IBM Software Group

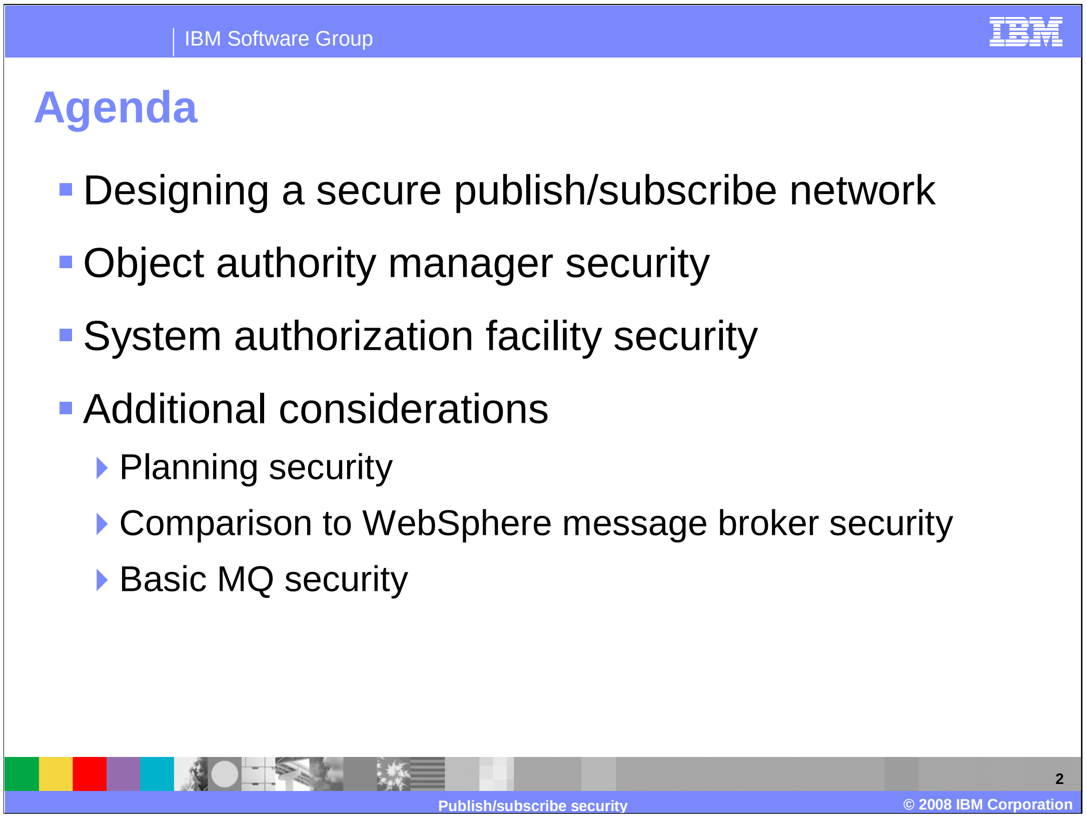
WebSphere® MQ V7

Publish/subscribe security

business on demand.

Updated August 1, 2008

This module provides information on designing and administering security for publish/subscribe.



Agenda

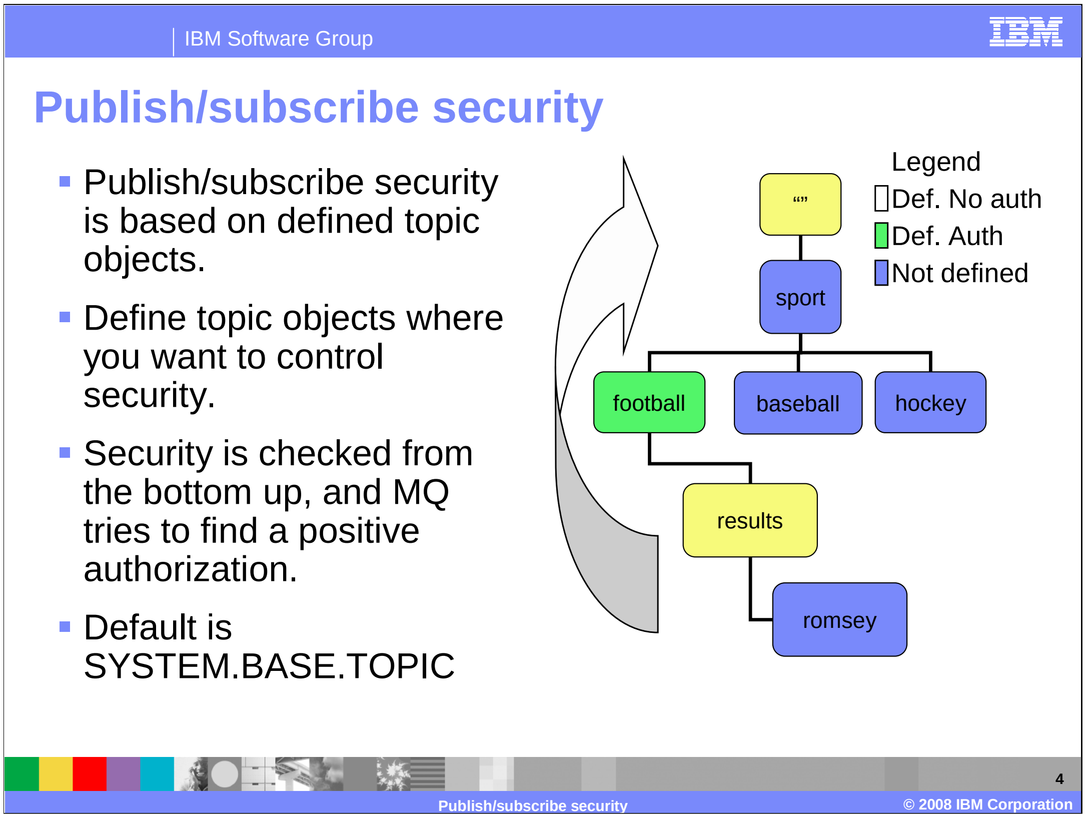
- Designing a secure publish/subscribe network
- Object authority manager security
- System authorization facility security
- Additional considerations
  - Planning security
  - Comparison to WebSphere message broker security
  - Basic MQ security

This module provides information on designing a secure publish/subscribe network. It describes using OAM to implement security on the distributed platforms and SAF on z/OS.

Section

Designing a secure publish/subscribe network

This section discusses security considerations while designing a publish/subscribe network.



IBM Software Group

Publish/subscribe security

- Publish/subscribe security is based on defined topic objects.
- Define topic objects where you want to control security.
- Security is checked from the bottom up, and MQ tries to find a positive authorization.
- Default is SYSTEM.BASE.TOPIC

Legend

□Def. No auth

🟩Def. Auth

🟦Not defined

“”

sport

football

baseball

hockey

results

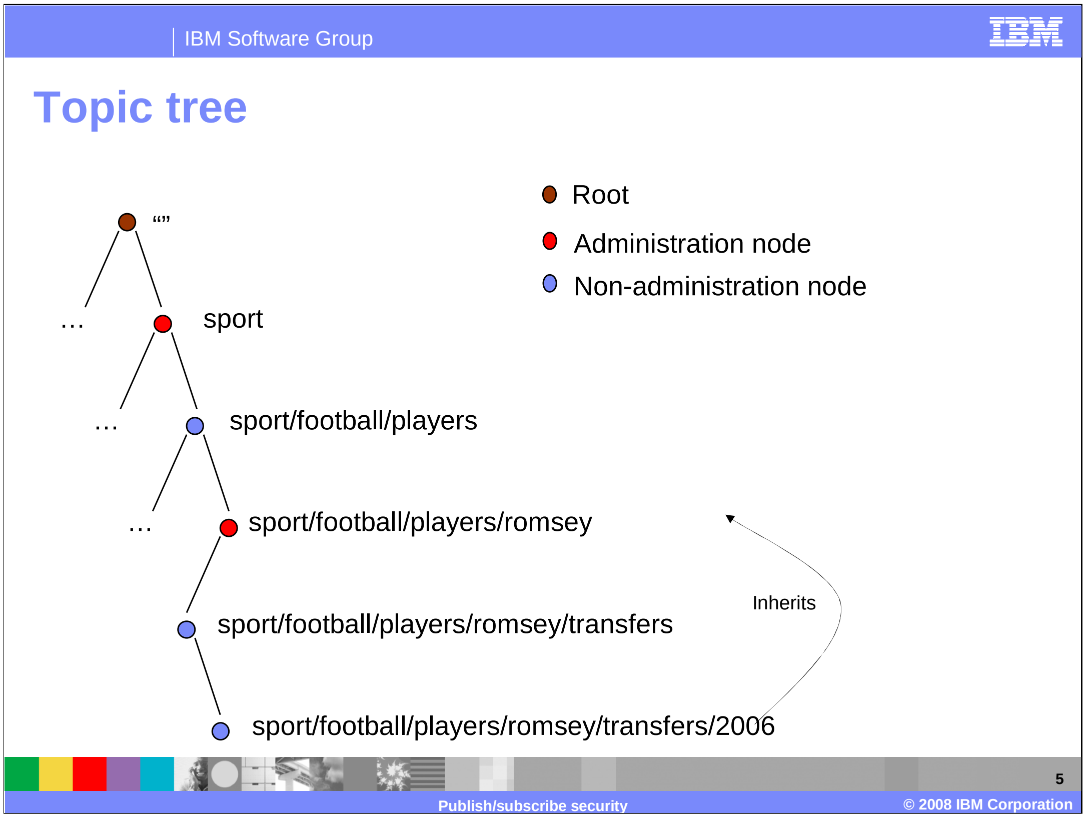
romsey

4

Publish/subscribe security

Each topic that you define is an element, or node, in the topic tree. The topic tree can either be empty to start with or contain topics that have been defined. You can define a new topic either by using the create topic commands or by specifying the topic for the first time in a publication or subscription. An *administrative topic object* is a WebSphere® MQ object that allows you to assign specific, non-default attributes to topics. Administrative topics must be defined.

Topics inherit their attributes from the first parent administrative node found in their topic tree. If there are no administrative topic nodes in a particular topic tree, then all topics will inherit their attributes from the base topic object, SYSTEM.BASE.TOPIC.



IBM Software Group

Topic tree

🟤 Root

🔴 Administration node

🔵 Non-administration node

“”

…

sport

…

sport/football/players

…

sport/football/players/romsey

sport/football/players/romsey/transfers

Inherits

sport/football/players/romsey/transfers/2006

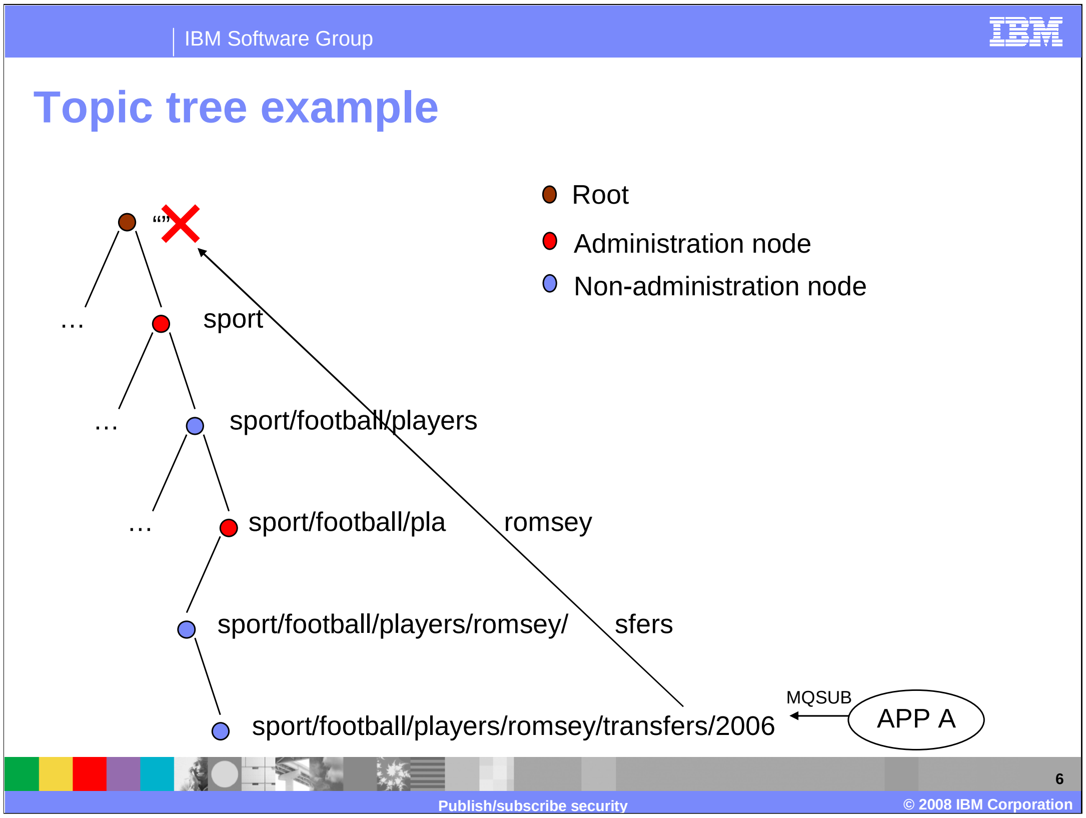
5

Publish/subscribe security

© 2008 IBM Corporation

Nodes in a topic tree, which have a topic object associated with them, are known as administration nodes.

Nodes which were automatically generated, inherit the properties of the first administration node above them in the tree structure



Topic tree example

● Root

● Administration node

● Non-administration node

“”

…

sport

…

sport/football/players

…

sport/football/pla romsey

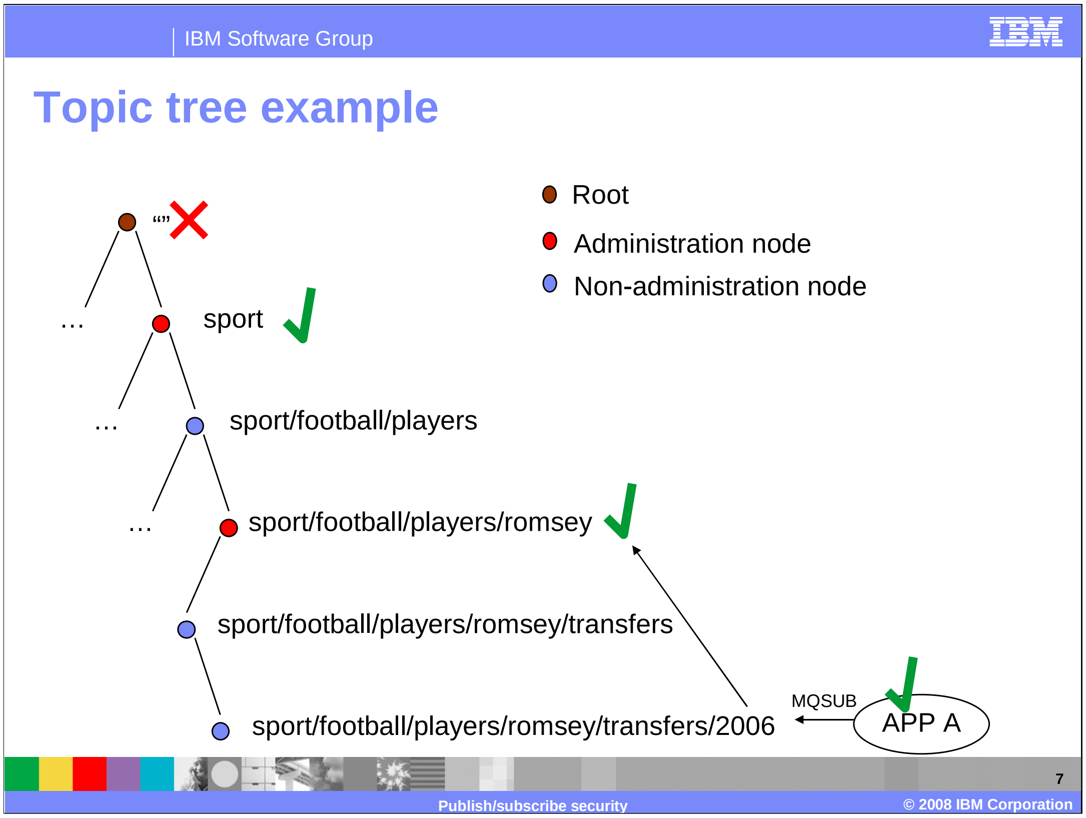
sport/football/players/romsey/ sfers

sport/football/players/romsey/transfers/2006

MQSUB

APP A

Administration nodes are also used to determine whether a user has authority to a node in the topic tree. In this example, APP A has not been permitted to subscribe to any administration nodes.



IBM Software Group

Topic tree example

● Root

● Administration node

● Non-administration node

“” ✗

…

sport ✓

…

sport/football/players

…

sport/football/players/romsey ✓

sport/football/players/romsey/transfers

sport/football/players/romsey/transfers/2006

MQSUB

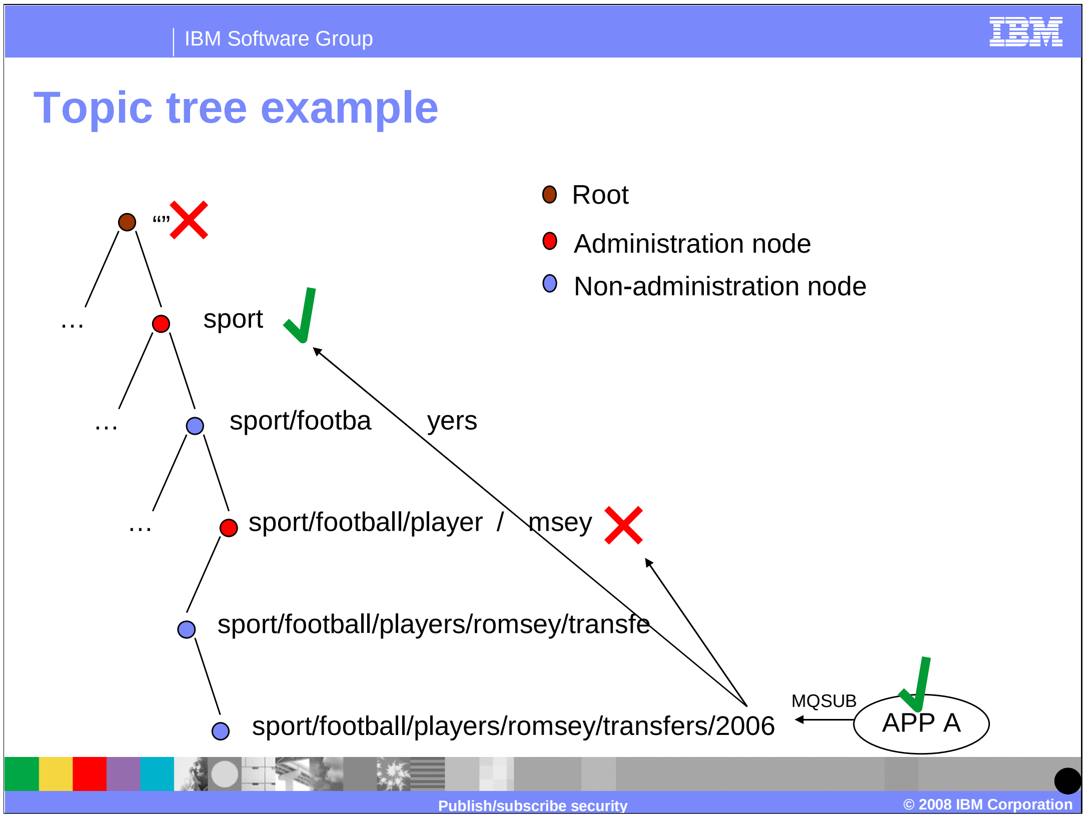
APP A ✓

7

Publish/subscribe security

© 2008 IBM Corporation

In this example, APP A wants to subscribe to topic **sport/football/players/romsey/transfers/2006.** Administration node **sport/football/players/romsey** allows APP A to subscribe, so access is granted even though the root node does not allow the subscription.



IBM Software Group

Topic tree example

● Root

● Administration node

● Non-administration node

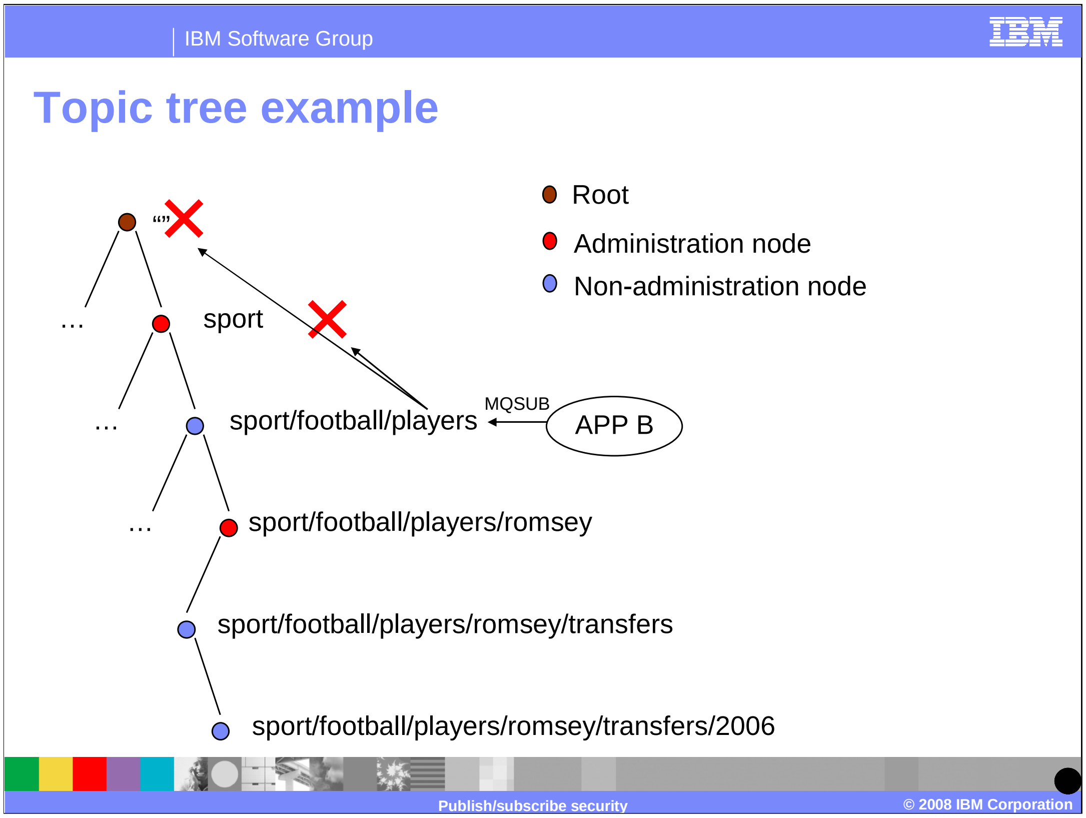
“”
…
sport
…
sport/footba yers
…
sport/football/player / msey
sport/football/players/romsey/transfe
sport/football/players/romsey/transfers/2006
MQSUB
APP A

Publish/subscribe security

© 2008 IBM Corporation

In this example, APP A wants to subscribe to topic **sport/football/players/romsey/transfers/2006.**

In this case, administration node **sport/football/players/romsey** does not allow APP A to subscribe. However, administration node **sport** does, so access is granted. This might not be your intention. Once permitted at an administration node you cannot be denied further down the tree. It is important from both an administration and security point of view to ensure that your trees are structured to align with how your subscriptions are made.



Topic tree example

● Root

● Administration node

● Non-administration node

“”

…

sport

…

sport/football/players

MQSUB

APP B

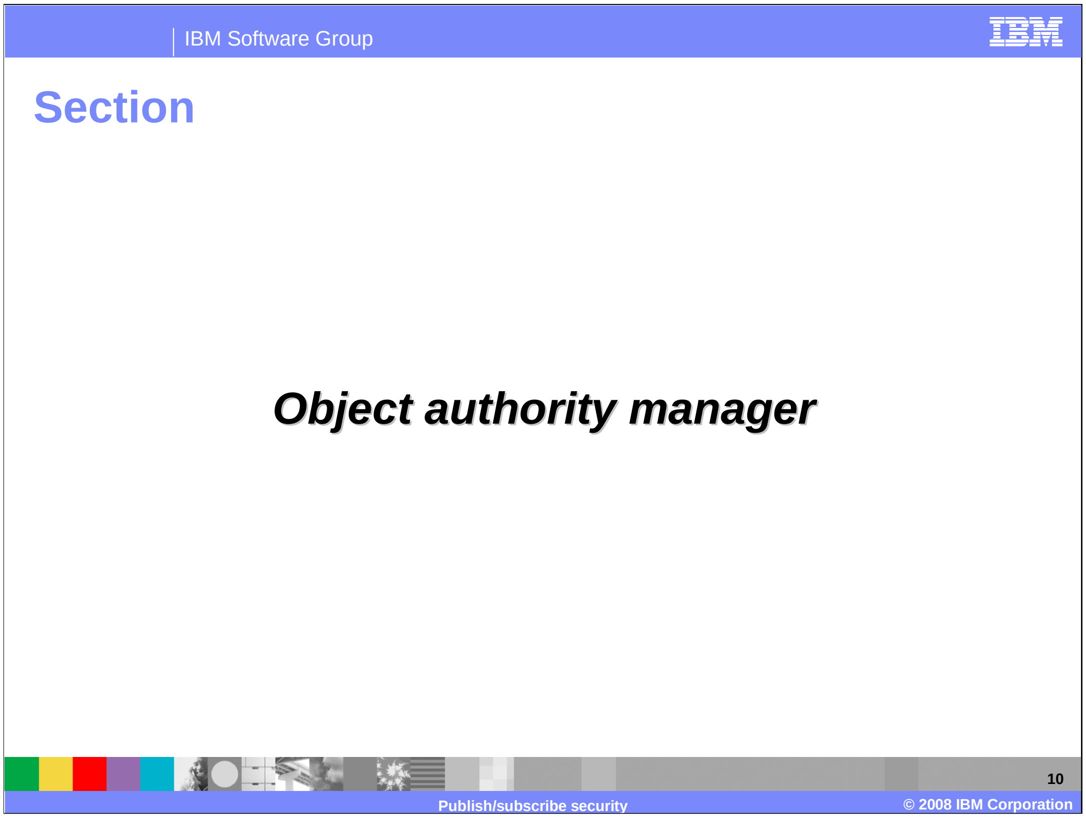
…

sport/football/players/romsey

sport/football/players/romsey/transfers

sport/football/players/romsey/transfers/2006

Here, APP B wants to subscribe to topic **sport/football/players.** The administration node **sport** does not allow APP B to subscribe, so access is denied.



IBM Software Group

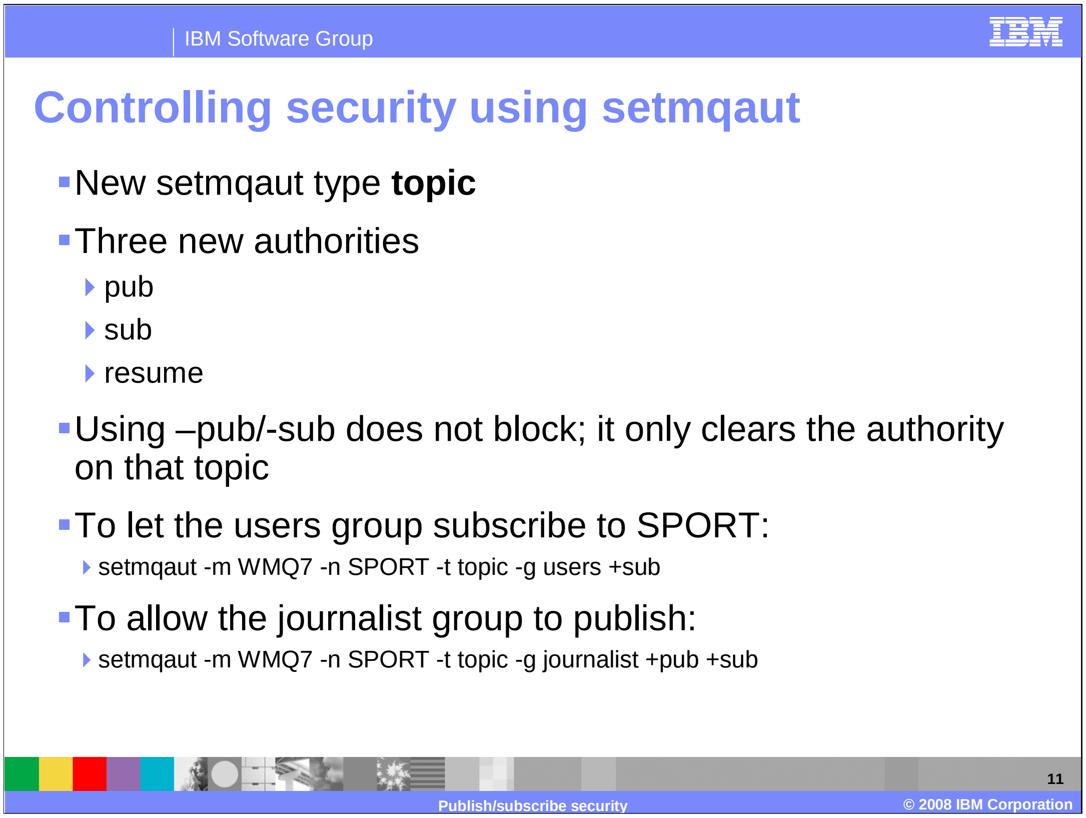
Section

Object authority manager

10

Publish/subscribe security

This section provides information on using the object authority manager (OAM) to control security in a publish/subscribe network on distributed platforms.



IBM Software Group

Controlling security using setmqaut

- New setmqaut type **topic**
- Three new authorities
  - pub
  - sub
  - resume
- Using –pub/-sub does not block; it only clears the authority on that topic
- To let the users group subscribe to SPORT:
  - setmqaut -m WMQ7 -n SPORT -t topic -g users +sub
- To allow the journalist group to publish:
  - setmqaut -m WMQ7 -n SPORT -t topic -g journalist +pub +sub

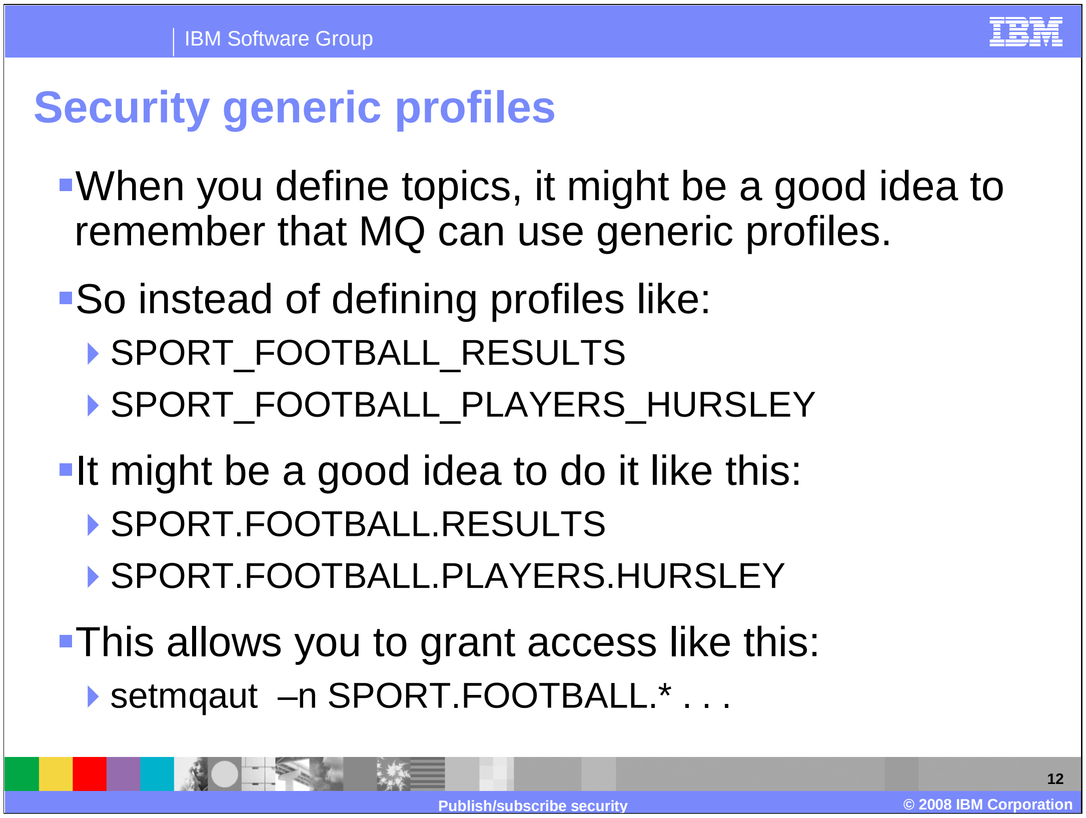
11

Publish/subscribe security

The **setmqaut** command is used to change the authorizations to a profile, object, or class of objects. Authorizations can be granted to, or revoked from, any number of principals or groups. The type ‘topic’ is used to control security for publish/subscribe topics. There are three authorities associated with type ‘topic’.

Use ’+pub’ to publish a message on a topic using the MQPUT call. Use ‘+resume’ to resume a subscription using the MQSUB call. Use ‘+sub’ to create, alter or resume a subscription to a topic using the MQSUB call.

Using –pub and -sub does not block the publication or subscription. It just clears the authority on that topic, so OAM will look higher in the tree for a +pub and +sub.



IBM Software Group

Security generic profiles

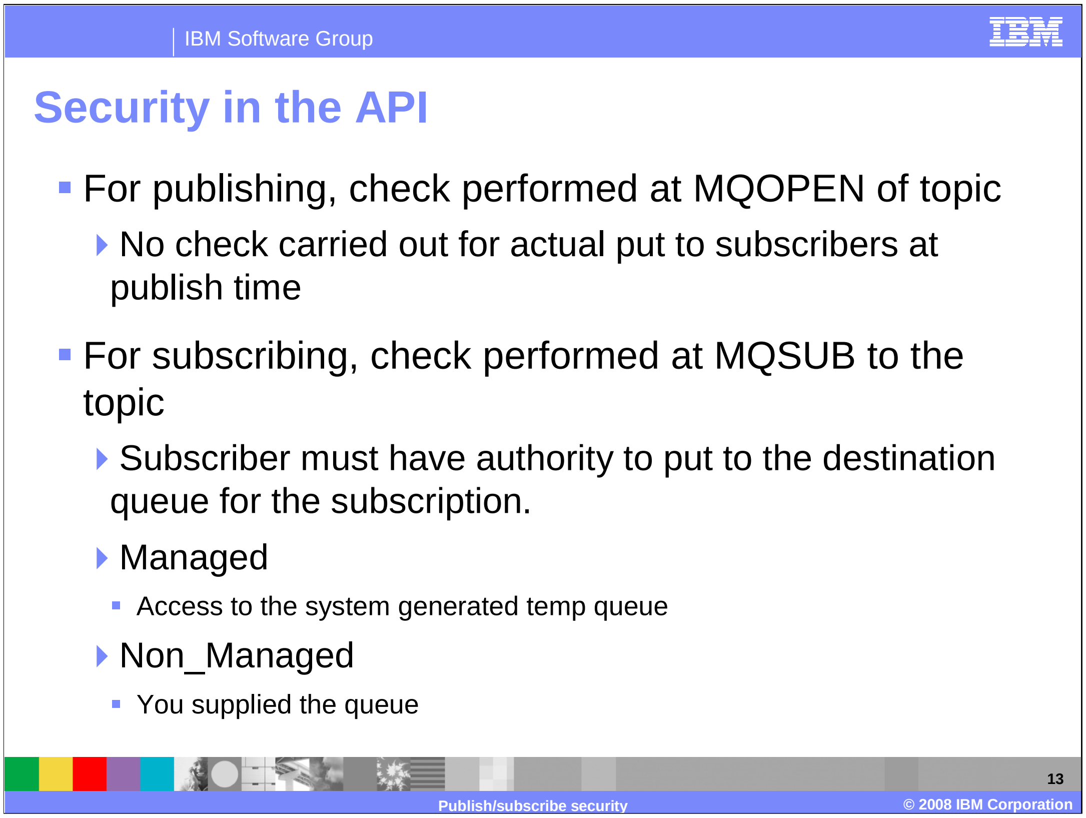
- When you define topics, it might be a good idea to remember that MQ can use generic profiles.
- So instead of defining profiles like:
  - SPORT_FOOTBALL_RESULTS
  - SPORT_FOOTBALL_PLAYERS_HURSLEY
- It might be a good idea to do it like this:
  - SPORT.FOOTBALL.RESULTS
  - SPORT.FOOTBALL.PLAYERS.HURSLEY
- This allows you to grant access like this:
  - setmqaut –n SPORT.FOOTBALL.* . . .

12

Publish/subscribe security

© 2008 IBM Corporation

OAM generic profiles enable you to set the authority a user has to many objects at once, rather than having to issue separate **setmqaut** commands against each individual object when it is created. Using generic profiles in the **setmqaut** command enables you to set a generic authority for all objects that fit that profile. What makes a profile generic is the use of wildcard characters in the profile name. In the example shown here, the setmqaut command applies to both SPORT.FOOTBALL.RESULTS and SPORT.FOOTBALL.PLAYERS.HURSLEY.



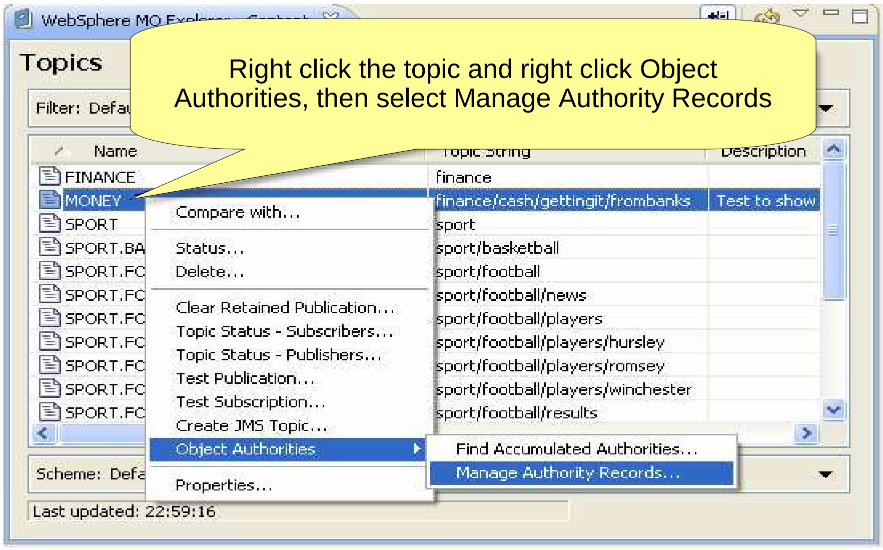
Security in the API

- For publishing, check performed at MQOPEN of topic
  - No check carried out for actual put to subscribers at publish time
- For subscribing, check performed at MQSUB to the topic
  - Subscriber must have authority to put to the destination queue for the subscription.
  - Managed
    - Access to the system generated temp queue
  - Non_Managed
    - You supplied the queue

When publishing, a check is performed at the MQOPEN of the topic you want to publish to. No check is carried out for actual put to subscribers at publish time; that is carried out at subscribe time.

When subscribing, a check is carried out when an MQSUB to the specified topic is received. The subscriber must also have authority to put to the destination queue for the subscription. This is either the system generated temporary queue or the queue you supplied.

Controlling security using MQ Explorer (1 of 5)



Right click the topic and right click Object Authorities, then select Manage Authority Records

Topics

Filter: Defa

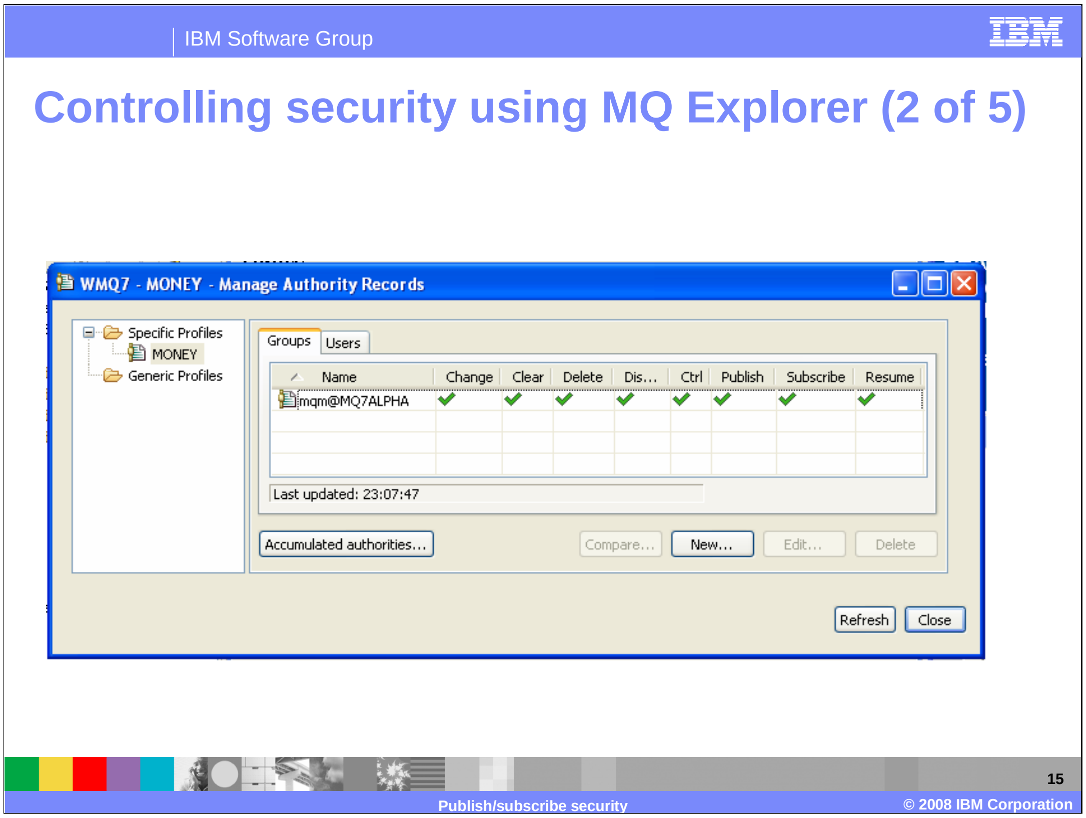
Name	Topic String	Description
FINANCE	finance	
MONEY	finance/cash/gettingit/frombanks	Test to show
SPORT	sport	
SPORT.BA	sport/basketball	
SPORT.FC	sport/football	
SPORT.FC	sport/football/news	
SPORT.FC	sport/football/players	
SPORT.FC	sport/football/players/hursley	
SPORT.FC	sport/football/players/romsey	
SPORT.FC	sport/football/players/winchester	
SPORT.FC	sport/football/results	

Scheme: Defa

Last updated: 22:59:16

WebSphere MQ Explorer - Content
Compare with...
Status...
Delete...
Clear Retained Publication...
Topic Status - Subscribers...
Topic Status - Publishers...
Test Publication...
Test Subscription...
Create JMS Topic...
Object Authorities
Properties...
Find Accumulated Authorities...
Manage Authority Records...

You can also use MQ Explorer to manage security on topics. First, select TOPICS and open Manage Authority Records.



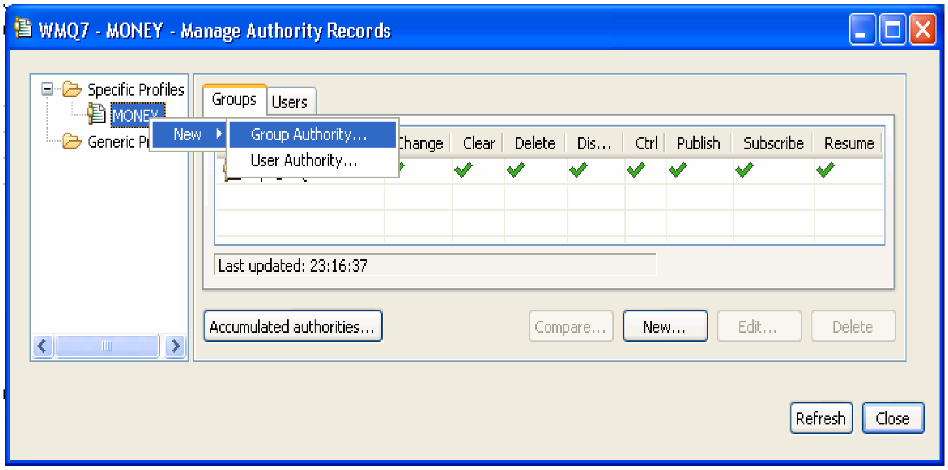
Controlling security using MQ Explorer (2 of 5)

Name	Change	Clear	Delete	Dis…	Ctrl	Publish	Subscribe	Resume
mqm@MQ7ALPHA	✓	✓	✓	✓	✓	✓	✓	✓

Last updated: 23:07:47

You can see which groups have access to the topic. In this example, there is only the default mqm group.

Controlling security using MQ Explorer (3 of 5)

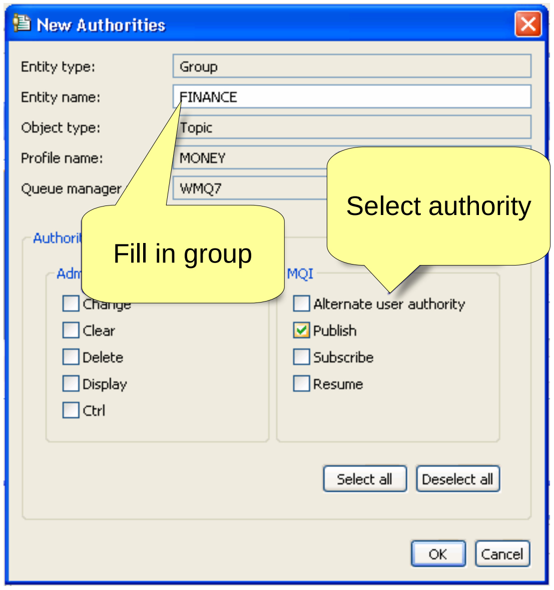


Change	Clear	Delete	Dis...	Ctrl	Publish	Subscribe	Resume
✓	✓	✓	✓	✓	✓	✓	✓

Last updated: 23:16:37

You can grant authority to another group. In this example, FINANCE group is selected to grant access to the MONEY topic.

Controlling security using MQ Explorer (4 of 5)



New Authorities

Entity type: Group

Entity name: FINANCE

Object type: Topic

Profile name: MONEY

Queue manager: WMQ7

Authori

Adm

- □ Change
- □ Clear
- □ Delete
- □ Display
- □ Ctrl

MQI

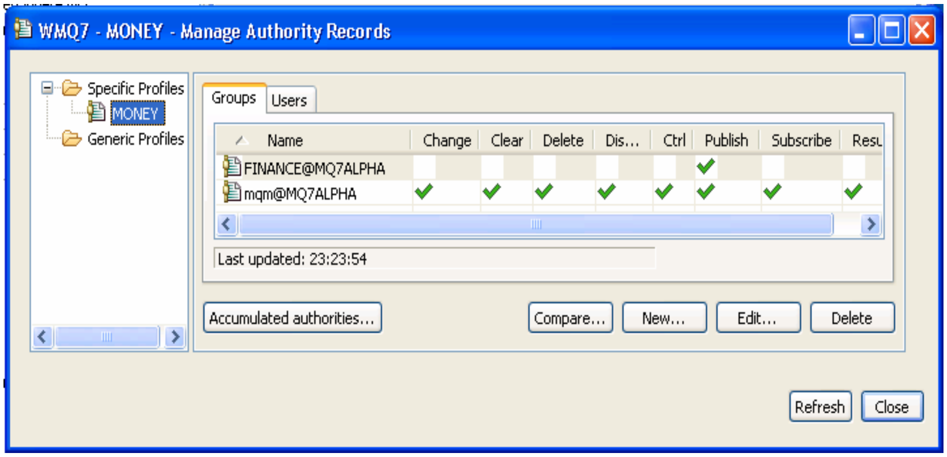
- □ Alternate user authority
- ☑ Publish
- □ Subscribe
- □ Resume

Fill in group

Select authority

To complete, fill in the group name, FINANCE, and select the authorities.

Controlling security using MQ Explorer (5 of 5)

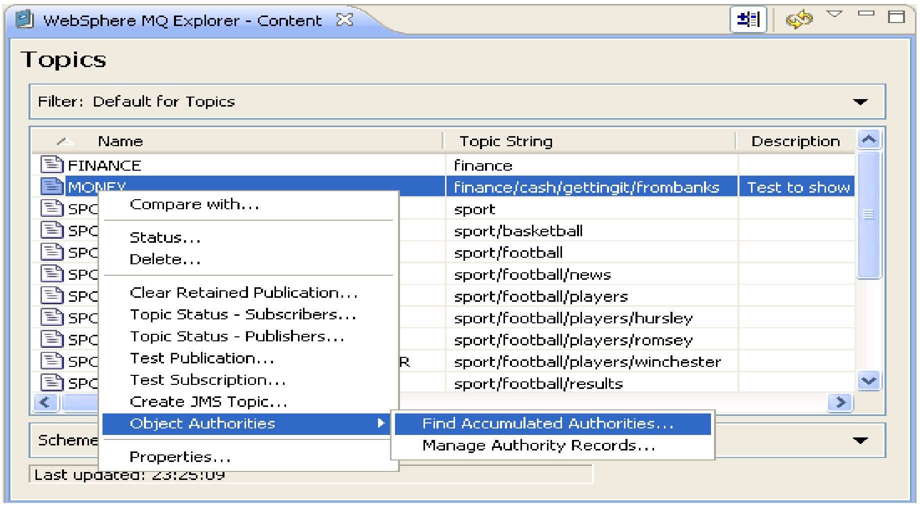


Name	Change	Clear	Delete	Dis...	Ctrl	Publish	Subscribe	Resu
FINANCE@MQ7ALPHA						✓		
mqm@MQ7ALPHA	✓	✓	✓	✓	✓	✓	✓	✓

Last updated: 23:23:54

Now when you display the authorities on MONEY, you see that FINANCE group now has publish authority.

Check TOPIC security with MQ Explorer (2 of 3)

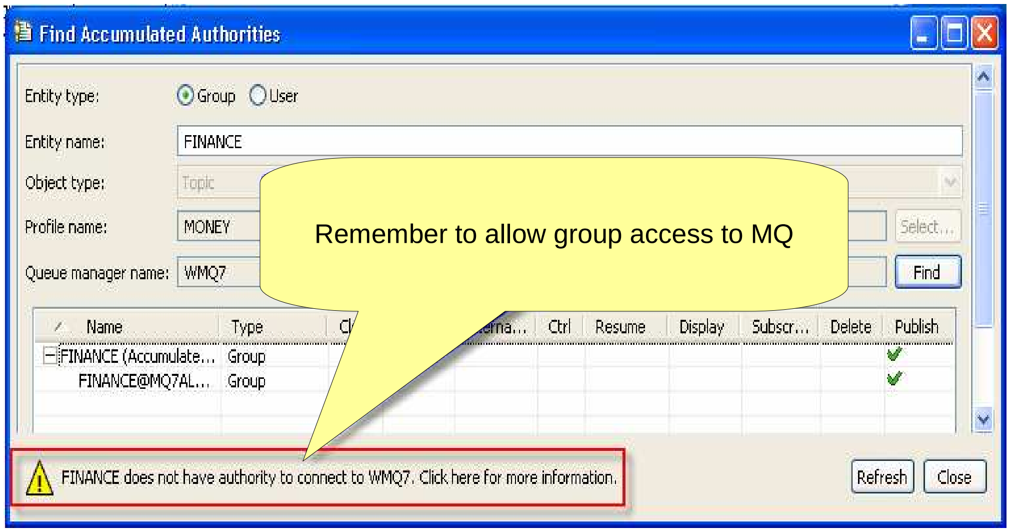

WebSphere MQ Explorer - Content
Topics
Filter: Default for Topics
Compare with...
Status...
Delete...
Clear Retained Publication...
Topic Status - Subscribers...
Topic Status - Publishers...
Test Publication...
Test Subscription...
Create JMS Topic...
Object Authorities
Find Accumulated Authorities...
Manage Authority Records...
Properties...
Scheme
Last updated: 23:25:09

Name	Topic String	Description
FINANCE	finance	
MONEY	finance/cash/gettingit/frombanks	Test to show
SPC	sport	
SPC	sport/basketball	
SPC	sport/football	
SPC	sport/football/news	
SPC	sport/football/players	
SPC	sport/football/players/hursley	
SPC	sport/football/players/romsey	
SPC R	sport/football/players/winchester	
SPC	sport/football/results	

To check TOPIC security with MQ Explorer, click on Find Accumulated Authorities.

IBM Software Group

Check TOPIC security with MQ Explorer (2 of 3)



Entity type: ● Group ○ User

Entity name: FINANCE

Object type: Topic

Profile name: MONEY

Queue manager name: WMQ7

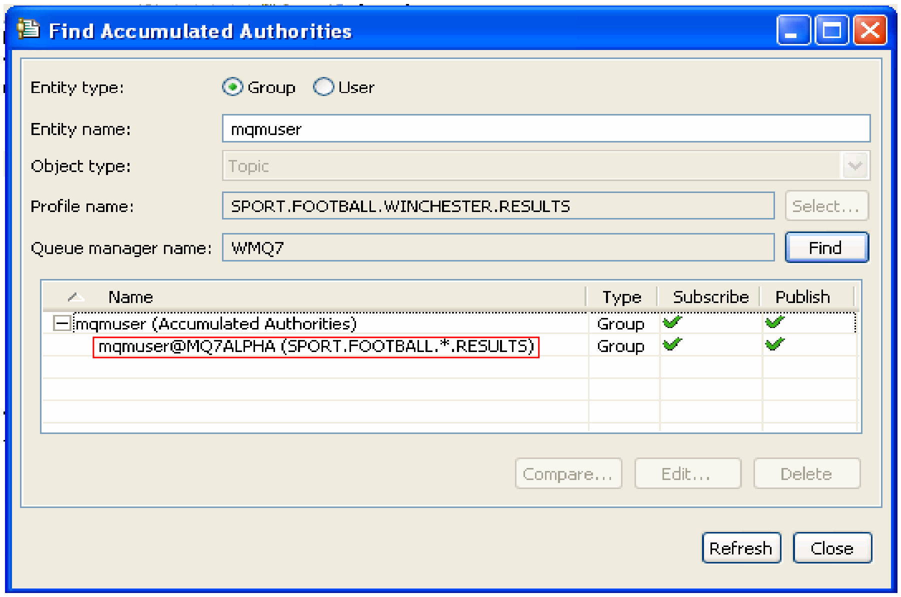
Name	Type	Cl	...erna...	Ctrl	Resume	Display	Subscr...	Delete	Publish
FINANCE (Accumulate...	Group								✓
FINANCE@MQ7AL...	Group								✓

FINANCE does not have authority to connect to WMQ7. Click here for more information.

Remember to allow group access to MQ

When asking about group FINANCE, there is an error since group FINANCE does not have access to the queue manager.

Check TOPIC security with MQ Explorer (3 of 3)



Entity type: ● Group ○ User

Entity name: mqmuser

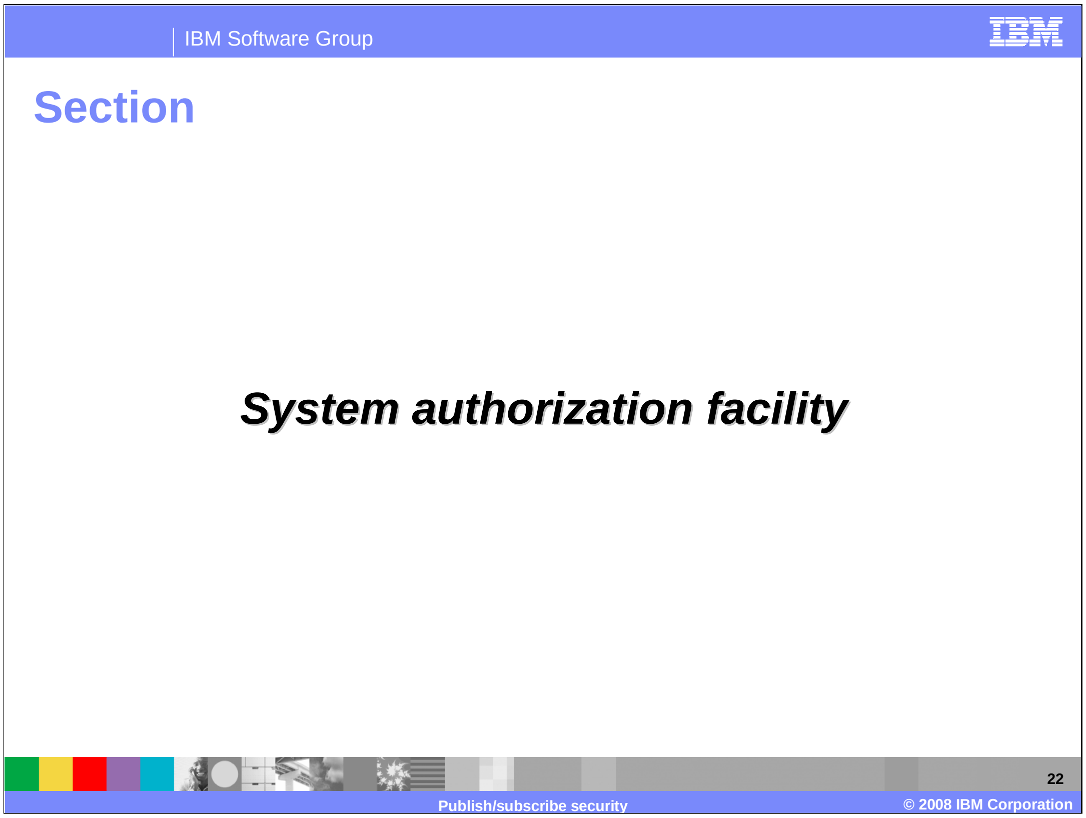
Object type: Topic

Profile name: SPORT.FOOTBALL.WINCHESTER.RESULTS

Queue manager name: WMQ7

Name	Type	Subscribe	Publish
mqmuser (Accumulated Authorities)	Group	✓	✓
mqmuser@MQ7ALPHA (SPORT.FOOTBALL.*.RESULTS)	Group	✓	✓

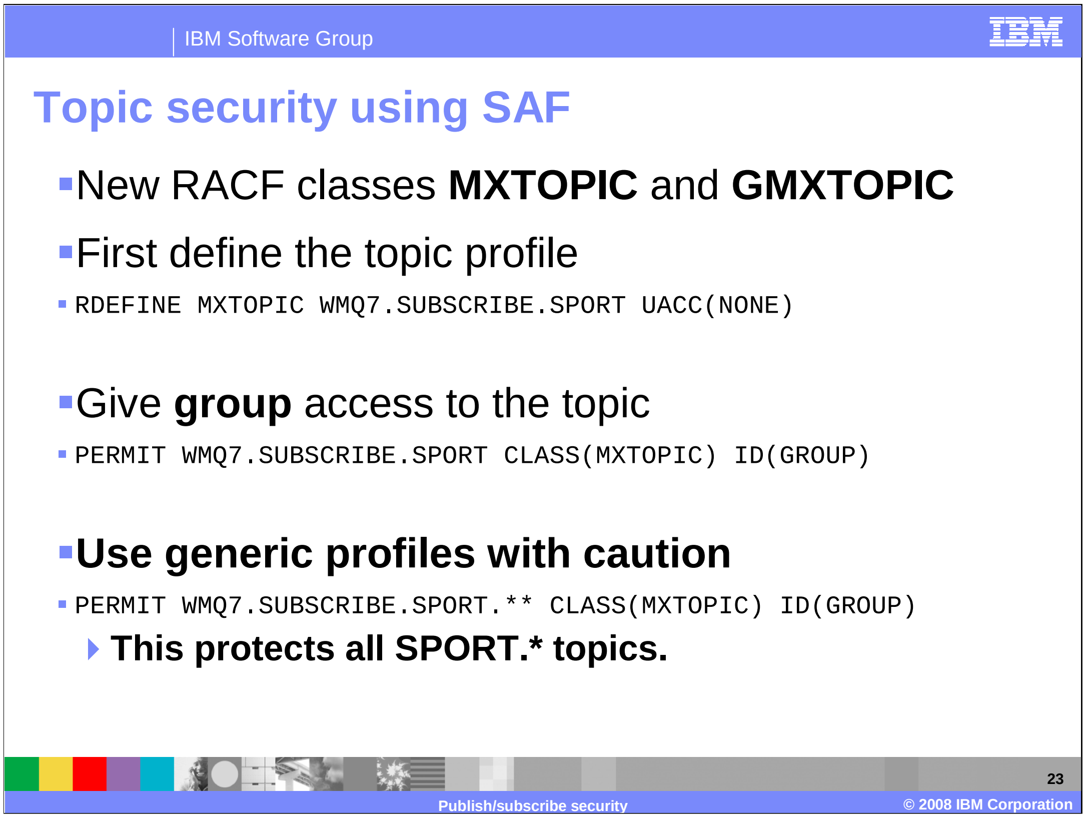
When the entity does have access to the queue manager, the display is rendered.



Section

System authorization facility

This section provides information on using a system authorization facility (SAF), such as RACF$^{®}$, to control security in a publish/subscribe network on distributed platforms.

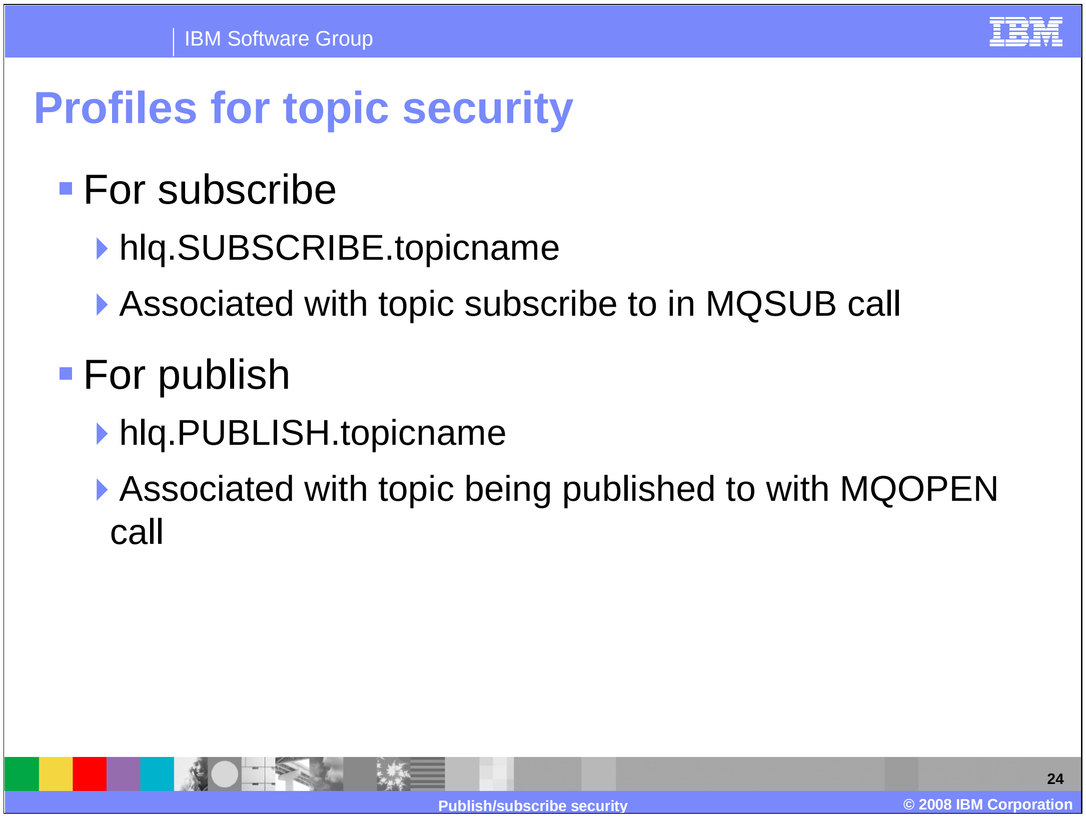


Topic security using SAF

- New RACF classes **MXTOPIC** and **GMXTOPIC**
- First define the topic profile
  - `RDEFINE MXTOPIC WMQ7.SUBSCRIBE.SPORT UACC(NONE)`
- Give **group** access to the topic
  - `PERMIT WMQ7.SUBSCRIBE.SPORT CLASS(MXTOPIC) ID(GROUP)`
- **Use generic profiles with caution**
  - `PERMIT WMQ7.SUBSCRIBE.SPORT.** CLASS(MXTOPIC) ID(GROUP)`
    - **This protects all SPORT.* topics.**

If topic security is active, you must define profiles in the MXTOPIC or GMXTOPIC classes.

Permit the necessary groups or user IDs access to these profiles, so that they can issue WebSphere MQ API requests that use topics.



IBM Software Group

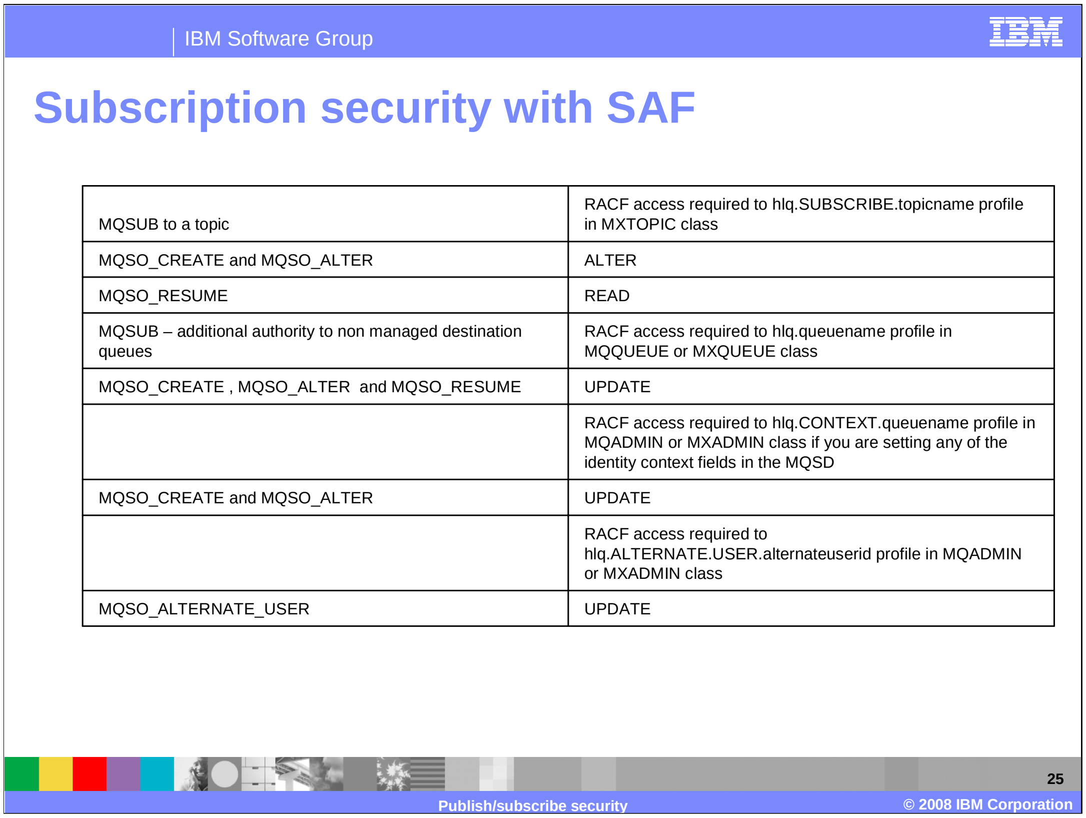
Profiles for topic security

- For subscribe
  - hlq.SUBSCRIBE.topicname
  - Associated with topic subscribe to in MQSUB call
- For publish
  - hlq.PUBLISH.topicname
  - Associated with topic being published to with MQOPEN call

24

Publish/subscribe security

Profiles for topic security take the form shown here. Hlq can be either queue manager name or queue-sharing group name. Topicname is the name of the topic administration node in the topic tree, associated either with the topic being subscribed to through an MQSUB call, or being published to through an MQOPEN call.

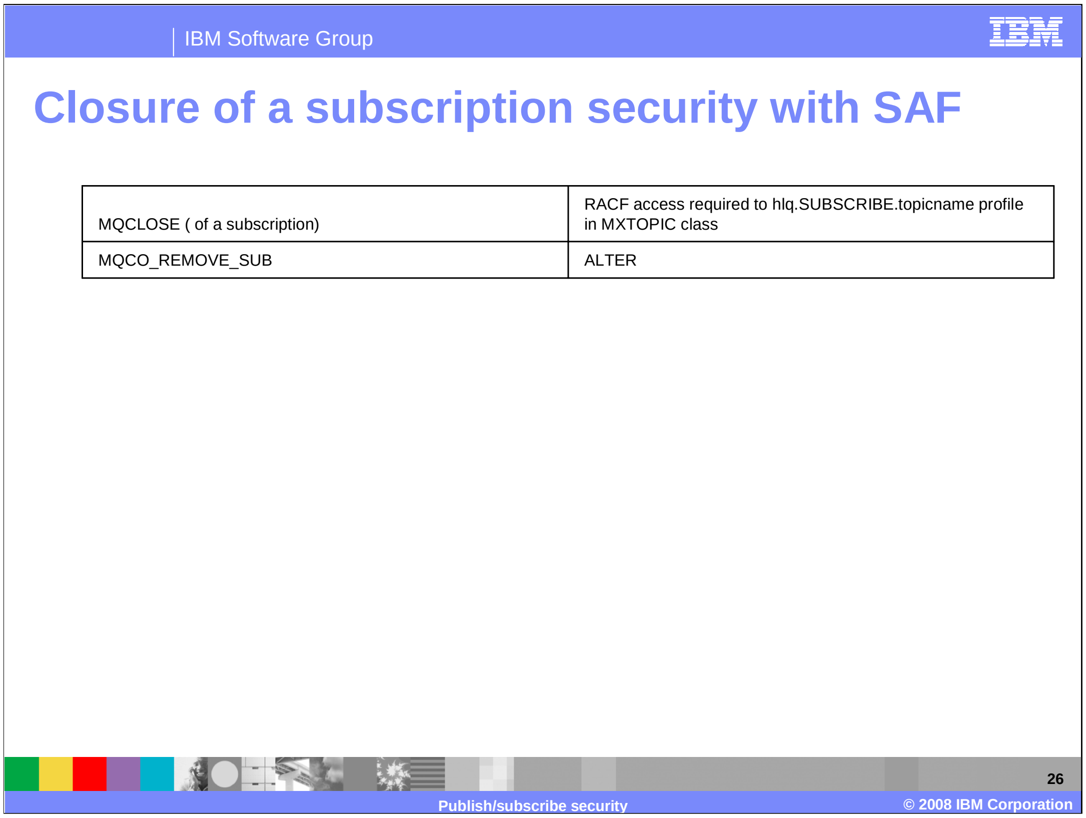


Subscription security with SAF

MQSUB to a topic	RACF access required to hlq.SUBSCRIBE.topicname profile in MXTOPIC class
MQSO_CREATE and MQSO_ALTER	ALTER
MQSO_RESUME	READ
MQSUB – additional authority to non managed destination queues	RACF access required to hlq.queuename profile in MQQUEUE or MXQUEUE class
MQSO_CREATE , MQSO_ALTER and MQSO_RESUME	UPDATE
	RACF access required to hlq.CONTEXT.queuename profile in MQADMIN or MXADMIN class if you are setting any of the identity context fields in the MQSD
MQSO_CREATE and MQSO_ALTER	UPDATE
	RACF access required to hlq.ALTERNATE.USER.alternateuserid profile in MQADMIN or MXADMIN class
MQSO_ALTERNATE_USER	UPDATE

In order to subscribe to a topic, you need access to both the topic you are trying to subscribe to, and the target queue for the publications. When you issue an MQSUB request, a check is made to ensure that you are allowed to subscribe to that topic, and that the target queue, if specified, is opened for output. You must also have the appropriate level of access to that target queue.

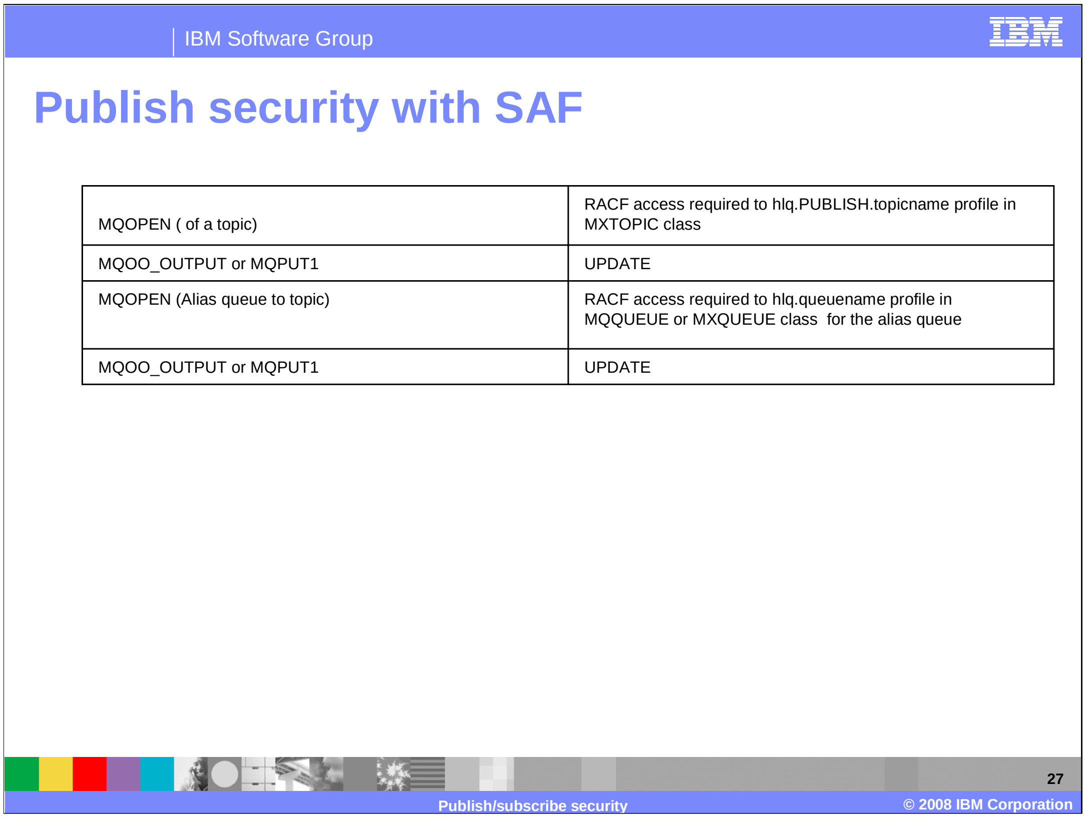
The table shown here lists the access levels required for topic security to subscribe.



Closure of a subscription security with SAF

MQCLOSE (of a subscription)	RACF access required to hlq.SUBSCRIBE.topicname profile in MXTOPIC class
MQCO_REMOVE_SUB	ALTER

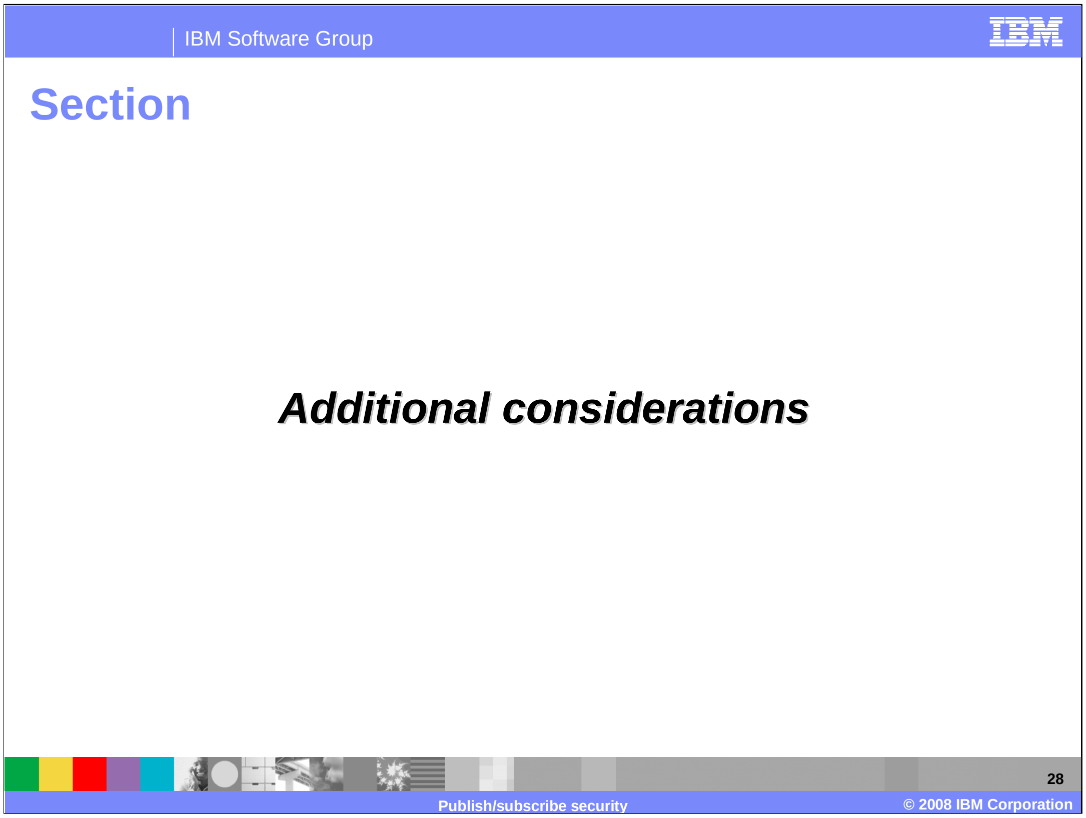
If you explicitly issue an MQCLOSE call for a subscription with the MQCO_REMOVE_SUB option specified, and you did not create the subscription you are closing under this handle, a security check is performed at the time of closure to ensure that you have the correct authority to perform the operation. The table shown here lists access levels required to profiles for topic security for closure of a subscribe operation.



Publish security with SAF

MQOPEN (of a topic)	RACF access required to hlq.PUBLISH.topicname profile in MXTOPIC class
MQOO_OUTPUT or MQPUT1	UPDATE
MQOPEN (Alias queue to topic)	RACF access required to hlq.queuename profile in MQQUEUE or MXQUEUE class for the alias queue
MQOO_OUTPUT or MQPUT1	UPDATE

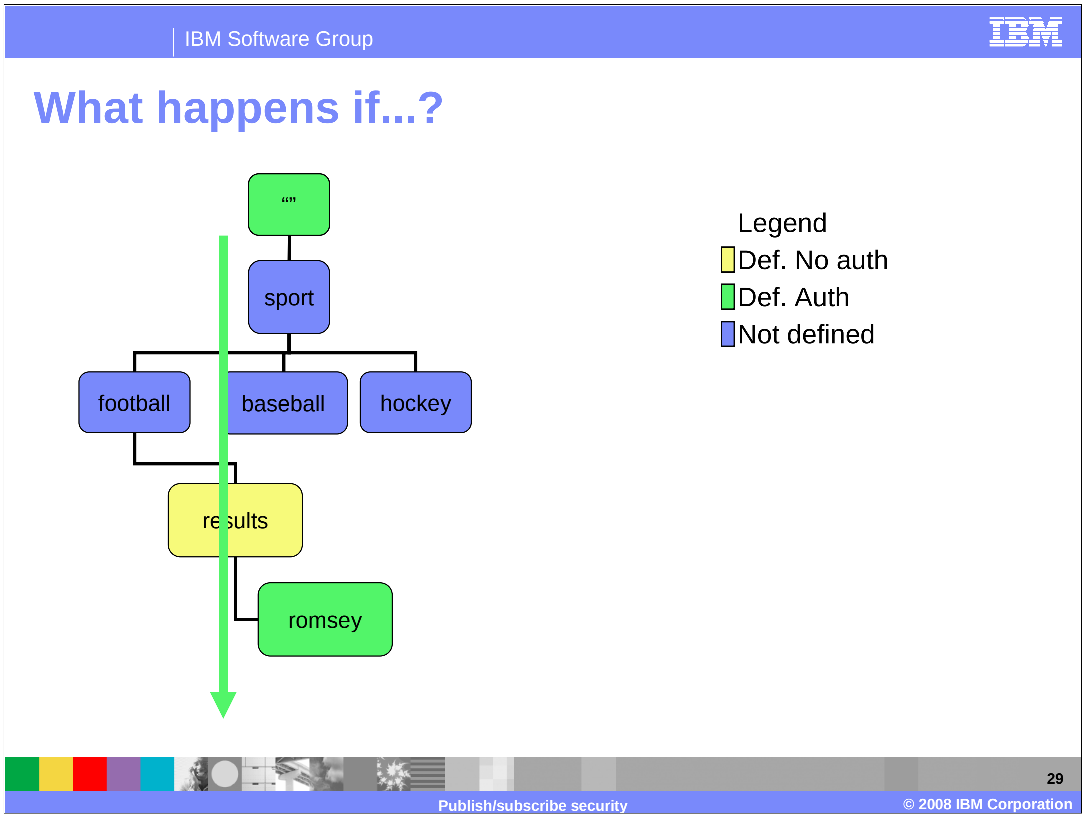
In order to publish on a topic you need access to the topic and, if you are using alias queues, to the alias queue as well. This table shows access levels required to profiles for topic security for a publish operation.



Section

Additional considerations

This section explains how security works given your topic architecture.



IBM Software Group

What happens if...?

“”

sport

football

baseball

hockey

results

romsey

Legend

🟨 Def. No auth

🟩 Def. Auth

🟦 Not defined

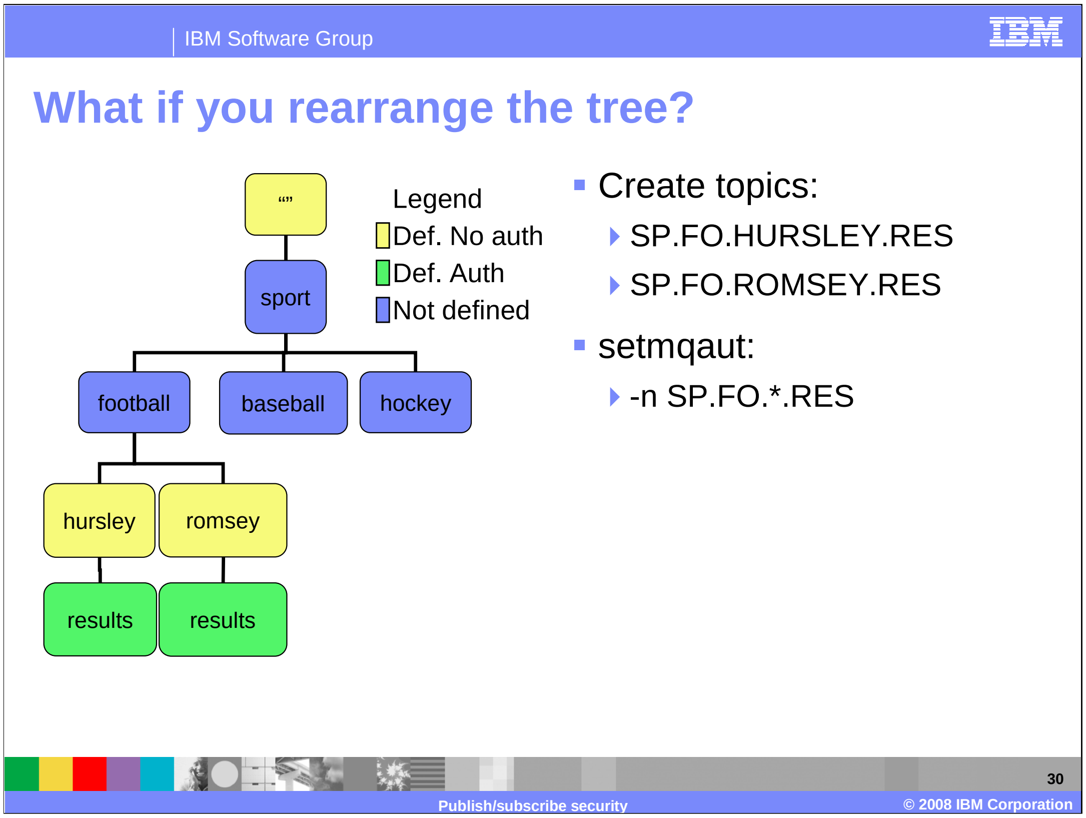
29

Publish/subscribe security

© 2008 IBM Corporation

Consider what happens if you grant publish and subscribe at the root level (SYSTEM.BASIC.TOPIC). This means that everyone has authority to everything.

Also in this example only members of the results group are allowed to publish to the results room. But the results room has been moved up the tree for ease of administration. But that means that any additional clubs can publish results to the same place and the results would not be specific to each club.



What if you rearrange the tree?

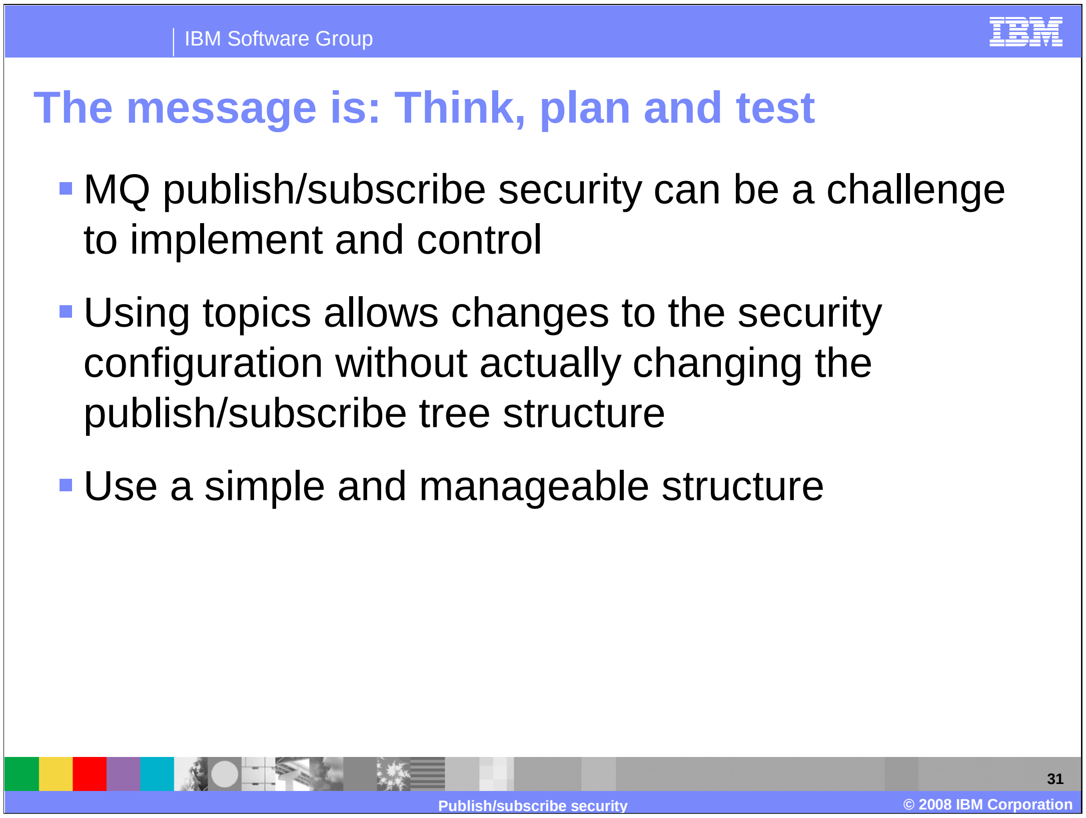
“”
sport
football
baseball
hockey
hursley
romsey
results
results

Legend
🟨Def. No auth
🟩Def. Auth
🟦Not defined

- Create topics:
  - SP.FO.HURSLEY.RES
  - SP.FO.ROMSEY.RES
- setmqaut:
  - -n SP.FO.*.RES

Here, the results have been placed under the clubs so there is no confusion about where the results belong.

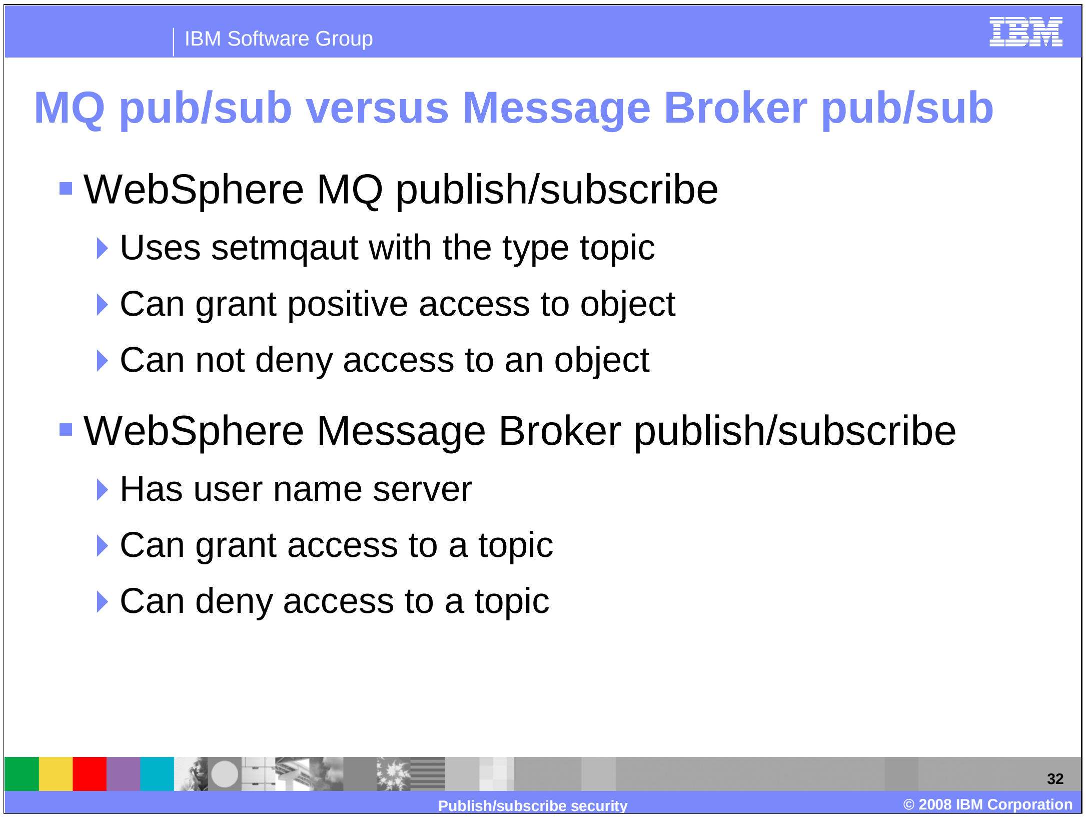
Create new topics as shown here. Use a generic profile to protect the results for ease of administration.



The message is: Think, plan and test

- MQ publish/subscribe security can be a challenge to implement and control
- Using topics allows changes to the security configuration without actually changing the publish/subscribe tree structure
- Use a simple and manageable structure

It is not a trivial job to design publish/subscribe security. You need to have a good plan and consider what parts of the topic tree need to be protected. Publish/subscribe security is similar to normal MQ security except it involves topic objects and topic strings.



IBM Software Group

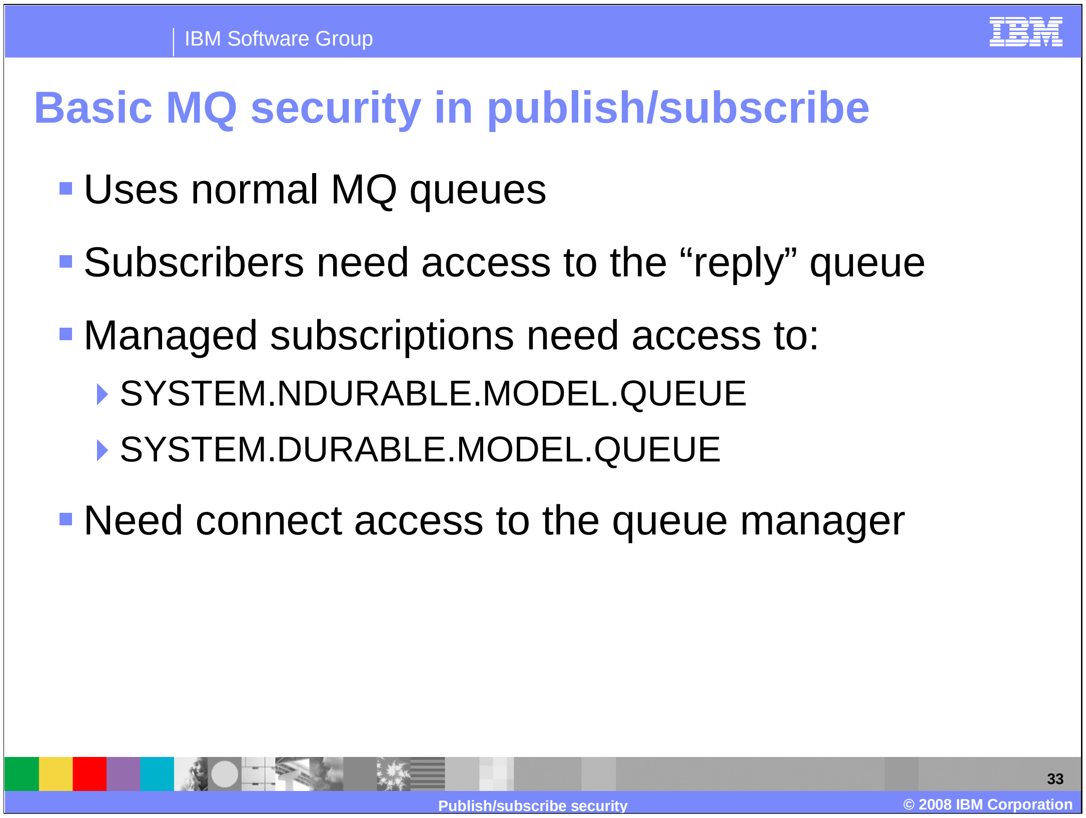
MQ pub/sub versus Message Broker pub/sub

- WebSphere MQ publish/subscribe
  - Uses setmqaut with the type topic
  - Can grant positive access to object
  - Can not deny access to an object
- WebSphere Message Broker publish/subscribe
  - Has user name server
  - Can grant access to a topic
  - Can deny access to a topic

32

Publish/subscribe security

WebSphere MQ publish/subscribe security uses topic objects to provide security. However, you can only grant positive access, not deny access to a topic. In WebSphere Message Broker publish/subscribe, a User Name Server can be used to grant and deny access to topics.



IBM Software Group

Basic MQ security in publish/subscribe

- Uses normal MQ queues
- Subscribers need access to the “reply” queue
- Managed subscriptions need access to:
  - SYSTEM.NDURABLE.MODEL.QUEUE
  - SYSTEM.DURABLE.MODEL.QUEUE
- Need connect access to the queue manager

33

Publish/subscribe security

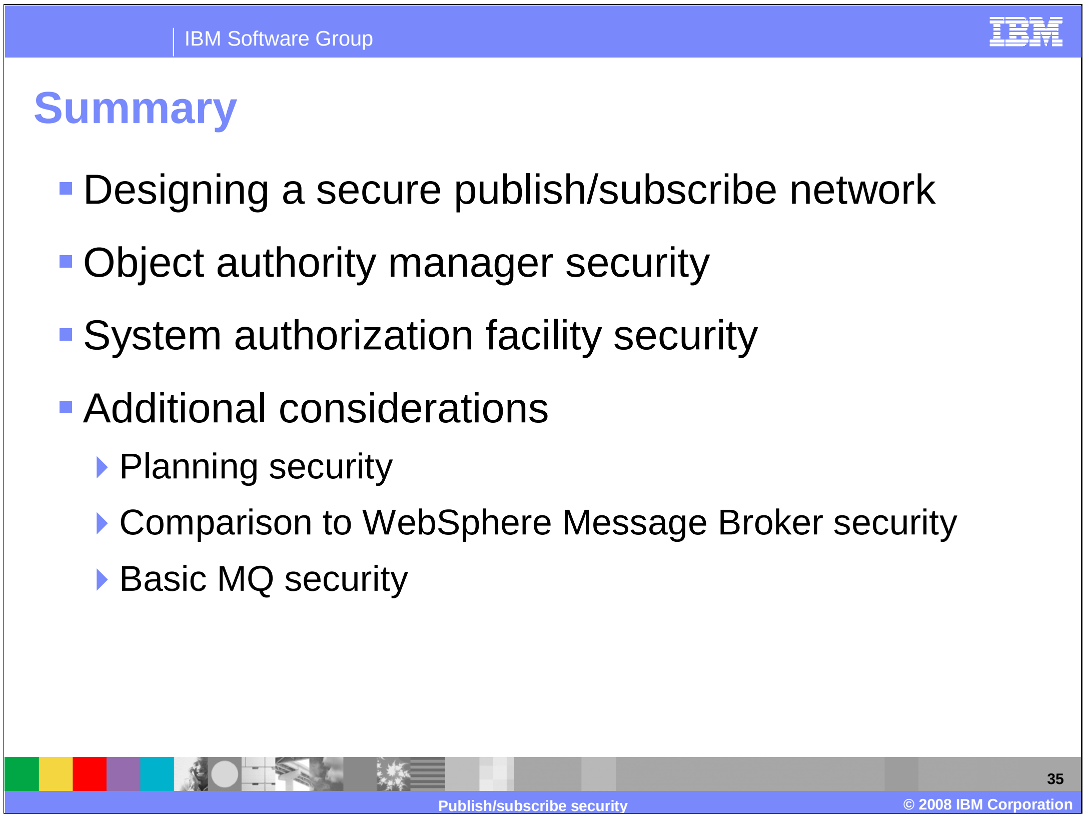
© 2008 IBM Corporation

WebSphere MQ publish/subscribe uses normal queues. Subscribers need access to the reply queue. When using managed subscriptions, access to the model queues listed here is required. Ability to connect to the queue manager is also required.

Section

Summary

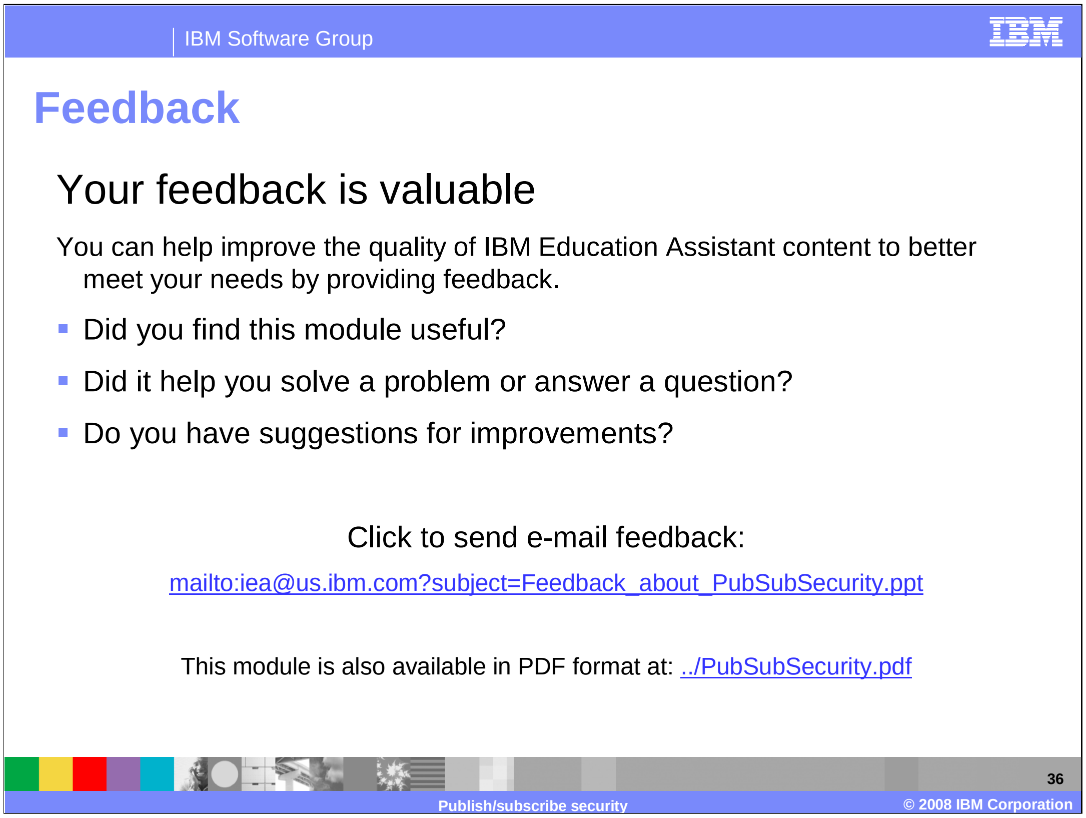
This section summarizes publish/subscribe security in WebSphere MQ V7.



Summary

- Designing a secure publish/subscribe network
- Object authority manager security
- System authorization facility security
- Additional considerations
  - Planning security
  - Comparison to WebSphere Message Broker security
  - Basic MQ security

This module discussed how to design a secure publish/subscribe network in WebSphere MQ V7. It covered how to set up security using OAM on distributed platforms and how to use RACF to implement security on z/OS. Additional security planning considerations were presented.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

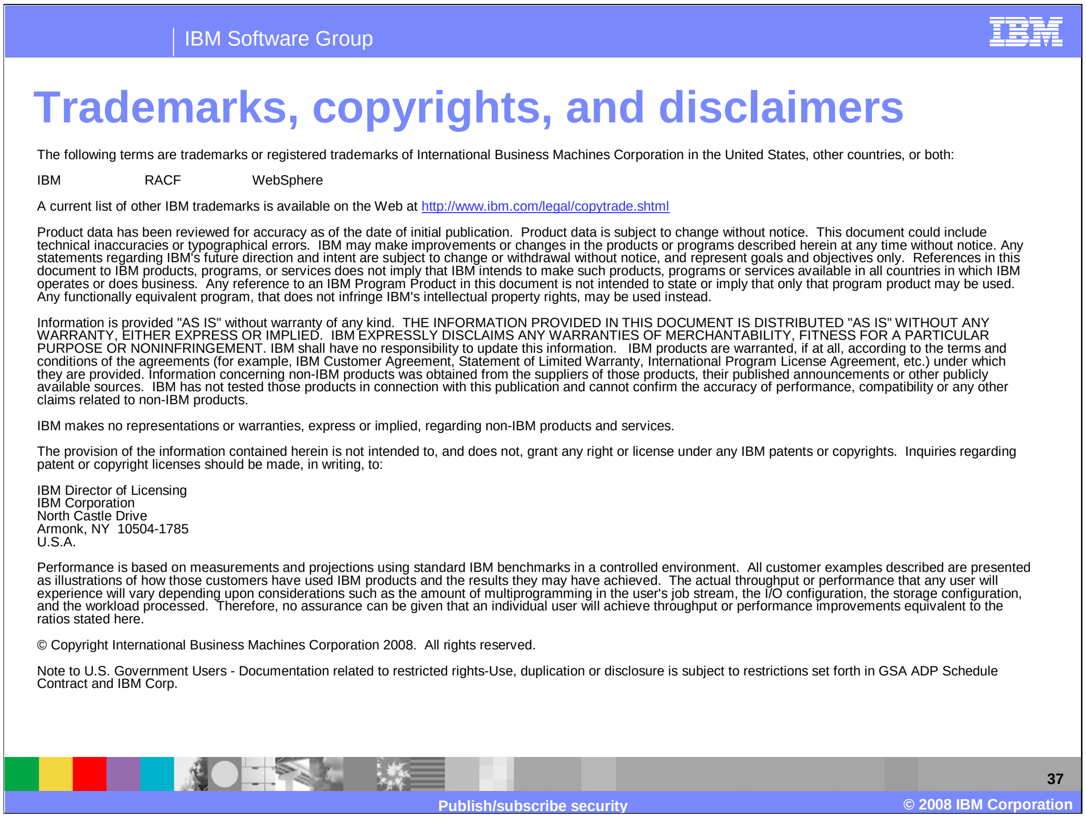
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_PubSubSecurity.ppt

This module is also available in PDF format at: ../PubSubSecurity.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, copyrights, and disclaimers

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

IBM RACF WebSphere

A current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.