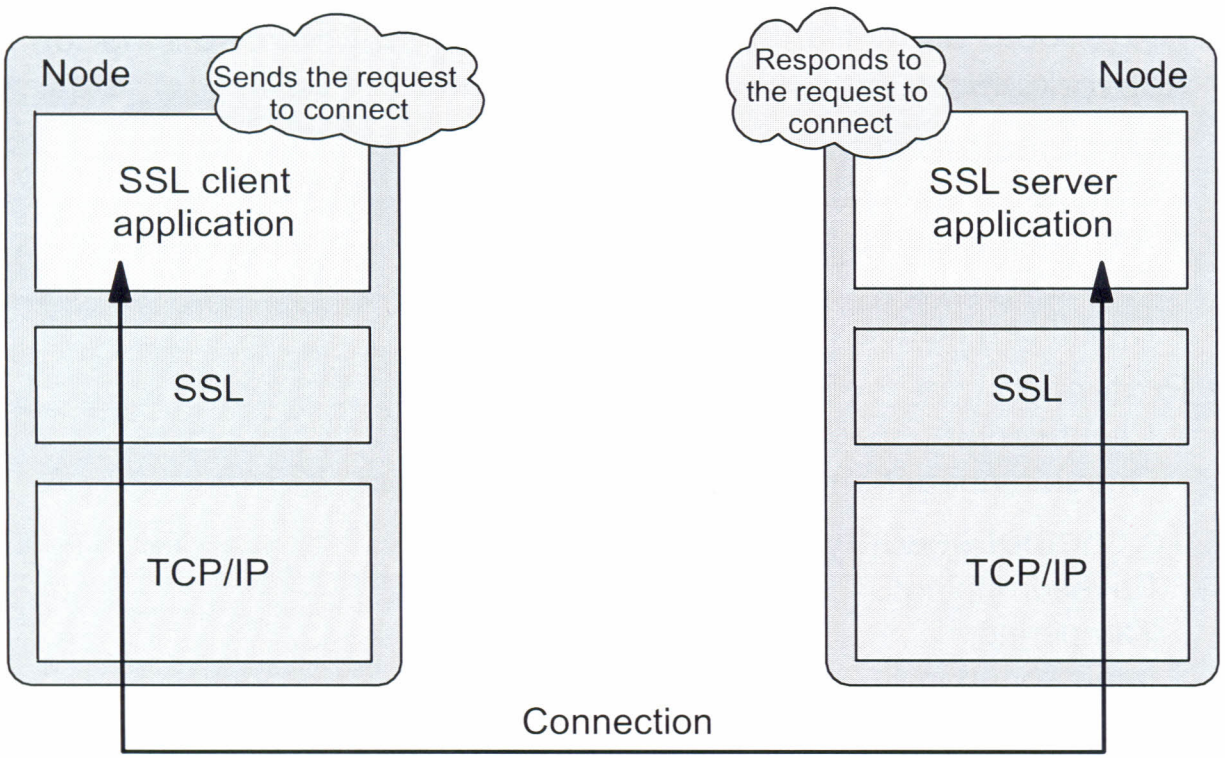


Figure 12-28. SSL

WM203 / VM2032.0

Notes:

WebSphere MQ SSL support

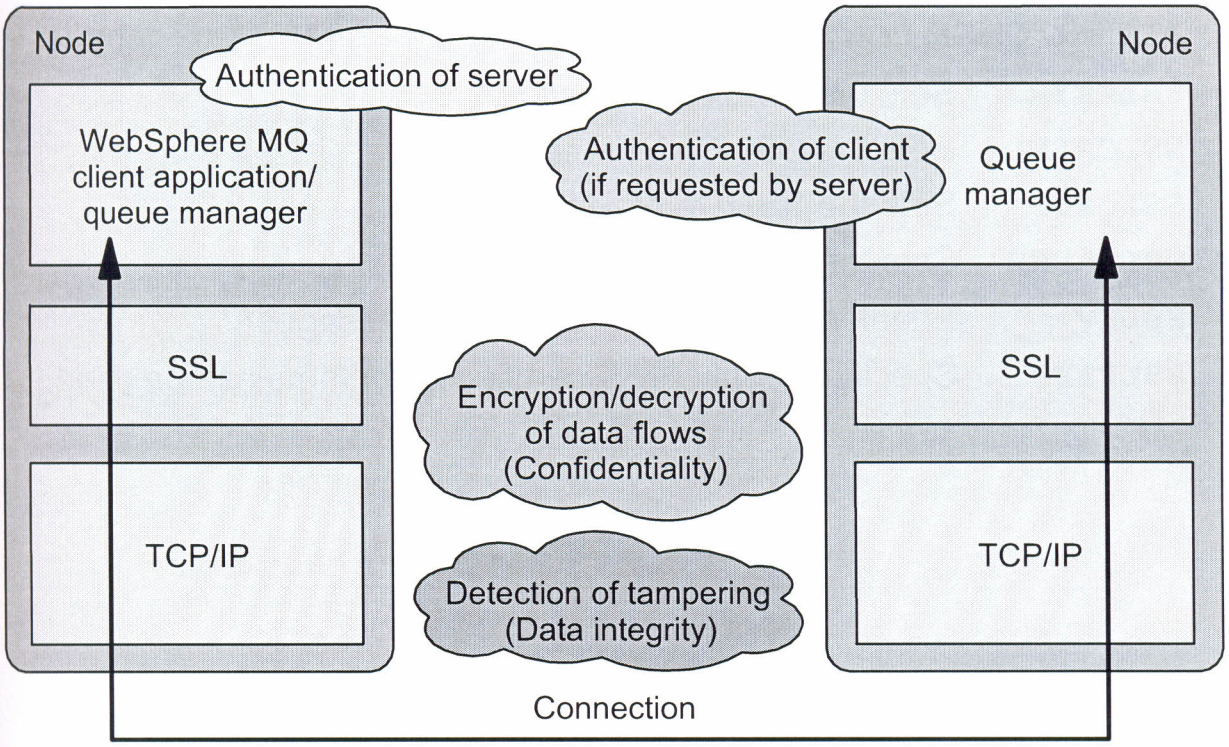


Figure 12-29. WebSphere MQ SSL support

Notes:

QMGR attributes for SSL

- **ALTER QMGR** command

SSLKEYR	Sets the SSL key repository
SSLCRLNL	Sets the SSL CRL namelist
SSLCRYP	Sets the SSL CryptoHardware
SSLTASKS	Sets the SSL tasks
SSLEV	Enables or disables SSL event messages
SSLFIPS	Specifies if only FIPS-certified algorithms can be used

Figure 12-30. QMGR attributes for SSL

Notes:

QMGR authentication object

- ALTER AUTHINFO
- DEFINE AUTHINFO
- DELETE AUTHINFO
- DISPLAY AUTHINFO

Figure 12-31. QMGR authentication object

Notes:

You can either alter, define, delete, or display the authentication information objects. These objects contain the definitions required to perform Certificate Revocation Lists (CRL) checking using LDAP servers.

The AUTHINFO queue manager attribute is supported on UNIX, Windows, i5/OS, HP NonStop Server, and HP OpenVMS.

Channel attributes for SSL

- **DEFINE** or **ALTER CHANNEL**

SSLCIPH	Defines a single CipherSpec for an SSL connection
SSLPEER	Specifies peer name used in SSL channel negotiation
SSLCAUTH	Specifies whether the channel carries out client authentication over SSL

Figure 12-32. Channel attributes for SSL WM203 / VM2032.0

Notes:

SSLCIPH specifies the encryption strength and function (CipherSpec), for example NULL_MD5 or RC4_MD5_US. The CipherSpec must match at both ends of the channel.

SSLPEER specifies the distinguished name (unique identifier) of allowed partners.

SSLCAUTH defines whether WebSphere MQ requires and validates a certificate from the SSL client.

Access control for a WebSphere MQ client

- Access control based on user ID used by server connection process (*MCAUserIdentifier* in MQCD)
- Security exits at both ends of the MQI channel
  - Client security exit can flow a user ID and password
  - Server security exit can authenticate the user ID and set *MCAUserIdentifier*
- No security exit at the client end of the MQI channel
  - Value of logged in user ID flows to the server system
  - Server security exit can authenticate the user ID and set *MCAUserIdentifier*
- No security exit at either end of the MQI channel
  - *MCAUserIdentifier* has the value of `MCAUSER` if it is nonblank
  - *MCAUserIdentifier* has the value of flowed user ID otherwise

Notes:

When a WebSphere MQ client application wants to access a **WebSphere MQ** object on the server queue manager (for example, connect to the queue manager, or open a queue), access control is based on a user ID used by the server connection process. The reason for this is that it is the server connection which actually issues the MQI calls. This user ID is determined by the value of the *MCAUserIdentifier* field in the active channel definition at the server end of the MQI channel instance. The active channel definition is defined by the structure MQCD and is documented in *WebSphere MQ Intercommunication* manual.

Remote queuing and clients

- Channel exits
  - A number of channel exits are available in the product and as SupportPacs
  - Several vendors in this market too
- MCAUSER
  - The default setting is wide open, especially for client attach
  - You may want to set this to restrict who can access your queue manager
- MQ_ USER_ ID environment variable
  - This was removed for WindowsNT and UNIX in the V5.1 release client environments
  - The logged-in username is now automatically used but this is not authenticated at the server; you may still need security exits

Figure 12-34. Remote queuing and clients WM203 / VM2032.0

Notes:

WebSphere MQ SSL support summary

Having completing this topic, you should be able to:
- Explain the SSL support provided in WebSphere MQ

Figure 12-35. WebSphere MQ SSL support summary

Notes:

Publish/subscribe security

- Publish/subscribe security is based on defined topic objects.
- You have to define topic objects to control security.
- Security is checked from the bottom up for authorization in the topics tree.
- When publishing, a check is performed at the MQOPEN of the topic you want to publish to.
- When subscribing, a check is carried out when an MQSUB to the specified topic is received.
- Subscriber must also have authority to put to the destination for the subscription – actual 'publish' check.

Figure 12-37. Publish/subscribe security

Notes:

Controlling security using WebSphere MQ Explorer (1 of 4)

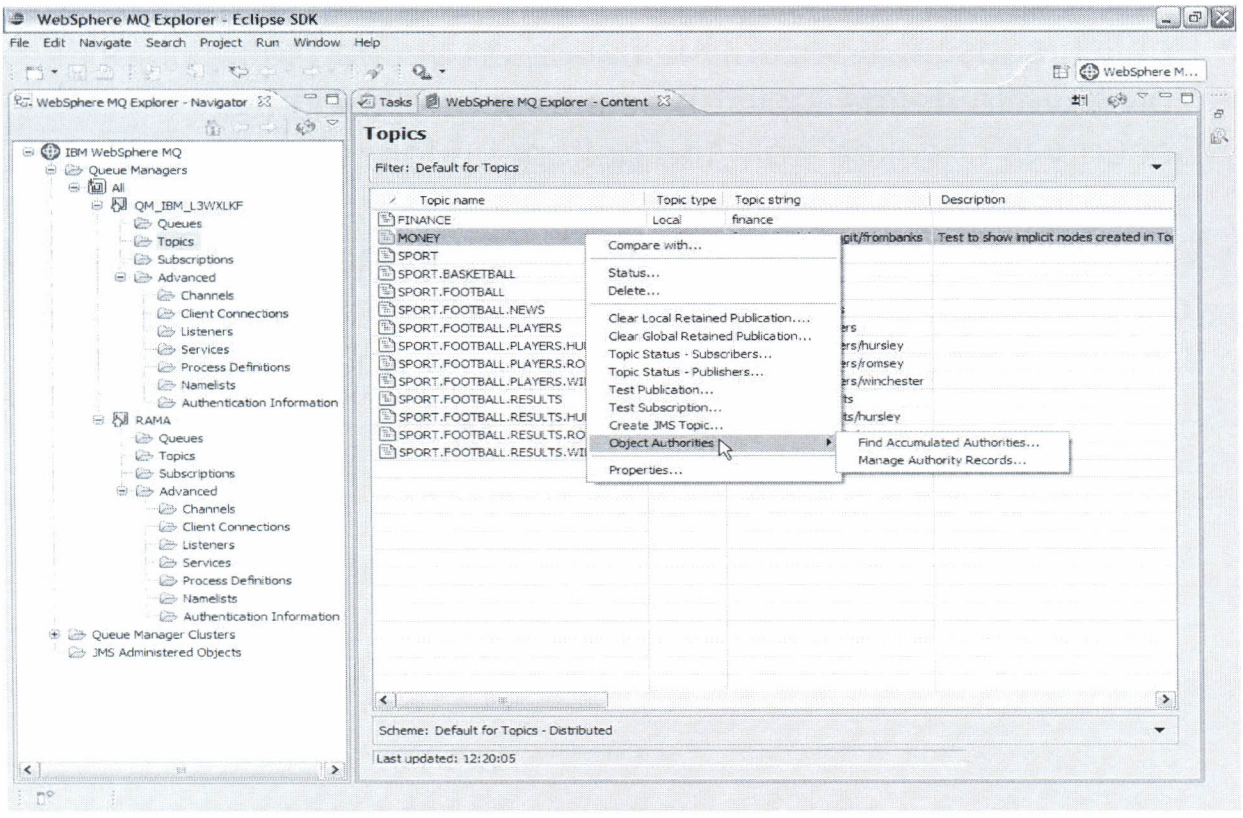


Figure 12-38. Controlling security using WebSphere MQ Explorer (1 of 4) WM203 / VM2032.0

Notes:

This screen shows you how to give "publish" authority to a user MQUSER for the topic MONEY.

1. Select TOPICS.
2. Right-click MONEY and select **Object Authorities** and then **Manage Authority Records.**
3. On the left panel, expand the *Specific Profiles* which displays the profile for MONEY. Click this MONEY icon to display the authorities to this TOPIC.
4. By default, groups that have access to this topic are displayed. Select **Users** to show the users who have access. This is shown on the next slide.

Controlling security using WebSphere MQ Explorer (2 of 4)

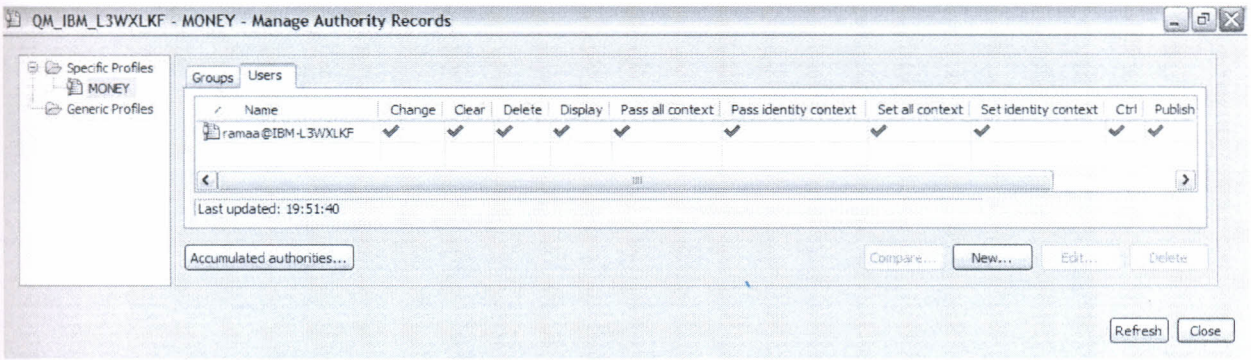


Figure 12-39. Controlling security using WebSphere MQ Explorer (2 of 4)

Notes:

On the left panel, right-click **MONEY**. Select **New** - **User Authority**.

Controlling security using WebSphere MQ Explorer (3 of 4)

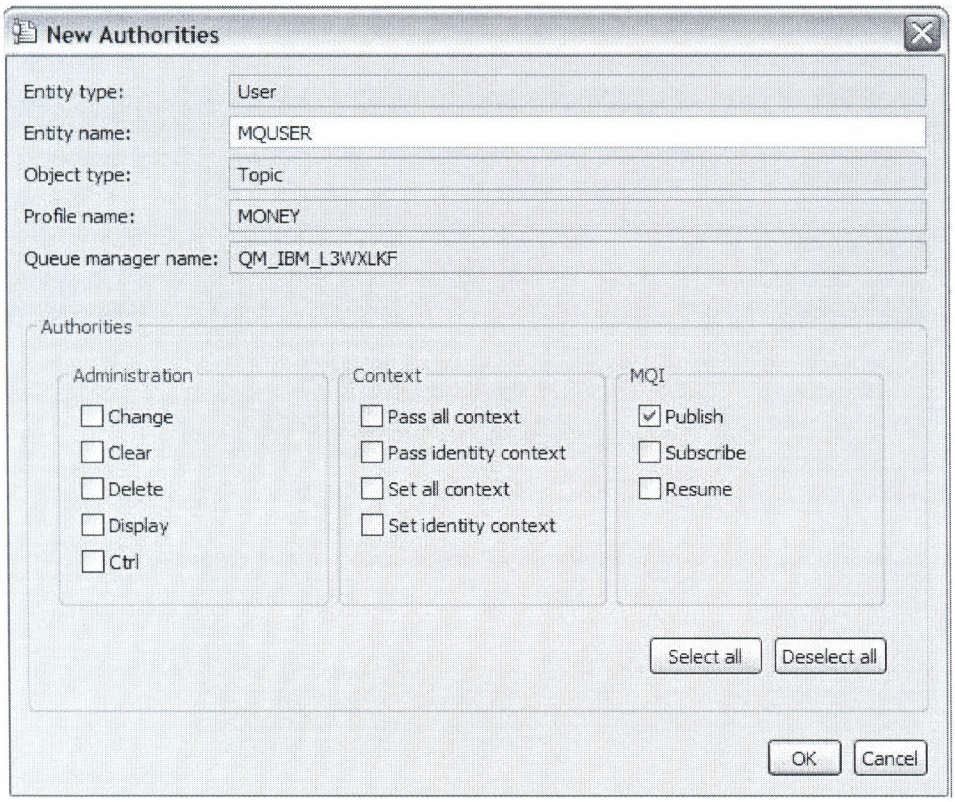


Figure 12-40. Controlling security using WebSphere MQ Explorer (3 of 4) WM203 / VM2032.0

Notes:

Specify MQUSER in the Entity name, select **Publish**, and click **OK**.

Controlling security using WebSphere MQ Explorer (4 of 4)

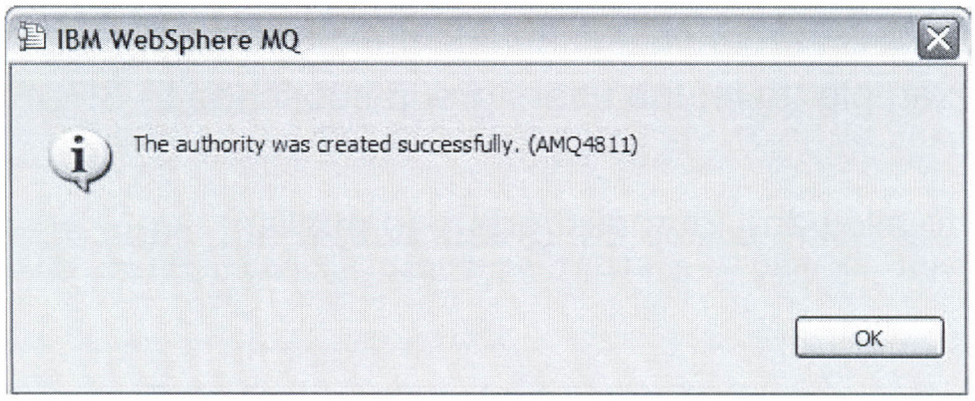


Figure 12-41. Controlling security using WebSphere MQ Explorer (4 of 4)

WM203 / VM2032.0

Notes:

See that MQUSER has been added with publish access.

Controlling security using setmqaut

- Controlling security using setmqaut
- Three new authorities are added pub, sub and resume.
- An example: to let the users group subscribe to SPORT:
  `setmqaut -m WMQ7 -n SPORT -t topic -g users +sub`
- And to allow the journalist group to publish:
  `setmqaut -m WMQ7 -n SPORT -t topic -g journalist +pub +sub`

Figure 12-42. Controlling security using setmqaut WM203 / VM2032.0

Notes:

The `-pub/-sub` attribute does not block the pub. It just clears the authority on that topic, so OAM looks higher in the tree for a `+pub/+sub`.

Basic MQ security on publish/subscribe queues

- MQ publish/subscribe uses normal MQ queues, and when subscribing you need to have access to the "reply" queue.
- When using managed subscriptions, you need access to:
  - SYSTEM.NDURABLE.MODEL.QUEUE
  - SYSTEM.DURABLE.MODEL.QUEUE
- You also need connect access to the queue manager.

Notes:

For WebSphere MQ publish/subscribe operations, the user should be authorized to have the right access to the destination queue ("reply" queue).

When resuming or alerting a subscription the user should have PUT, GET and BROWSE authority on the destination queue.

The system managed operations use the SYSTEM.NDURABLE.MODEL.QUEUE and SYSTEM.DURABLE.MODEL.QUEUE and the user should have access to them.

Publish/subscribe security topic summary

Having completing this topic, you should be able to:

- Use WebSphere MQ explorer to control publish/subscribe security

Figure 12-44. Publish/subscribe security topic summary

WM203 / VM2032.0

Notes:

Checkpoint questions

1. True or false - The MQSC command **REFRESH SECURITY** must be issued to make OAM changes take effect.

2. Using OAM, how would you protect local queue REBATE.IN on MY.QMGR for:
   a. MQPUT access only by group ASSESSORS
   b. MQGET by id PROCESSOR
   c. MQGET browse only by group AUDITOR

3. For an application to open a queue using an alternate userid, the initial userid requires:
   a. OAM delegate authority
   b. OAM alternate user authority
   c. Authority to use "runas" on Windows or "su" on UNIX.
   d. password of alternate userid
   e. None of the above

Notes:

Unit summary

Having completed this unit, you should be able to:

- Explain the role of object authority manager (OAM) to provide security to WebSphere MQ resources
- Use access control lists (ACLs) to protect WebSphere MQ resources using OAM
- Use some OAM control commands
- Explain how to use message context information
- Explain the Secure Sockets Layer (SSL) support provided in WebSphere MQ
- Use WebSphere MQ Explorer to control publish/subscribe security

Figure 12-46. Unit summary

WM203 / VM2032.0

Notes: