IBM Tivoli Composite Application Manager for Applications
Version 7.3

WebSphere MQ Configuration Agent User's Guide

SC14-7525-01

IBM Tivoli Composite Application Manager for Applications
Version 7.3

WebSphere MQ Configuration Agent User's Guide

SC14-7525-01

Note!

Before using this information and the product it supports, read the information in “Notices” on page 289.

This edition applies to version 7.3 of WebSphere MQ Configuration agent (product number 5725-I45) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

Chapter 1. Introducing WebSphere MQ Configuration agent

This topic provides an overview of WebSphere® MQ Configuration agent and explains how it can help you manage the configuration of your WebSphere MQ environment.

It also contains a scenario that is designed to explain how the elements of WebSphere MQ Configuration agent work together to help you ensure a cohesive network whose interrelationships are correctly defined.

Building a network for your WebSphere MQ messaging middleware can be a slow and difficult task. As your network grows and queue managers span dozens of systems running on a variety of operating systems, it becomes even more difficult to determine where and how to configure new queue managers and their resources.

The WebSphere MQ Configuration agent simplifies the tasks of defining your configuration of WebSphere MQ. You can use WebSphere MQ Configuration agent to do the following tasks:

- Manage your WebSphere MQ network, including local or remote nodes, from a single point of control
- See how your WebSphere MQ queue managers and resources are related by viewing a hierarchical representation of your entire network
- Manipulate WebSphere MQ objects across one or more networks of queue managers from a single workstation
- Base configurations on prototype models so you can implement global updates with the click of a mouse
- Save time and resources by doing many difficult development tasks automatically
- Group related WebSphere MQ resources together in ways that reflect the business-oriented relationships between them and the logical structure of your enterprise

New in version 7.3

Version 7.3 of WebSphere MQ Configuration agent has the following changes and enhancements:

- Support of IBM® MQ V8.0 is provided.

Supported versions of WebSphere MQ

WebSphere MQ Configuration agent supports the following versions of WebSphere MQ:

- On distributed systems:
  - WebSphere MQ 6.0
  - WebSphere MQ 7.0
  - WebSphere MQ 7.0.1
- On z/OS® systems:
  - WebSphere MQ 6.0

- WebSphere MQ 7.0
- WebSphere MQ 7.0.1

Remember: A client component of WebSphere MQ must be installed on the same system where the WebSphere MQ Configuration agent is installed and running.

IBM Tivoli Monitoring

IBM Tivoli® Monitoring manages system and network applications on several operating systems and keeps track of the availability and performance of all parts of your enterprise. It provides IBM Tivoli OMEGAMON® XE products with a common agent-server-client architecture, which is shown in Figure 1

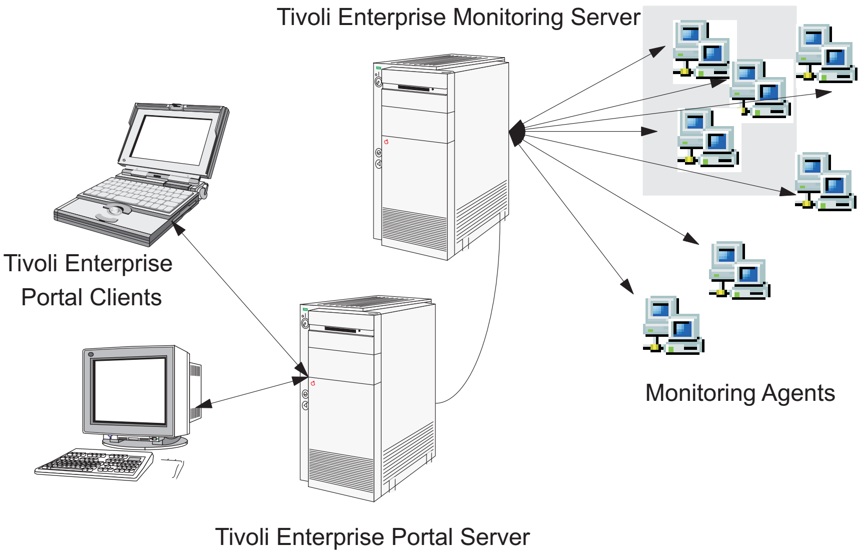

Tivoli Enterprise Monitoring Server
Tivoli Enterprise
Portal Clients
Monitoring Agents
Tivoli Enterprise Portal Server

Figure 1. Agent–Server–Client Architecture

Tivoli Enterprise Monitoring Server

Tivoli Enterprise Monitoring Server (monitoring server) gathers data from the Tivoli Enterprise Monitoring agents and acts as a collection and control point for alerts that are received from the agents. The monitoring server sends the data that it receives from the agents to Tivoli Enterprise Portal clients, where it is displayed in tabular or graphic views in a set of predefined or customized workspaces. The monitoring server also accepts requests for information or action from Tivoli Enterprise Portal clients and distributes them to the agents for processing.

Tivoli Enterprise Portal

Tivoli Enterprise Portal (portal) is the user interface to the data monitoring and management resources of IBM Tivoli Monitoring. Depending on how it is installed, Tivoli Enterprise Portal can be used as either a desktop or a browser-based client.

Tivoli Enterprise Portal has its own server, Tivoli Enterprise Portal Server (portal server). Tivoli Enterprise Portal Server performs common Tivoli Enterprise Portal functions, which reduces the processing that is performed by the Tivoli Enterprise Portal client.

Tivoli Enterprise Monitoring agent

Tivoli Enterprise Monitoring agents collect system or application data from monitored, or *managed*, systems. The WebSphere MQ Monitoring agent, for example, can be used to easily collect and analyze WebSphere MQ-specific data for all your remote and local queue managers. The data is passed to the Tivoli Enterprise Monitoring Server and displayed in the Tivoli Enterprise Portal client.

Tivoli Enterprise Monitoring agents can also compare the current values of monitored properties against a set of defined conditions, and trigger alerts or actions when those conditions occur. They can accept and perform requested actions that are relayed to them from Tivoli Enterprise Portal clients by the Tivoli Enterprise Monitoring Server.

Configuration agents can create and configure objects. The WebSphere MQ Configuration agent can configure objects such as WebSphere MQ queue managers and their components (queues, channels, processes, and other objects).

Agent Management Services

With IBM Tivoli Monitoring 6.2.2, WebSphere MQ Configuration agent can be managed by the Agent Management Services. These services are available in the OS Monitoring Agent for Windows, Linux, and UNIX systems, and are designed to keep WebSphere MQ Configuration agent available and to provide information about its status to the Tivoli Enterprise Portal. More information about Agent Management Services can be found at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.2/itm_agentmgmtsvcs_intro.htm.

IBM Tivoli OMEGAMON XE

The IBM Tivoli OMEGAMON DE feature package for Tivoli Enterprise Portal offers a process-driven view of your enterprise. You can use it to bring together information from disparate sources, including a range of operating systems, servers, databases, mainframes, and network and Internet components, which is displayed in one workspace. You can also use it to create a single point of control from which you can manage all the resources that your business-critical applications rely on.

Tivoli OMEGAMON DE has the following extended capabilities:

- Enterprise-specific Navigator views

  The Navigator physical view displays the hierarchy of your managed enterprise by operating system and type of Tivoli Enterprise Monitoring agents. The Navigator business view offered by Tivoli OMEGAMON DE displays the hierarchy of managed objects. You can also define Navigator views for any logical groupings, such as business processes or departmental hierarchy.
- Views of data from different types of monitoring agents in one workspace

  In a single workspace, you can build a table or chart with data from one type of monitoring agent, and another table or chart with data from a different agent. Within that workspace, you can show views from as many different agent types as are included on that branch of the Navigator.
- Linking application workspaces

  You can define links from a workspace that is associated with one type of monitoring agent to workspaces that are associated with other types of agents.

WebSphere MQ Configuration agent

The WebSphere MQ Configuration agent is based on a agent-server-client architecture as show in Figure 1 on page 2:

- **Client:**

  The Tivoli Enterprise Portal client is a Java™ based graphic user interface (GUI). The Tivoli Enterprise Portal GUI is used to view, manage, and change your configuration of WebSphere MQ queue managers across your enterprise.
- **Server:**

  The Tivoli Enterprise Portal client connects to its server, the Tivoli Enterprise Portal Server. The portal server connects to the Tivoli Enterprise Monitoring Server, which acts as a collection and control point for alerts that are received from the monitoring agents, and collects performance and availability data. The hub Tivoli Enterprise Monitoring Server correlates the monitoring data collected by agents and remote servers and passes it to the portal server for presentation and your evaluation. A central processing component that is specific to WebSphere MQ configuration at the hub monitoring server satisfies requests from the portal GUI and manages the database containing the configuration details.
- **Agent:**

  WebSphere MQ Configuration agents that are on the systems with queue managers or remotely connect to those queue managers provide data from the queue managers and make changes to queue managers.

Configuration database

In a highly distributed network, WebSphere MQ can run on several operating systems. No matter where your resources are, WebSphere MQ Configuration agent provides simplification by offering a single repository for all your WebSphere MQ configuration data, called the *configuration database*.

The configuration database is stored at the hub Tivoli Enterprise Monitoring Server and includes a default set of objects to help you start using WebSphere MQ Configuration agent.

Adding Configuration view to your list of Tivoli Enterprise Portal Navigator views

WebSphere MQ Configuration agent uses the Tivoli Enterprise Portal interface and adds the Configuration view and the Configuration Authorities items to the interface.

To get started using the Configuration view, do the following steps:

1. Log on to Tivoli Enterprise Portal, and from the list of available Navigator views, click **Configuration**. Figure 2 on page 5 shows the Configuration selection in the list of available navigator views.

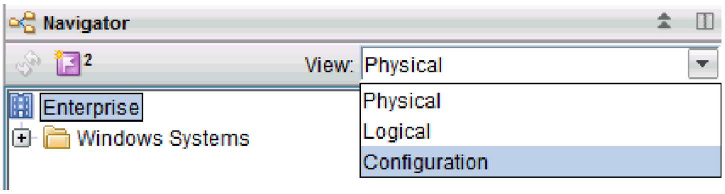


Figure 2. Configuration selection in the list of available navigator views

Tip: The Configuration selection is available in this list after initial installation of WebSphere MQ Configuration agent. If the Configuration selection is not displayed in your list of available Navigator views, your IBM Tivoli Monitoring administrator must assign the view to your user ID.

2. Add the Configuration view to your list of available Navigator views:
   a. Open the **Administer Users** window from the **Edit** menu (or ask your IBM Tivoli Monitoring administrator to open it for you) and select your user ID.
   b. Click the **Navigator Views** tab and add **Configuration** to your list of **Assigned Views**, as shown in Figure 3.

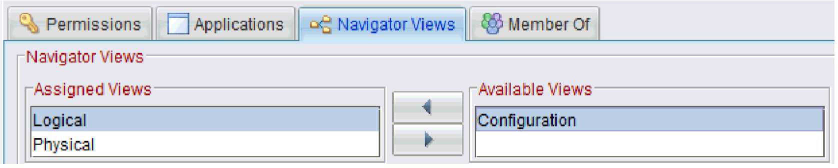
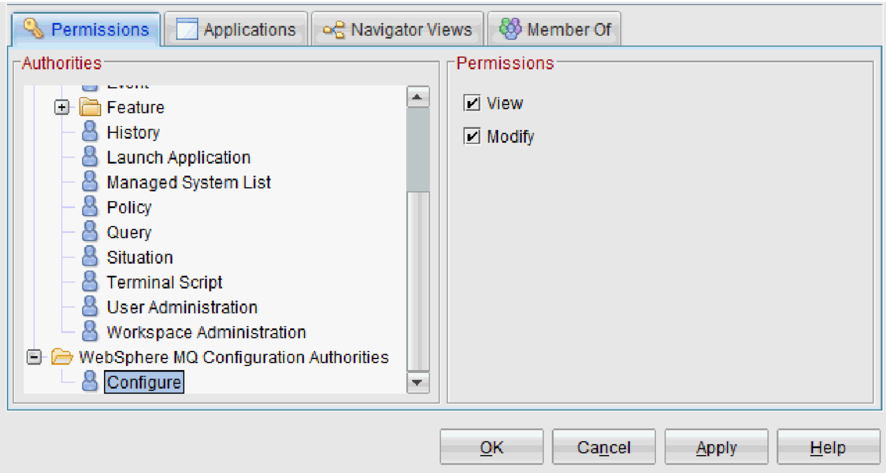


Figure 3. Add Configuration to Assigned Views

Remember: If you move **Configuration** to the top of the list of **Assigned Views**, **Configuration** becomes your default view. If **Configuration** is not listed in the **Administer Users** window on the **Navigator Views** page, either in the list of **Available Views** or in the list of **Assigned Views**, application support for WebSphere MQ Configuration agent is not correctly installed. See the *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide* for more information about how to install application support.

3. Click the **Permissions** tab and scroll down the list of authorities. The **WebSphere MQ Configuration Authorities** item is displayed in the list, as shown in Figure 4 on page 6.



Permissions

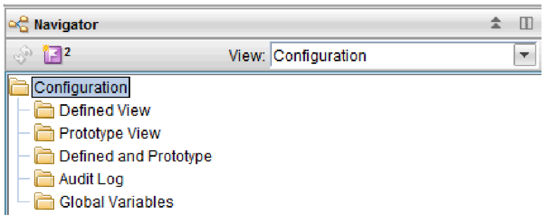
☑ View

☑ Modify

Figure 4. WebSphere MQ Configuration Authorities item

Remember: If **WebSphere MQ Configuration Authorities** is not listed in the **Authorities** list, application support for WebSphere MQ Configuration agent is not correctly installed. See the *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide* for information about how to install application support. Your user ID requires the **Modify** permission (Modify includes View) so that you can change the configuration of your WebSphere MQ or to schedule configuration updates using WebSphere MQ Configuration agent, which might include access from the WebSphere MQ Monitoring agent by means of enhanced integration using OMEGAMON DE.

4. Click **OK** to save your changes.
5. Close and start Tivoli Enterprise Portal again to update the **List of Available Navigator Views** and click the **Configuration** view. The **Configuration** view is displayed as shown in Figure 5



View: Configuration

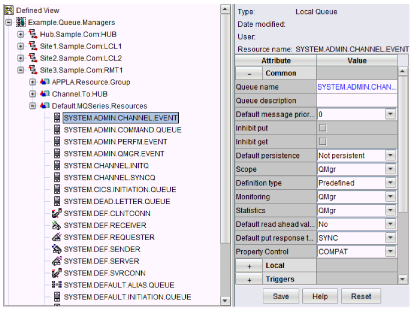
Figure 5. Display of Configuration view

Tip: The **Configuration** view is the usual way to access WebSphere MQ Configuration agent. (You can also access it by means of enhanced integration with WebSphere MQ Monitoring agent using OMEGAMON DE.)

A hierarchical representation of the configuration of your WebSphere MQ environment

To help you understand the structure of the configuration of your WebSphere MQ environment, WebSphere MQ Configuration agent provides a hierarchical representation of your WebSphere MQ configuration called the *Defined View*. Defined objects in this view represent current or potential WebSphere MQ resources, such as queue managers, channels, queues, processes, and namelists, all of which are managed by WebSphere MQ Configuration agent, as shown in

Figure 6.



- Defined View
  - Example.Queue.Managers
    - Hub.Sample.Com:HUB
    - Site1.Sample.Com:LCL1
    - Site2.Sample.Com:LCL2
    - Site3.Sample.Com:RMT1
      - APPLA.Resource.Group
      - Channel.To.HUB
      - Default.MQSeries.Resources
        - SYSTEM.ADMIN.CHANNEL.EVENT
        - SYSTEM.ADMIN.COMMAND.QUEUE
        - SYSTEM.ADMIN.PERFM.EVENT
        - SYSTEM.ADMIN.QMGR.EVENT
        - SYSTEM.CHANNEL.INITQ
        - SYSTEM.CHANNEL.SYNCQ
        - SYSTEM.CICS.INITIATION.QUEUE
        - SYSTEM.DEAD.LETTER.QUEUE
        - SYSTEM.DEF.CLNTCONN
        - SYSTEM.DEF.RECEIVER
        - SYSTEM.DEF.REQUESTER
        - SYSTEM.DEF.SENDER
        - SYSTEM.DEF.SERVER
        - SYSTEM.DEF.SVRCONN
        - SYSTEM.DEFAULT.ALIAS.QUEUE
        - SYSTEM.DEFAULT.INITIATION.QUEUE

Type: Local Queue
Date modified:
User:
Resource name: SYSTEM.ADMIN.CHANNEL.EVENT

Attribute	Value
- Common	
Queue name	SYSTEM.ADMIN.CHAN...
Queue description	
Default message prior...	0
Inhibit put	□
Inhibit get	□
Default persistence	Not persistent
Scope	QMgr
Definition type	Predefined
Monitoring	QMgr
Statistics	QMgr
Default read ahead val...	No
Default put response t...	SYNC
Property Control	COMPAT
+ Local	
+ Triggers	

Figure 6. A hierarchical representation of the configuration of your WebSphere MQ environment

You can use the discovery feature to quickly and easily build defined objects that represent your actual WebSphere MQ configuration.

You can also use the Defined View to safely validate changes to the configuration of your WebSphere MQ environment before applying them to your actual WebSphere MQ configuration.

Common prototype models for creating WebSphere MQ objects

The prototype function can be used to create blueprints for queue managers, resource groups, and resources that you can use as templates for defining configurations. After you create a prototype object, you can drag it from the Prototype View into the Defined View as needed, to build or update the configuration of your WebSphere MQ environment.

Any object that is created from a prototype inherits the characteristics of the prototype unless you specifically override them. If you update a prototype, WebSphere MQ Configuration agent automatically updates all objects that are based on that prototype. Using prototypes makes maintaining your WebSphere MQ configuration much easier, because instead of having to update many defined objects, you can update just the prototype on which they are based.

You can decrease your maintenance costs even further by using variables in your prototypes. WebSphere MQ Configuration agent includes a Global Variables workspace that can be used to quickly and easily change variable values that are inherited by subordinate objects.

Managing resources from a business perspective

Using WebSphere MQ Configuration agent, you can organize WebSphere MQ resources into groups according to their business purpose. A queue manager is called a *configured system*. *Configured system groups* can be used to organize queue managers into groups that you choose. For example, you can group and manage all resources that are related to a particular application, and create a configuration that closely matches the logical structure of your enterprise. At a lower level, *resource groups* make it easy to organize queue manager resources (such as channels, queues, processes, and namelists) by the business purpose that they serve.

Keeping your actual and defined configurations in sync

After you develop and test the Defined View, you can implement your changes in your actual WebSphere MQ configuration. Or you can change your actual configuration manually and update the Defined View accordingly. The update features of WebSphere MQ Configuration agent can be used to keep your actual configuration and defined configuration in sync.

You must reconcile differences between the Defined View and your actual WebSphere MQ configuration before attempting any type of update operation. By using the **View discrepancies** action you can resolve specific differences either in favor of the defined configuration or in favor of the actual configuration. For more information about how to use the **View discrepancies** function, see "Viewing discrepancies" on page 81.

When you click **Update** > **Actual from defined**, WebSphere MQ Configuration agent first validates your Defined View to prevent errors from being implemented in your actual configuration, and then updates your actual configuration to match the defined configuration. For more information about how to use the **Update** > **Actual from defined** function, see "Updating objects in your actual WebSphere MQ configuration" on page 86.

Another way to keep your actual configuration and defined configuration in sync is to click **Update** > **Defined from actual**, which changes the defined configuration to match your actual WebSphere MQ configuration. For more information about how to use the **Update** > **Defined from actual** function, see "Updating the configuration database from your actual WebSphere MQ configuration" on page 83.

Both the **Update** > **Defined from actual** and **Update** > **Actual from defined** actions can delete objects from the configuration that is being updated; you should click **View discrepancies** before you do either update action to ensure that you know that changes that you will implement.

Scheduling actions

You can either do the **Update** > **Actual from defined**, **Update** > **Defined from actual**, or **View discrepancies** actions as you update the configuration of your WebSphere MQ environment, or you can schedule these actions to run at specific intervals. For more information about scheduling actions, see Chapter 8, "Scheduling actions," on page 197.

You have options available for doing long-running tasks. Based on how you set the product options, you can always run the tasks in the foreground, in the background, or be prompted each time. You can do the following actions in the background:

- **Update** > **Actual from defined**
- **Update** > **Defined from actual**
- **View discrepancies**
- **Delete** (defined, actual, or both actual and defined)
- **Validate**
- **Discover new resources**
- **Back up configuration database**

For example, if you have the product option set to prompt each time, when you click **Update** > **Actual from defined**, you are prompted for whether the update should run in the background. If you specify yes, WebSphere MQ Configuration agent creates an internal scheduled action that does the update.

Monitoring network performance with WebSphere MQ Monitoring agent

You can use WebSphere MQ Monitoring agent to collect WebSphere MQ data from all your remote and local queue managers and to analyze it from a single vantage point.

WebSphere MQ Configuration agent and WebSphere MQ Monitoring agent can be used independently of one another. However, when used together, one component enhances the other. Tivoli Enterprise Portal integrates the monitoring functions that are provided by WebSphere MQ Monitoring agent with the configuration functions that are provided by WebSphere MQ Configuration agent. Thus a single WebSphere MQ administrator can address both needs from a single computer.

The monitoring and performance information that is provided by WebSphere MQ Monitoring agent can also help you configure your WebSphere MQ network for maximum efficiency. For example, you can use WebSphere MQ Monitoring agent to determine if there are any bottlenecks in the configuration of your WebSphere MQ environment. Then you can use WebSphere MQ Configuration agent to resolve bottlenecks by moving or adding queues or by reconfiguring queues and channels.

Viewing statistics provided by WebSphere MQ Monitoring agent from WebSphere MQ Configuration agent

When you do a **View actual** request against a queue manager, a local queue, or a channel, WebSphere MQ Configuration agent queries the appropriate WebSphere MQ Monitoring agent to pick up the most current monitoring statistics.

The statistics that are collected are presented in the **Statistics** section of the settings list for the object. The **Statistics** section is included in the settings list only when you perform the **View Actual** request (it is not present for a typical settings list open). If the WebSphere MQ Monitoring agent is not available, you can still perform the **View actual** request without errors. But if the WebSphere MQ Configuration agent is not available, the following message is displayed:

```
KCF0127E The configuration manager was unable to obtain configuration data
from agent RC=0 Reason=0
```

Entering WebSphere MQ commands from the defined view

When you click the **Submit MQ Command** option (for example, right-click a channel in the **Defined View** and click **Action** > **Submit MQ command**), a window is displayed where you can enter a free-form WebSphere MQ operator command. The resulting return code is displayed at the client.

Remember: WebSphere MQ Configuration agent submits WebSphere MQ commands through the WebSphere MQ Monitoring agent. To use the **Submit MQ command** function in WebSphere MQ Configuration agent, make sure that a WebSphere MQ Monitoring agent is running on the same two-system cluster where the WebSphere MQ Configuration agent is installed. And the user ID that is used by WebSphere MQ Monitoring agent to interact with WebSphere MQ must belong to the **mqm** group.

Putting all the pieces together: A typical scenario

This section presents a scenario that might help you understand how the features of WebSphere MQ Configuration agent work together to help you build your WebSphere MQ network. At this point, you do not need to know exactly how each task is performed; subsequent topics describe these tasks in detail. Instead, note how the company in the scenario uses WebSphere MQ Configuration agent to minimize the effort when introducing and maintaining a new application to many sites.

Scenario background

The XYZ company has only recently begun to use WebSphere MQ for application-to-application integration. The company expects their WebSphere MQ network to grow rapidly in size and complexity. As the system administrator, you suggest that they purchase WebSphere MQ Configuration agent to help them manage an increasingly challenging environment.

One of their first uses of WebSphere MQ is to integrate two applications:

- An order-processing application that currently runs on a central z/OS system at company headquarters.
- An order-entry application that runs on AIX® systems located at each of the seven branch offices; the application will be introduced in the seven offices over the next two weeks.

Before you installed WebSphere MQ Configuration agent, you created a queue manager and supporting queues on the central z/OS system for the order-processing application. You also created queue managers on each of the remote AIX systems in anticipation of the order-entry application.

Each AIX queue manager requires four queues. Because each group of four queues supports the same application, the WebSphere MQ administrator expects to configure each group the same way.

After you install WebSphere MQ Configuration agent, you want to use its features to minimize the cost of the following actions:

- Designing and testing your planned configuration of the four queues that support the order-entry application on each AIX system
- Deploying the planned configuration on the seven remote AIX systems
- Maintaining the configuration of the queues over the life of the application

Scenario strategy

After reviewing the goals and the tools that are provided by WebSphere MQ Configuration agent, you work out the following strategy for designing, testing, and deploying the planned configuration.

Because the planned configuration comprises sets of four queues on each of the seven systems, you decide to create prototypes of the four queues. You also decide to create a resource group prototype to hold the four queue prototypes.

This strategy simplifies the work that is required to build the initial configuration, because when you are satisfied with the configuration of the queue prototypes, you can use them as needed, to quickly create queues for the new application. All you do is to drag an instance of the resource group prototype to the queue manager on each system in the defined view.

Using prototypes also minimizes the effort that is required to maintain the queues that support the order-entry application. If changes to the application require additional queues or changes to the existing queues, you can change the prototypes directly instead of manually changing each copy.

After copying the resource group prototype to a queue manager in the defined view, you use WebSphere MQ Configuration agent to test the defined configuration. When you are satisfied with the results, use WebSphere MQ Configuration agent to update the actual WebSphere MQ configuration with a few clicks of your mouse.

Implementing your plan

To implement this strategy, do the following steps:

1. Discover and view your existing configuration of WebSphere MQ.

   You use the discovery feature to upload your existing WebSphere MQ configuration so that you can view a representation of it in the **Defined View** , as shown in Figure 7 (See Chapter 2, “Viewing your current WebSphere MQ configuration,” on page 17 for more information about how to view your current WebSphere MQ configuration). Now that you can see and manipulate the structure of your existing configuration, you can easily make configuration decisions.

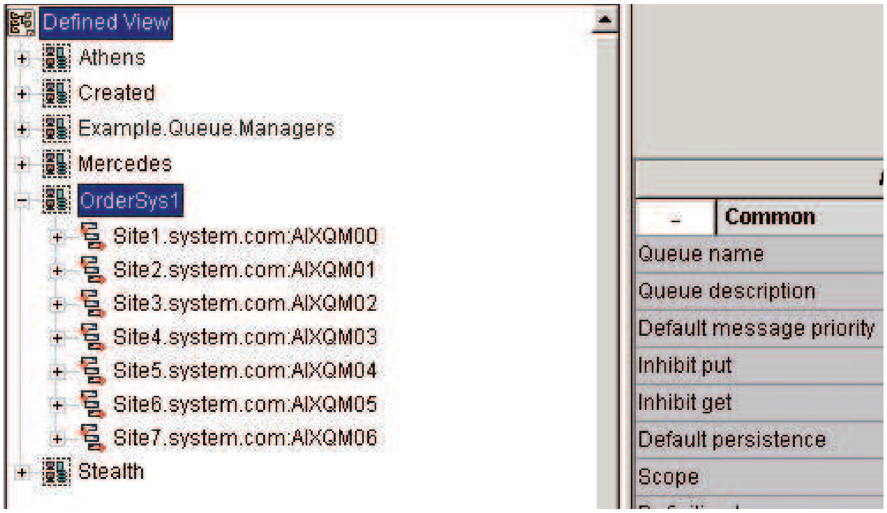


Figure 7. Discover and view the existing configuration of WebSphere MQ

2. Create queue prototypes.

   You create a prototype of each of the four queues that support the order-entry application. These prototypes serve as the models for queue objects that you add later to the defined view. After the queues are added to the seven AIX systems in the defined view, you can change the queues by changing the original four prototypes on which they are based.

   When you create the four queue prototypes, you specify a name for the prototype, ProtoOrderEntryQ*n*, and another name for defined objects that are based on the prototype, OrderEntryQ*n* on System *Y*, where *n* is in the range 1 - 4, and *Y* is the AIX node name. By using similar names for defined objects and for the prototypes on which they are based, you can keep track of related objects. Figure 8 on page 12 shows the Prototype View in which the queue prototypes are created.

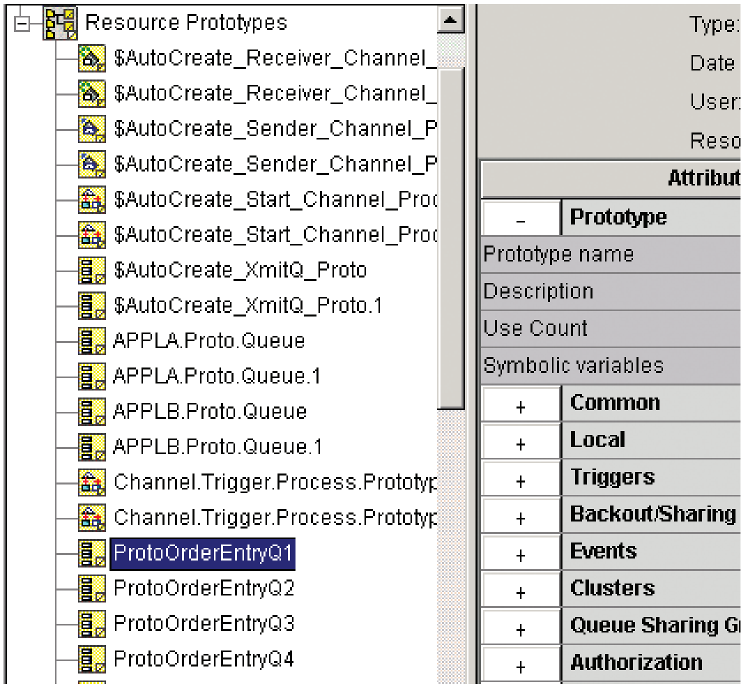


Figure 8. Create queue prototypes

3. Create a resource group prototype.

   You create a resource group prototype to contain the four queues that support the order-entry application. Creating a resource group prototype makes it easy to configure each AIX system for the order-entry application.

   When creating the resource group prototype, you specify a name for the prototype, ProtoOrderEntryGroup, and another name for the defined objects, OrderEntryGroup on system *Y*, which are based on the prototype. Using similar names makes it easier to keep track of related objects.

4. Drag an instance of the queue prototypes into the resource group prototype.

   You can drag an instance of the four queue prototypes into the resource group prototype. Moving the instances creates references to each of the four queue prototypes. These references act as pointers that link the queue prototypes to the resource group prototype. If you make changes to a queue prototype, the change is automatically reflected in the resource group prototype and in each defined object that is based on these prototypes. Figure 9 on page 13 shows the resource group prototype with references to the four queue prototypes

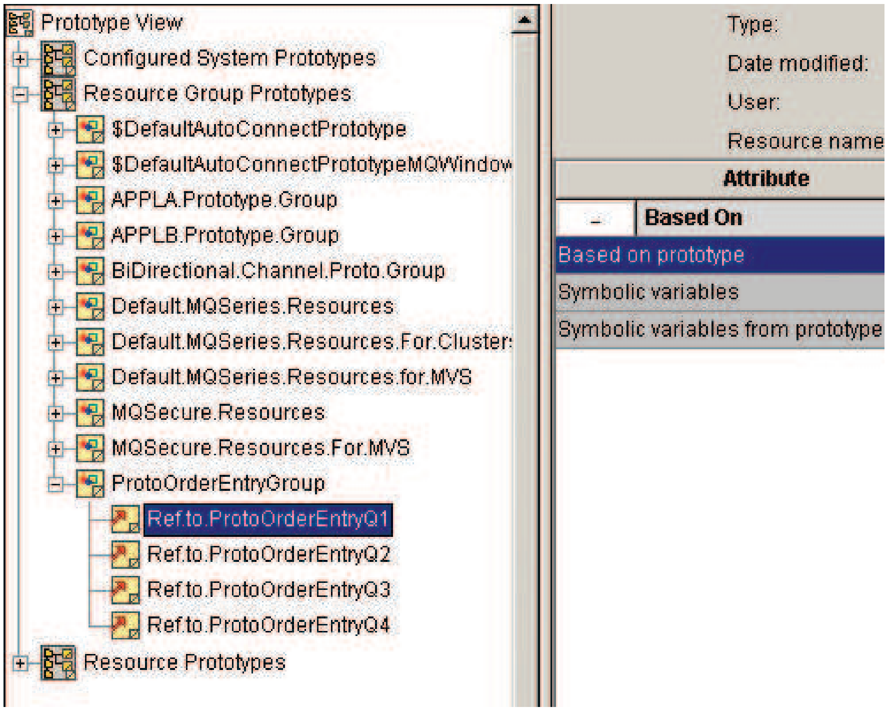

Prototype View
Configured System Prototypes
Resource Group Prototypes
$DefaultAutoConnectPrototype
$DefaultAutoConnectPrototypeMQWindow
APPLA.Prototype.Group
APPLB.Prototype.Group
BiDirectional.Channel.Proto.Group
Default.MQSeries.Resources
Default.MQSeries.Resources.For.Cluster:
Default.MQSeries.Resources.for.MVS
MQSecure.Resources
MQSecure.Resources.For.MVS
ProtoOrderEntryGroup
Ref.to.ProtoOrderEntryQ1
Ref.to.ProtoOrderEntryQ2
Ref.to.ProtoOrderEntryQ3
Ref.to.ProtoOrderEntryQ4
Resource Prototypes
Type:
Date modified:
User:
Resource name
Attribute
Based On
Based on prototype
Symbolic variables
Symbolic variables from prototype

Figure 9. Drag an instance of the queue prototypes into the resource group prototype

5. Drag an instance of the resource group prototype to the defined view tree.

   In the **Configuration** view click **Defined and Prototype** and drag the resource group prototype to the queue manager in the defined view. Dragging an instance of a prototype to the defined view does not affect your actual WebSphere MQ configuration.

   Dragging the resource group prototype to the defined view creates a defined resource group called OrderEntryGroup on System *Y*. The defined resource group contains the four queues that are referenced in the resource group prototype on which it is based. As defined in their prototypes, all the queues on System *Y* are named OrderEntryQ*n*. Figure 10 on page 14 shows the queue manager with the resource group and four queues.

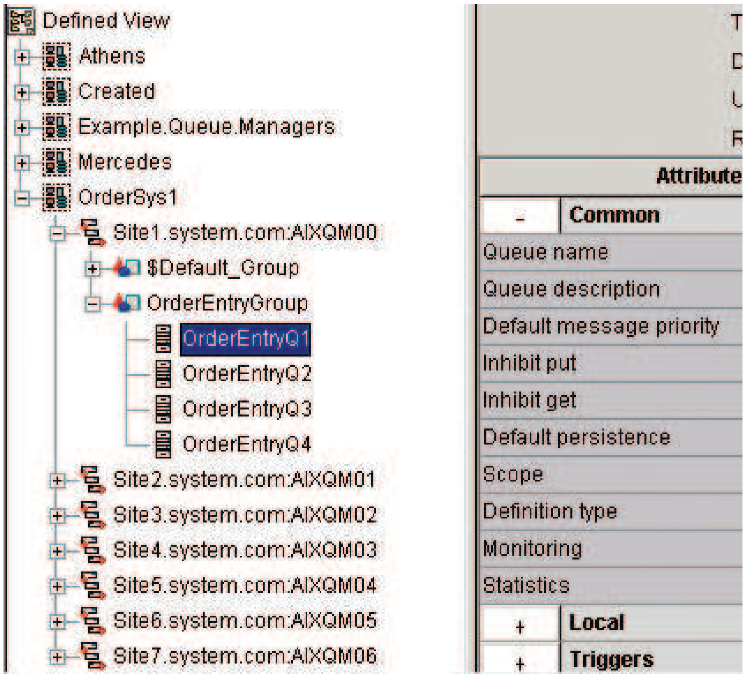


Figure 10. Drag an instance of the resource group prototype to the defined view tree

6. Validate the queue manager definition.

   To ensure that there are no errors in the queue manager definition or in any of its new underlying resource definitions, use WebSphere MQ Configuration agent to validate the queue manager with the new resource group.

   If you find any errors in the four new queues, edit the queue prototypes on which they are based, not the queues in the defined view, then validate the queue manager again.

7. Update the WebSphere MQ configuration.

   After you validate the queue manager definition, use WebSphere MQ Configuration agent to automatically update the actual WebSphere MQ configuration. Instead of implementing the changes by using multiple commands, right-click the queue manager that you want to update and click **Update** > **Actual from defined**.

8. Repeat the process as needed for each of the remaining six AIX systems as the order-entry application is implemented throughout your environment.

Maintaining your system

One year later, an upgrade to the order-entry application requires the addition of a fifth queue to each of the seven AIX systems. Because you used prototypes to build the original four queues for the application, it is easy and fast to add another queue.

1. Create a fifth queue prototype in the same way that you created each of the original four queue prototypes.

   You use the same naming convention: ProtoOrderEntryQ5 for the prototype name and OrderEntryQ5 on System *Y* for the name of defined objects that are based on the prototype.

2. Add ProtoOrderEntry5 to the resource group prototype ProtoOrderEntryGroup.

   WebSphere MQ Configuration agent adds a reference to the fifth queue prototype to the resource group prototype. Now that the resource group prototype has been changed, a fifth defined queue is automatically added to all the defined resource groups that are based on the prototype ProtoOrderEntryGroup.

3. Run the **Update** > **Actual from defined** operation on the entire configured system group to add a fifth queue to the seven AIX systems.

   WebSphere MQ Configuration agent checks for validation errors that might be introduced with the fifth queue. If no errors are found, WebSphere MQ Configuration agent adds the fifth queue to the actual WebSphere MQ configurations on the seven AIX systems.

Chapter 2. Viewing your current WebSphere MQ configuration

This section explains how to use WebSphere MQ Configuration agent to view your existing WebSphere MQ configuration.

You can use the Defined View to create a hierarchical representation of your WebSphere MQ configuration. The Defined View provides functions that help you manage your actual WebSphere MQ queue managers and resources. For more information about the Defined View and how to create a hierarchical representation of your WebSphere MQ configuration, see “Defined View” and “Creating a hierarchical representation of your WebSphere MQ configuration in the Defined View” on page 18.

WebSphere MQ Configuration agent uses configured system groups to organize the WebSphere MQ resources. You can organize queue managers into groups of your own choosing. For information about configured system group and how to create configured system groups, see “Configured system group” on page 19 and “Creating a configured system group” on page 19.

Defined View

After you use the discovery function to populate a configured system group, you can see your existing WebSphere MQ configuration in the Defined View. The configuration of your WebSphere MQ environment is displayed in a tree view. In this view, different icons represent each type of object in your WebSphere MQ configuration: queue managers, queues, channels, processes, namelists, and other objects.

The left side of the display shows a hierarchical representation of configured system groups, configured systems (queue managers), resource groups, and resources. Click the plus sign (+) or the minus sign (-) to expand or collapse the display.

The right side of the display shows the settings list of the currently selected object.

When you populate a configured system group in the Defined View using the discovery feature, resources that are associated with each active queue manager are put into the $Default_Group resource group. For detailed description about the $Default_Group resource group, see “$Default_Group resource group” on page 28.

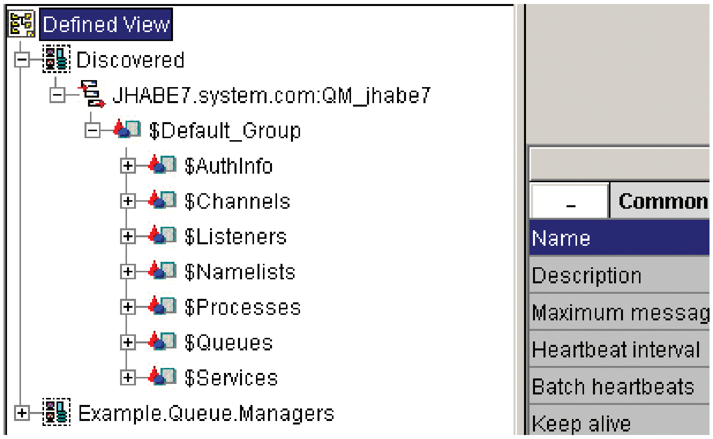


Figure 11. Configuration of WebSphere MQ in the Defined View

Creating a hierarchical representation of your WebSphere MQ configuration in the Defined View

Use the Defined View to create a hierarchical representation of your WebSphere MQ configuration. The defined view provides features that help you manage your actual WebSphere MQ queue managers and resources.

You can initially build this representation using one of the following methods:

- Using your existing WebSphere MQ configuration as the basis for your representation in the Defined View.
- Creating your representation in the Defined View directly. See Chapter 4, “Creating and defining objects in the defined view,” on page 51.

Creating a representation that is based on your existing WebSphere MQ configuration in the Defined View comprises the following tasks:

1. Enter update mode so that you can make changes to the configuration database as described in “Entering update mode.”
2. Create a new configured system group, as described in “Creating a configured system group” on page 19.
3. Use the discovery feature to populate the configuration database with resources in your actual WebSphere MQ environment, as described in “Discovering your WebSphere MQ configuration” on page 20.
4. Review the hierarchical representation of your WebSphere MQ configuration.

Entering update mode

Do the following steps to enter the update mode:

Important: To enter update mode, your user ID must have Modify WebSphere MQ Configuration agent permission, and the Navigator Configuration view as an Assigned View as described in “Adding Configuration view to your list of Tivoli Enterprise Portal Navigator views” on page 4. See *IBM Tivoli Monitoring Administrator's Guide* for detailed information about user administration.

1. Ensure that in the **List of available Navigator Views** in the Tivoli Enterprise Portal, the **Configuration** view is selected.

2. In the configuration navigator tree, click **Configuration** (the root-level item). The **Update mode** check box is displayed in the Configuration workspace.
3. Select the **Update mode** check box.

Now you are in update mode and can make changes to the configuration database. When you are in update mode, you can do the following things:

- Change your Defined View; use the configuration database to update your actual configuration (as described in Chapter 6, "Maintaining the configuration of your WebSphere MQ environment," on page 81); use your actual configuration to populate the configuration database (as described in "Discovering your WebSphere MQ configuration" on page 20).
- Change your Prototype View. See Chapter 3, "Designing and planning with prototypes," on page 31.
- Use the Global Variables workspace to create, delete, and change the values that are assigned to the global variables of your site. See "Variables and prototypes" on page 37.
- Back up and restore the configuration database. See Chapter 11, "Backing up and restoring the configuration database," on page 223

Configured system group

A *configured system group* is a unit of organization within WebSphere MQ Configuration agent. A *configured system* is a queue manager. By using a configured system group, you can organize queue managers into groups of your own choosing. A configured system group has no corresponding component in an actual WebSphere MQ configuration; it is simply a collection of queue managers, which in turn contain resource groups. Resource groups contain individual resources, such as queues, channels, and other WebSphere MQ objects (see "Resource group" on page 65). Configured system groups are the highest unit of organization within WebSphere MQ Configuration agent.

You can create any number of configured system groups and organize them in any way that is meaningful for your site.

Creating a configured system group

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

To create a new configured system group:

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Click **Defined View** in the configuration view to open the defined view.
3. In the Defined View on the left side of the workspace, right-click **Defined View** (the root-level item) and click **Create Configured System Group**, as shown in Figure 12 on page 20.

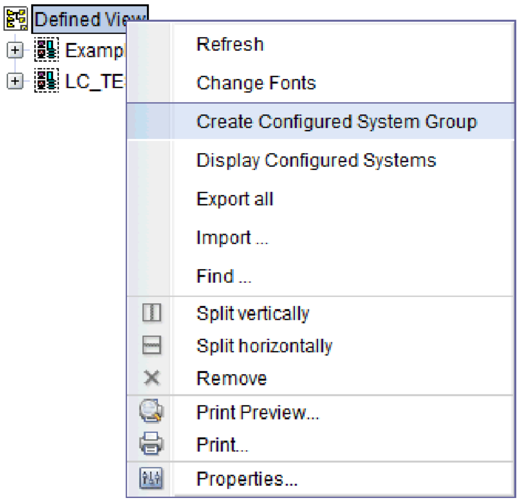


Figure 12. Create Configured System Group

4. When prompted to enter a name, enter an alphanumeric name for the new configured system group and click **OK**.

   The new configured system group is added to the defined view tree.

   Remember:

   a. Do not use non-English characters for the new object name.
   b. SYSTEM should not be used as the prefix name that you assign to your own resource. WebSphere MQ Configuration agent identifies the resource with a prefix name of SYSTEM as the IBM provided default resource and therefore skips the validation process.
   c. On z/OS systems with CCSID 1390, no WebSphere MQ objects support lowercase characters.
5. In the defined view tree, click the new configured system group.
6. In the settings list on the right side of the Defined View, complete the settings list as necessary.
7. Click **Help** to display information about each parameter.
8. Click **Save** to save your changes.

Discovering your WebSphere MQ configuration

The discovery process populates the configuration database with data from existing queue managers in your WebSphere MQ network. When you run the discovery process, your entireWebSphere MQ network is searched for queue managers that are not already defined in the configuration database, and they are then added to the selected configured system group. This function is only available at the configured system group level.

Tip: The terms, *discover* and *discovery*, describe the default Discover process of WebSphere MQ Configuration agent unless specifically noted.

Discovery function considerations

- The discovery process detects only previously undiscovered queue managers on systems that are running a WebSphere MQ Configuration agent (hereafter referred to as the *configuration agent*) that is connected to the Tivoli Enterprise

Monitoring Server. If the configuration agent discovers a queue manager that is already defined in the configuration database, that queue manager is ignored.

- All z/OS queue managers must be defined as z/OS subsystems.
- On systems other than z/OS systems, the configuration agent scans for all queue managers that are defined using the WebSphere MQ control command.
- For the configuration agent to detect resource information, a queue manager must be active when the discovery process takes place. Inactive queue managers are displayed in the defined view as a single node with no resource groups. In this case, you can use one of the following options to add resource information about the queue managers:
  - Start the queue manager and use the **Update** function to update the queue manager in the Defined View from the actual queue manager. See “Updating the configuration database from your actual WebSphere MQ configuration” on page 83.
  - Open the queue manager settings list in the defined view, expand the **Auto Start** section, and select the **Auto start** check box. Then use the **Update** function to update the queue manager in the Defined View from the actual queue manager; see “Updating the configuration database from your actual WebSphere MQ configuration” on page 83.
- WebSphere MQ Configuration agent can automatically perform a discovery if you select the **Auto Discover** option in the Product Options section of the Configuration workspace. By default, the **Auto Discover** option is disabled.
- Depending on the size and complexity of your existing WebSphere MQ configuration, the discovery process might take a long time to complete, and after the process begins, it cannot be interrupted. If you have a large number of queue managers, you can select the **Discover Lite** option in the Product Options section of the Configuration workspace. By default, the **Discover Lite** option is disabled. The **Discover Lite** option discovers *the names only* of queue managers in your WebSphere MQ environment and uses them to define placeholder queue managers in the Defined View. This option is intended as a quick way to populate the Defined View with the names of queue managers in your WebSphere MQ environment. To completely define these placeholder queue managers, you can use the **Update** function on each one to update the queue manager in the Defined View from the actual queue manager. see “Updating the configuration database from your actual WebSphere MQ configuration” on page 83. You can also use the **Discover new resources** function on each one to add resources to the queue managers in the Defined View. Alternatively, you can complete the definitions of placeholder queue managers by using the **Scheduled Action** function to automatically run the **Update** > **Defined from actual** operation or the **Discover new resources** operation at a convenient time.

Discovering queue managers and their resources

If the queue manager that you want to discover is a multi-instance queue manager, ensure that the AMQ_MQS_INI_LOCATION parameter in the `mc.ini` file is set to the full path of the `mqs.ini` file that the multi-instance queue manager uses. For example, `AMQ_MQS_INI_LOCATION=/user1/mqs.ini`. The `mc.ini` file is located in the *`ITM_HOME`*`/config` directory, where *ITM_HOME* is the directory where IBM Tivoli Monitoring is installed.

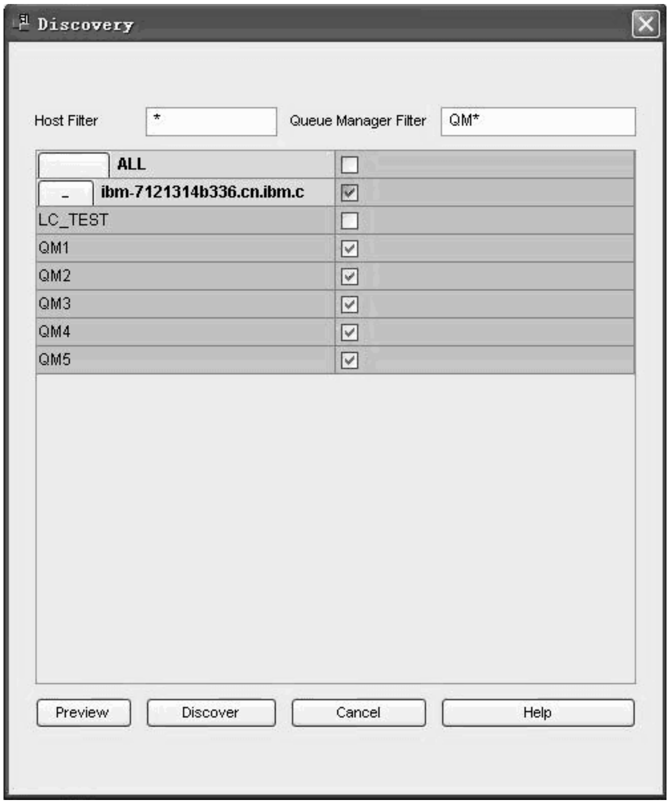
To search your WebSphere MQ environment for queue managers and to add them to the current configured system group, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined View.
3. In the Defined View, right-click the configured system group to which you want to add the discovered queue managers and click **Discover** from the menu.

   A list of undiscovered queue managers, grouped by host name, is displayed in the Discovery Selection window.
4. In the Discovery Selection window, select the queue managers that you want to discover and add to the configured system group.

   You can use the **Host Filter** and **Queue Manager Filter** fields to select a particular subset of queue managers that you are interested in. To do this, enter your filter criteria and click **Preview**, as shown in Figure 13.



Host Filter: *

Queue Manager Filter: QM*

ALL	□
- ibm-7121314b336.cn.ibm.c	☑
LC_TEST	□
QM1	☑
QM2	☑
QM3	☑
QM4	☑
QM5	☑

Figure 13. A filter has been applied to select all hosts and all queue managers with names beginning with QM.

   Remember: If the name of a host exceeds 24 characters in length, only the first 24 characters of its name are displayed.
5. Click **Discover** to begin the discovery process.

   Your WebSphere MQ environment is searched for unknown queue managers, which, with their associated resources (queues, channels, and other objects) are added to the configured system group that you selected. For each queue manager that is discovered, by default a $Default_Group resource group is created, and the resources of the queue manager are added to it. After the discovery process is completed, a report is displayed.

Discovering new resources for queue managers

To discover new resources that are added to a queue manager after it is discovered and added to a configured system group, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined View.
3. In the Defined View, right-click the queue manager in the configured system group and click **Discover new resources** menu item.

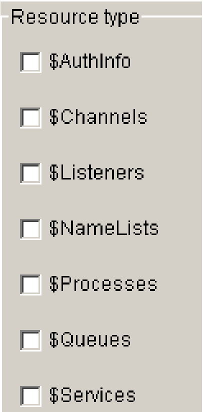
Remember: This process only discovers the new resources that are added to a queue manager. To update the queue manager level attributes, you must perform an Update operation to update the queue manager in the defined view from the queue manager in the actual WebSphere MQ environment; see "Updating the configuration database from your actual WebSphere MQ configuration" on page 83.

Creating separate resource groups for discovered resources

By default, resources of the same type are added to one resource group. For example, queues on a queue manager are added to the resource group named $Queues and channels are added to the resource group named $Channels. If the queue manager that you want to discover has a large number of resources that are associated with it, you can use options in the **Dynamically created resource groups** area in the Configuration workspace to create separate resource groups for holding the discovered resources. Do the following steps:

1. Ensure that you are in update mode. For information about how to enter update mode, see "Entering update mode" on page 18.
2. Select the resource types for which you want to create separate resource groups from the resource types listed in the **Resource Type** section.

   The options are shown in Figure 14.



Resource type

□ $AuthInfo

□ $Channels

□ $Listeners

□ $NameLists

□ $Processes

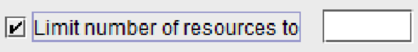
□ $Queues

□ $Services

Figure 14. Resource type options

3. Optional: To set a limit to the number of resources that are contained in each resource group, select the **Limit number of resources to** check box, and specify the value. The default value is 200. To achieve better performance, set this

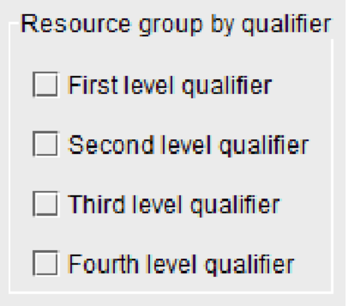
value to a number between 50 and 300.



☑ Limit number of resources to

4. Optional: Select the level qualifiers by which you want to group discovered resources.

   The options are shown in Figure 15. For example, if the name of a queue is APP1.local.system.queue, the first level qualifier is *APP1*, the second level qualifier is *local*, the third level qualifier is *system* and the fourth level qualifier is *queue*.



Resource group by qualifier

□ First level qualifier

□ Second level qualifier

□ Third level qualifier

□ Fourth level qualifier

Figure 15. Four level qualifiers

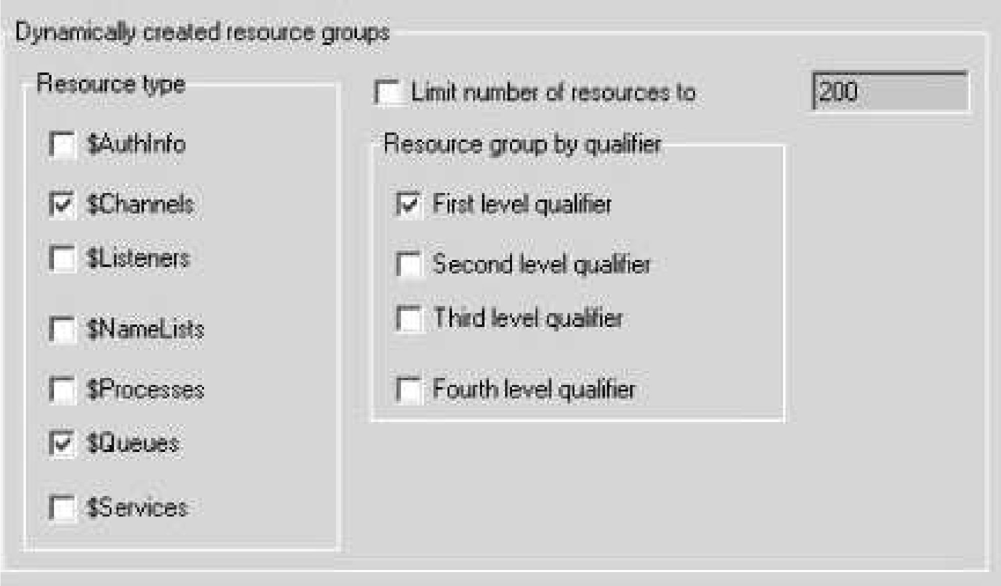
5. Click **Save** to save your changes.
6. Run the discovery process.
   - If you want to run the discovery process to discover new queue managers, see "Discovering queue managers and their resources" on page 21.
   - If you want to run the discovery process to discover new resources of a queue manager, see "Discovering new resources for queue managers" on page 23.

After the discovery process is completed, discovered resources are added to separate resource groups.

For detailed description about the grouping options that are provided in the **Dynamically created resource groups** area, see "Automatic grouping of discovered resources."

Automatic grouping of discovered resources

The **Dynamically created resource groups** area in the Product Options area of the Configuration workspace provides the options for controlling how discovered resources are grouped. Figure 16 on page 25 shows the options for controlling how discovered resources are grouped.



Dynamically created resource groups

Resource type

☐ $AuthInfo

☑ $Channels

☐ $Listeners

☐ $NameLists

☐ $Processes

☑ $Queues

☐ $Services

☐ Limit number of resources to 200

Resource group by qualifier

☑ First level qualifier

☐ Second level qualifier

☐ Third level qualifier

☐ Fourth level qualifier

Figure 16. Controlling how discovered resources are automatically grouped

With the dynamically created resource groups function, you can control the number of resources that are automatically put into a resource group and the number of resource groups for each resource type that you select, you can also refine the classification of discovered resources by selecting different prefix level of the resource name.

The **Resource type** area includes the following resource types:

- AuthInfo
- Channels
- Listeners
- NameLists
- Processes
- Queues
- Services

The **Limit number of resources to** and **Resource group by qualifier** functions are only available after you select one or more of the resource types.

Select the **Limit number of resources to** check box to indicate that the number of resources that are placed into a resource group during discovery and the number of resource groups for each resource type that you select in the **Resource Type** area should be limited to the number that you specify. Use the entry field to indicate the maximum size (it is set to 200 in Figure 16). If the number of resources or resource groups exceeds the number that you specify, a new resource group is created and a numeric suffix (starting with 0001) is added to the resource group name to make it unique.

By default, WebSphere MQ Configuration agent limits the number of resources that are placed into a resource group to 200. To achieve better performance, set this value to a number between 50 and 300. The number that you specify in the entry field also affects the number of resource groups that are contained in the $Default_Group resource group. If the number of discovered resource groups exceeds the number that you specify, a new default group is created.

The **Resource group by qualifier** area provides four prefix levels of the resource name for classifying discovered resources to create distinct resource groups.

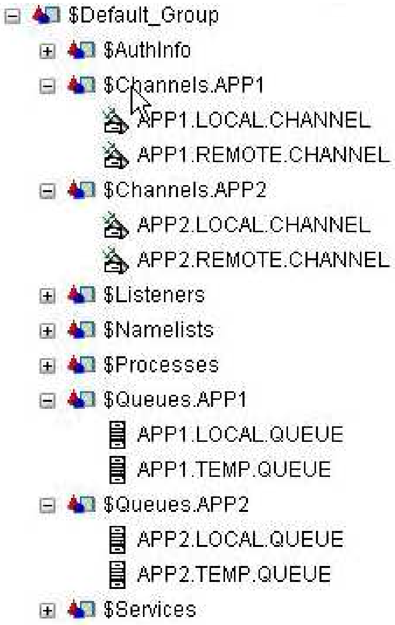
If you select the **First level qualifier** check box, the discovered resources that are of the same resource type and have the same first level qualifier are added to the same resource group, which is named using the selected resource type name and the first level qualifier name separated by a period. If you select the **Second level qualifier**, **Third level qualifier** or **Fourth level qualifier** check box, the discovered resources are added to separate resource groups in a similar way as when the **First level qualifier** is selected.

You can also select multiple level qualifier check boxes. For example, if you select both the **First level qualifier** and **Second Level qualifier** check boxes, the discovered resources that are of the same resource type and have the same first and second level qualifiers are added to the same resource group, which is named using the selected resource type, the first and the second level qualifier names separated by periods.

In the following example, it is assumed that you have the following four queues and four channels on the queue manager that you want to discover, and the **$Queues** and **$Channels** resource types are selected in the **Resource Type** area:

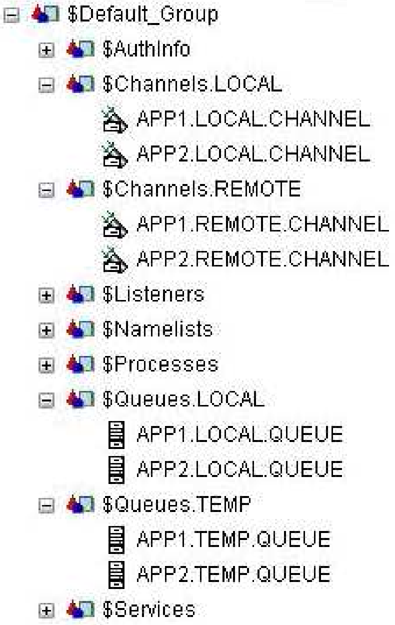
- APP1.LOCAL.QUEUE
- APP2.LOCAL.QUEUE
- APP1.TEMP.QUEUE
- APP2.TEMP.QUEUE
- APP1.LOCAL.CHANNEL
- APP2.LOCAL.CHANNEL
- APP1.REMOTE.CHANNEL
- APP2.REMOTE.CHANNEL

If you select **$Queues** and **$Channels** in the **Resource Type** section and the **First level qualifier** check box in the **Resource group by qualifier** section, two resource groups named $Queues.APP1 and $Queues.APP2 are created for the four queues in the previous list and another two resource groups named $Channels.APP1 and $Channels.APP2 are created for the four channels in the previous list during the discovery process, which are shown in the figure below:



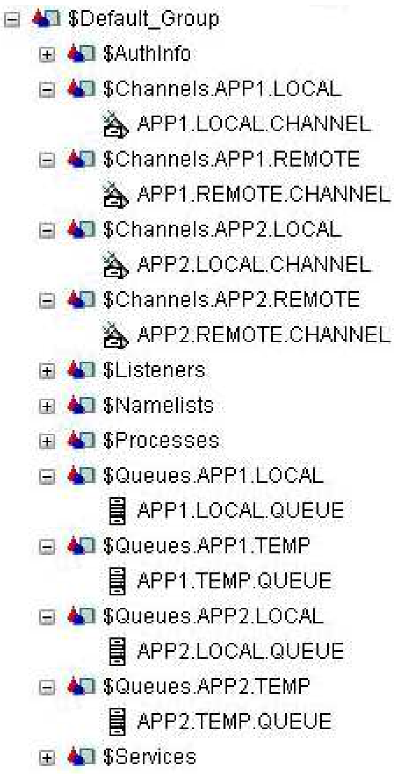
```
$Default_Group
    $AuthInfo
    $Channels.APP1
        APP1.LOCAL.CHANNEL
        APP1.REMOTE.CHANNEL
    $Channels.APP2
        APP2.LOCAL.CHANNEL
        APP2.REMOTE.CHANNEL
    $Listeners
    $Namelists
    $Processes
    $Queues.APP1
        APP1.LOCAL.QUEUE
        APP1.TEMP.QUEUE
    $Queues.APP2
        APP2.LOCAL.QUEUE
        APP2.TEMP.QUEUE
    $Services
```

If you select **$Queues** and **$Channels** in the **Resource Type** section and the **Second level qualifier** check box in the **Resource group by qualifier** section, two resource groups named $Queues.LOCAL and $Queues.TEMP are created for the four queues in the previous list and another two resource groups named $Channels.LOCAL and $Channels.REMOTE are created for the four channels in the previous list during the discovery process, which are shown in the figure below:



```
$Default_Group
    $AuthInfo
    $Channels.LOCAL
        APP1.LOCAL.CHANNEL
        APP2.LOCAL.CHANNEL
    $Channels.REMOTE
        APP1.REMOTE.CHANNEL
        APP2.REMOTE.CHANNEL
    $Listeners
    $Namelists
    $Processes
    $Queues.LOCAL
        APP1.LOCAL.QUEUE
        APP2.LOCAL.QUEUE
    $Queues.TEMP
        APP1.TEMP.QUEUE
        APP2.TEMP.QUEUE
    $Services
```

If you select **$Queues** and **$Channels** in the **Resource Type** section, and **First level qualifier** and **Second Level qualifier** in the **Resource group by qualifier** section, four resource groups named $Queues.APP1.LOCAL, $Queues.APP2.LOCAL, $Queues.APP1.TEMP and $Queues.APP2.TEMP are created for the four queues in the previous list and another four resource groups named $Channels.APP1.LOCAL, $Channels.APP2.LOCAL, $Channels.APP1.REMOTE and $Channels.APP2.REMOTE are created for the four channels in the previous list during the discovery process, which are shown in the figure below:



```
$Default_Group
  $AuthInfo
  $Channels.APP1.LOCAL
    APP1.LOCAL.CHANNEL
  $Channels.APP1.REMOTE
    APP1.REMOTE.CHANNEL
  $Channels.APP2.LOCAL
    APP2.LOCAL.CHANNEL
  $Channels.APP2.REMOTE
    APP2.REMOTE.CHANNEL
  $Listeners
  $Namelists
  $Processes
  $Queues.APP1.LOCAL
    APP1.LOCAL.QUEUE
  $Queues.APP1.TEMP
    APP1.TEMP.QUEUE
  $Queues.APP2.LOCAL
    APP2.LOCAL.QUEUE
  $Queues.APP2.TEMP
    APP2.TEMP.QUEUE
  $Services
```

$Default_Group resource group

When you use the discovery function to populate a configured system group in the Defined View, resources that are associated with each active queue manager are put into a $Default_Group resource group. Each active queue manager that you discover has its own $Default_Group resource group. After the discovery process is complete, you can use this pool of definitions to populate resource groups that you create.

The discovery process (or alternatively, the Auto Discover product option or the Discover New Resources option for Configured Systems) separates the $Default_Group resources into sub-resource group types. This process reduces potential performance issues because you have smaller resource groups, which require less client processing time.

In each $Default_Group resource group, the resources are separated into the following subgroups:

- *$AuthInfo* contains all WebSphere MQ authentication information objects.
- *$Channels* contains all channels.
- *$Listeners* contains all channel listeners.
- *$Namelists* contains all namelists.
- *$Processes* contains all processes.
- *$Queues* contains all queues.
- *$StorageClasses* contains all storage classes.
- *$Service* contains all services.

For dynamic resources (permanent dynamic queues), the $DynamicResources resource group also contains sub-groups for each resource type. However, only the

$Queues resource group exists, because queues are the only type of dynamic resource that is supported. Permanent dynamic queue definitions are not created in the configuration database, unless you enabled the **Configure permanent dynamic queues** option in the **Auto Start** section of the queue manager settings list.

Chapter 3. Designing and planning with prototypes

You can use prototypes to design and plan your WebSphere MQ configuration. Sample prototype objects are provided. You can use these samples to build objects that might later become part of your WebSphere MQ configuration. Any object that is created from a prototype inherits the characteristics of the prototype, unless you specifically override them. If you update a prototype, all objects that are based on that prototype are automatically updated, regardless of their locations.

Using prototypes is useful if you have a distributed network and you want to place identical objects in different locations while ensuring that they always remain in sync. For example, you might need to create several identical queue managers. After you define the queue manager prototype, you can use it to create as many queue managers in the Defined View as you need and to deploy them to different locations. If you decide to change the queue manager configuration in all locations, simply change the original queue manager prototype.

Creating prototypes: two methods

You can work entirely within the Prototype View to create a new prototype, or you can use a defined object from the Defined View to create a prototype.

- Before you add objects to your WebSphere MQ configuration, you might want to design and create your own prototypes in the Prototype View. The advantage to creating your own prototypes is that you can design the prototypes to your exact specifications and use them to create objects that are later deployed to your WebSphere MQ configuration.
- You can also use an object that you uploaded from your WebSphere MQ configuration or that you created in the Defined View, and copy it to the Prototype View to create a prototype. The advantage to this method is that your current WebSphere MQ objects are already configured to your specifications, so you can easily create other objects that are based on them.

Prototype View

The Prototype View, where you work with prototypes, is divided into the following organizational levels:

- Configured System Prototypes, which represent queue managers
- Resource Group Prototypes, which you can use to gather resources into logical groups
- Resource Prototypes, which represent channels, queues, processes, namelists, storage classes, and other objects

Figure 17 on page 32 shows the Prototype View.

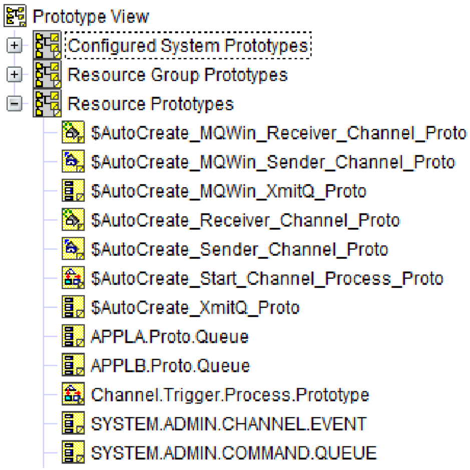

Prototype View
Configured System Prototypes
Resource Group Prototypes
Resource Prototypes
$AutoCreate_MQWin_Receiver_Channel_Proto
$AutoCreate_MQWin_Sender_Channel_Proto
$AutoCreate_MQWin_XmitQ_Proto
$AutoCreate_Receiver_Channel_Proto
$AutoCreate_Sender_Channel_Proto
$AutoCreate_Start_Channel_Process_Proto
$AutoCreate_XmitQ_Proto
APPLA.Proto.Queue
APPLB.Proto.Queue
Channel.Trigger.Process.Prototype
SYSTEM.ADMIN.CHANNEL.EVENT
SYSTEM.ADMIN.COMMAND.QUEUE

Figure 17. The Prototype View

Sample prototypes

In the Prototype View, WebSphere MQ Configuration agent provides the following types of sample prototypes that you can use to design and create all or part of your WebSphere MQ configuration. Sample prototypes include standard defined resources that are created automatically by WebSphere MQ.

- Configured system prototypes

  Use a configured system prototype sample to create queue manager prototypes. Queue manager prototypes consist of a set of queue manager properties and zero or more references to resource group prototypes.
- Resource Group prototypes

  Use a resource group prototype sample to create resource group prototypes that refer to one or more resource prototypes. When you reference a resource prototype within a resource group, a reference object is displayed. References are pointers to the original prototype.
- Resource prototypes

  Use a resource prototype sample to create individual resource prototypes. Resource prototypes correspond to the WebSphere MQ resource types. For example, a local queue prototype and a sender channel prototype are provided.

When you drag a prototype directly to a higher-level prototype, the prototype copy semantics setting (in the Configuration view) determines whether the resource is copied directly to the higher-level prototype, or whether a reference object is created that points back to the prototype that you drag. The default setting is to create a copy. However, if the prototype copy semantics setting is **Create reference**, a prototype reference object is created.

Creating prototypes in the Prototype View

You can create prototypes as models on which to base future objects. If you want to change the parameters of an object, change the prototype on which the object is based, and all objects that are based on that prototype are updated automatically.

When you drag a prototype to the Defined View, you actually create an object that is based on the prototype.

Do the following steps to create a new prototype in the Prototype View:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Prototype View.
3. In the Prototype View, use one of the following options:
   - To create a queue manager prototype, right-click **Configured System Prototypes** and then click **Create** > **Queue Manager**.
   - To create a resource group prototype, right-click **Resource Group Prototypes** and click **Create Resource Group**.
   - To create a resource prototype, right-click **Resource Prototypes**, click **Create** and then click the type of prototype object that you want to create.

   You are prompted to supply a name for the new prototype.
4. Enter an alphanumeric name for the new object and click **OK**.

   Important:

   a. Do not input non-English characters for the new object name.
   b. SYSTEM should not be used as the prefix name that you assign to your own resource. WebSphere MQ Configuration agent identifies the resource whose prefix name is SYSTEM as the IBM provided default resource and therefore skips the validation process.
   c. For prototype queue managers and resource groups, if the name that you assign to this prototype object already exists in the configuration database, WebSphere MQ Configuration agent appends the number 1 to the prototype object. If you create another prototype object with the same name again, WebSphere MQ Configuration agent increments this number by one.
   d. On a z/OS system with CCSID 1390, no WebSphere MQ objects support lowercase characters.

   The new prototype object is added to the prototype view tree.
5. In the prototype view tree, click the new prototype. The settings list for the object is displayed on the right side of the Prototype View.
6. Complete the settings list as necessary. Click **Help** to display information about each parameter.

   Important: Although some values are displayed as default settings in enumeration fields, you must manually select the value and then click **Save** . For example, although TCP is displayed as the default value of the **Network protocol** field, you must select it and click **Save** if you want to set TCP as your network protocol.
7. If you are creating a new queue manager prototype, add the Default.MQSeries.Resources resource group to the new queue manager prototype as follows:
   a. In the Prototype View, expand **Resource Group Prototypes**.
   b. Locate the resource group named **Default.MQSeries.Resources**.
   c. Drag the **Default.MQSeries.Resources** icon to the appropriate queue manager icon in the prototype view tree.

An instance of the default resource group is added to the new queue manager prototype.

8. Click **Save** to save your changes.

Creating prototypes from defined objects

You can create a prototype by dragging a defined object from the Defined View to the Prototype View.

To create prototypes from defined objects, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined and Prototype View by clicking **Defined and Prototype** in the Configuration view.

   The defined view tree and prototype view tree are positioned and sized so that you can easily drag objects between them, as shown in Figure 18.

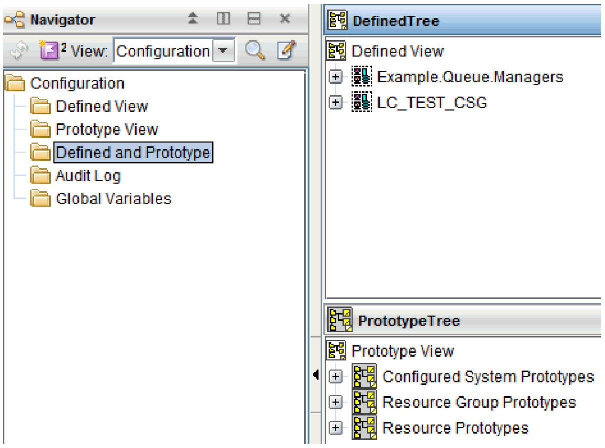


Figure 18. Defined and Prototype view

3. In the defined view tree, click the object that you want to use to create a prototype.

   Important: The defined object that you click cannot be based on a prototype.
4. Drag the defined object from the defined view tree to the appropriate icon in the prototype view tree.

   A prototype is built based on the defined object. The original object remains unchanged in the Defined View and in the configuration database.

Creating a new queue manager from a predefined prototype

Do the following steps to create a new queue manager from a predefined queue manager prototype:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the **Defined and Prototype** view by clicking **Defined and Prototype** in the Configuration view.

   The defined view tree and prototype view tree are positioned and sized so that you can easily drag objects between them, as shown in Figure 19.

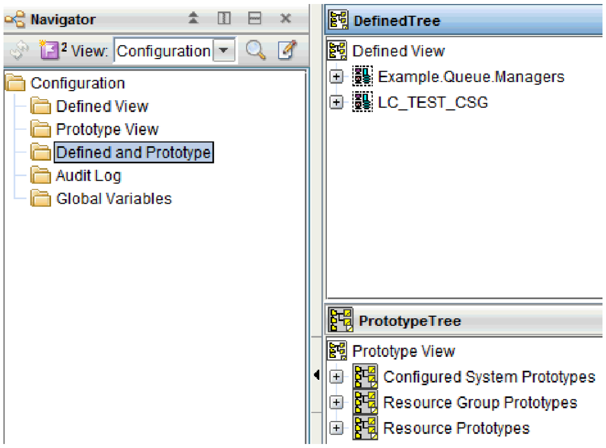
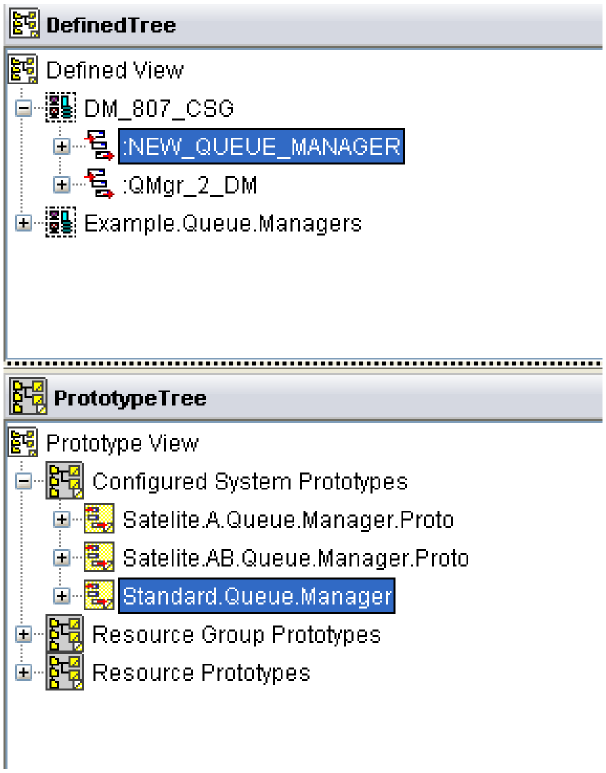


Figure 19. Defined and Prototype view

3. In the prototype view tree, expand **Configured System Prototypes**.
4. Locate the prototype named Standard.Queue.Manager.
5. Drag the Standard.Queue.Manager icon to the icon of the configured system group to which you want to add the new queue manager in the defined view tree.

   A queue manager named NEW_QUEUE_MANAGER is created in the configured system group, as shown in Figure 20 on page 36
6. Modify the name of the queue manager in its settings list on the right side of the defined view.
7. In the **Manager** section of the settings list, enter a host system name in the **Host system name** field or select a name from the list.

   The host system name is the name of the host on which you plan to create this queue manager.



DefinedTree

Defined View

DM_807_CSG

:NEW_QUEUE_MANAGER

:QMgr_2_DM

Example.Queue.Managers

PrototypeTree

Prototype View

Configured System Prototypes

Satelite.A.Queue.Manager.Proto

Satelite.AB.Queue.Manager.Proto

Standard.Queue.Manager

Resource Group Prototypes

Resource Prototypes

Figure 20. Creating a new queue manager from a predefined prototype

Guidelines for dragging objects

Use these guidelines when dragging objects:

- You must be in update mode to drag objects.
- You can drag instances of queue manager prototypes into defined configured system groups only.
- You can drag instances of resource group prototypes into defined queue managers or defined resource groups.
- You can drag instances of resources into defined resource groups or defined queue managers.

Creating objects from prototypes in the Defined View

After you create a prototype, you can create an object that is based on that prototype in the Defined View. When you drag a prototype to the Defined View, WebSphere MQ Configuration agent adds a new icon to the Defined View, creates a defined object that is based on the prototype, and adds its definitions to the configuration database.

Any changes that you make to the original prototype in the Prototype View automatically updates the objects that are based on the prototype.

Remember: When you delete a prototype, the defined objects that are created based on this prototype are also deleted automatically.

To create an object that is based on a prototype in the Defined View, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Open the Defined and Prototype View by clicking **Defined and Prototype** in the Configuration view. The defined view tree and prototype view tree are positioned and sized so that you can easily drag objects between them, as shown in Figure 21.

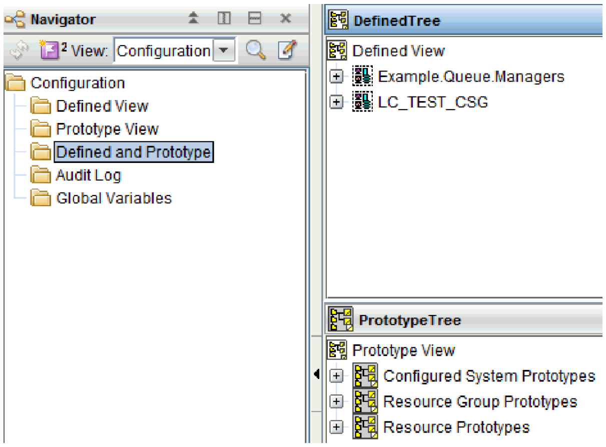


Figure 21. Defined and Prototype View

3. In the prototype view tree, click the prototype that you want to use as the basis for the new object.
4. Drag the selected prototype from the prototype view tree to the appropriate location in the defined view tree. An object that is based on the prototype is added to the configuration database. The prototype icon changes to the corresponding defined icon.

   Hint: The new object has the name that is specified by the prototype unless another object with the same name already exists. In this case, a number is appended automatically to the name of the new object to make it unique.
5. If necessary, right-click the defined object and click **Refresh** to update the Defined View display. Although the object is now part of the defined configuration, it is not added to your actual WebSphere MQ configuration until you click **Update** > **Actual from defined** to update the actual configuration. See “Updating your actual configuration from defined objects” on page 85.

Variables and prototypes

When used with prototypes, variables ensure consistency throughout your configuration and can help you quickly identify objects that are based on the same prototype.

WebSphere MQ Configuration agent provides a **Global Variables** workspace that you can use to create your own global user variables. Global user variables are available for use by any individual object in the configuration.

Symbolic variables are local to a particular defined or prototype object. All the subordinate objects of a prototype can inherit the symbolic variables. Symbolic variables are defined in the **Symbolic variables** field of the settings list for the object (for example, in the Prototype section of a prototype object).

Variables resolve only after you create an instance of the prototype in the Defined View. If necessary, you can override variables after the objects are defined in the Defined View.

You can view resolved global variables or symbolic variables in the Defined View using the **View Resolved** menu option. For more information see "Viewing resolved variables" on page 45.

Global variables versus symbolic variables

You can use global variables with prototypes to provide a powerful way to define and maintain a value in a single place; the value can be referred to symbolically in many resources. You can use global variables with any object.

Symbolic variables are variables that apply to only one prototype and can be inherited by subordinate objects within that prototype. For example, a symbolic variable that you define at the queue manager level is available to all subordinate resource groups and resources.

Product provided global variables

WebSphere MQ Configuration agent provides the following global variables:

APPLNAME
The application type (for example, MQ) that is associated with the current object.

CFGSYSNM
The name of the current configured system (for example, queue manager).

HOSTNAME
The host name that is associated with the current configured system.

You cannot delete, or modify these global variables. You might see them in some of the sample prototypes and you can use them in your prototypes.

Dynamic variables

WebSphere MQ Configuration agent provides the following dynamic variables. These variables are dynamic in the sense that they are likely to have a different value each time they are referenced.

DATE Current local date at the Tivoli Enterprise Monitoring Server, in the *yymmdd* format. You can use this variable when you are dynamically creating multiple resources; use the date to form part of a unique resource name.

JDATE
Current Julian local date at the Tivoli Enterprise Monitoring Server, in the *yyddd* format. You can use this variable when you are dynamically creating multiple resources; use the date to form part of a unique resource name.

TIME Current local time at the Tivoli Enterprise Monitoring Server, in the *hhmmss* format. You can use this variable when you are dynamically creating multiple resources; use the time to form part of a unique resource name.

User ID
Current logged on user ID. This value is displayed in the **System Information** area of the Configuration workspace. This is the user ID that you typed in the Tivoli Enterprise Portal Logon window; the case of the ID (uppercase or lowercase) is also the same.

Use dynamic variables with resources in the Prototype View. When you drag a prototype that uses a dynamic variable to the Defined View, the dynamic variable references the value that is current at the time that you drag the prototype. For example, you might create a prototype that contains `Created by &MYUSER on &MYDATE at &MYTIME` in the **Description** field and that contains `MYDATE=&DATE,MYTIME=&TIME,MYUSER=&USERID` in the **Symbolic Variables** field.

Do not use dynamic variables if you are creating resources in the Defined View without using a prototype. For example, if you create a resource in the Defined View without using a prototype and you use the &TIME variable, the dynamic variable references one value when you save the resource, but when you perform a View discrepancies action, the resource in the Defined View references a new value and always causes a discrepancy.

Global Variables workspace

Use the Global Variables workspace to view the global user variables that are currently defined for your WebSphere MQ Configuration agent. Global user variables are variables that your site creates. The values of these variables can be referenced in the settings list of any WebSphere MQ Configuration agent object.

If you are authorized to do so, you can use the Global Variables workspace to create, modify the values of, or delete global user variables of your site.

The Global Variables workspace displays global user variables of your site in a report-like format. The workspace lists the following information for each variable:

Variable
The name of the global user variable.

Value The value that the variable resolves to.

Description
An optional text description of the variable.

Adding, modifying, or deleting global user variables

You can add, modify, and delete global user variables.

Guidelines for adding, modifying, or deleting global user variables

Use these guidelines when adding, modifying, or deleting global user variables:

- You must be in update mode to add, modify, or delete variables.
- You can modify the value or description of an existing global user variable, but you cannot modify its name directly. If you want to change the name of a variable, you must delete the variable and then create a new one.

Best practice: Because global variables can be updated by multiple user IDs at the same time, to avoid conflict, use only one single ID to add, modify, or delete global variables.

Adding a global user variable

To add a global user variable, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Global Variables workspace.

   The list of global user variables is displayed.
3. Click **Add User Variable**.

   The Add User Variable window opens, as shown in Figure 22.

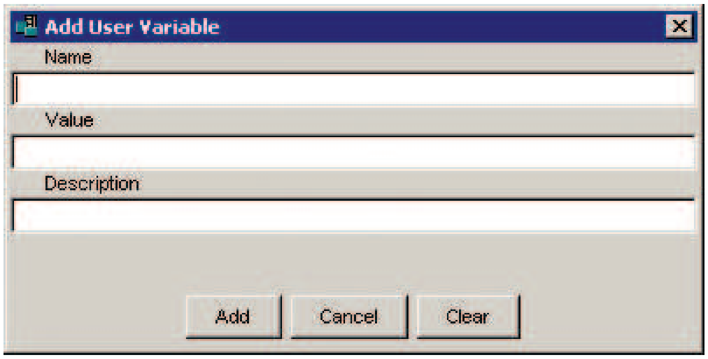


Figure 22. Add User Variable dialog

4. Enter the name of your new variable (1 - 48 case-sensitive characters) in the **Name** field.
5. Enter the value of your new variable (1 - 64 case-sensitive characters) in the **Value** field.
6. Enter an optional text description for the new variable (1 - 64 case-sensitive characters) in the **Description** field.
7. Click **Add**.

The variable is added to the list of global user variables.

Modifying a global user variable

Do the following steps to modify a global user variable:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

Remember: You can modify the value or description of an existing global user variable, but you cannot modify its name directly. If you want to change the name of a variable, you must delete the variable and then create a new one.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Global Variables workspace.

   The list of global user variables is displayed.

3. Double-click in the **Value** field or the **Description** field of the variable that you want to modify.

   A blinking text cursor is displayed in the field; you can now edit the field.
4. Edit the variable as appropriate.
5. Click **Save** to save your changes.

Deleting a global user variable

To delete a global user variable, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. For information about how to enter update mode, see "Entering update mode" on page 18.
2. Open the Global Variables workspace. The list of global user variables is displayed.
3. Select the variable that you want to delete and click **Delete User Variable**.

   Remember: When you delete a variable, be sure to also delete any references to the variable from any settings list.
   The user variable is deleted from the Global variable editor.
4. Click **Save** to save your changes.

Adding global variables to a prototype

You can add global variables to a prototype. Follow the guidelines in "Guidelines for using global variables with an object" when you add global variables to a prototype. "Example of adding a global variable to a prototype" on page 42 shows how to add a global variable to a prototype.

Guidelines for using global variables with an object

Use these guidelines when using global variables with an object:

- You must be in update mode to add global variables to an object.
- When you reference a global variable in the text field of a settings list, it must be preceded by an ampersand (&). For example, if the APPLNAME global variable has a value of MQ, you can reference the variable by entering `&APPLNAME`.
- To use multiple global variables together or use global variables together with descriptive text, use a period to indicate the end of a variable name. The period is not displayed when the variable is resolved. For example, if the APPLNAME global variable has a value of MQ and the HOSTNAME variable has a value of tiv01, `&APPLNAME..&HOSTNAME.New_Queue` resolves to `MQ.tiv01New_Queue`.
- The values of variables can reference other variables, but circular references are not supported. For example, the following variables are not supported:

  ```
  DESC1=&DESC2.1
  DESC2=&DESC1.1
  ```
- To use a global user variable, be sure that it is defined in the **Global Variables** workspace.
- You can use a global variable in any text field of a settings list.
- Variable names cannot include the period (.), equal sign (=), comma (,), space, ampersand (&) or left angle bracket (<).
- Variable values cannot include the equal sign (=) or comma (,).

Example of adding a global variable to a prototype

In the following example, you create a global variable to identify your payroll system on the west coast in California. You want to be able to identify that the system is WebSphere MQ in the Los Angeles office.

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform the operations described in this example.

1. Ensure that you are in update mode. For information about how to enter update mode, see "Entering update mode" on page 18.
2. Open the Global Variables workspace.
3. Click **Add User Variable**.
4. Enter `LAQ` in the **Name** field.
5. Enter `Los_Angeles` in the **Value** field.
6. Click the **Value** field of the APPLNAME variable and enter `MQ`.
7. Create a queue manager prototype:
   a. Open the Defined and Prototype View.
   b. Right-click **Configured System Prototypes** and click **Create** > **Queue Manager**.
   c. When prompted for the name of the queue manager prototype, enter `My_New_Queue_Manager`.
   d. Open the settings list of the queue manager prototype.
   e. Expand the **Manager** section and enter `&APPLNAME..&LAQ..Payroll_West` in the **Name** field.
   f. Complete the settings sections and click **Save** to save your changes.
8. Drag an instance of the prototype to the Defined View, the queue manager name is displayed as `MQ.Los_Angeles.Payroll_West`. The name is based on the global variables that you entered.

Adding symbolic variables to prototypes

You can add symbolic variables to prototypes. Follow the guidelines in "Guidelines for adding symbolic variables to prototypes" when adding symbolic variables to a prototype. "Example of adding symbolic variables to prototypes" on page 43 shows how to add symbolic variables to a prototype.

Guidelines for adding symbolic variables to prototypes

Use these guidelines when adding symbolic variables to prototypes:

- You must be in update mode to add symbolic variables to prototypes.
- Before you can add symbolic variables to prototypes, you must define them in the **Symbolic variables** field in the Prototype section of the settings list.
- You can use a symbolic variable in any text field of a settings list.
- When you reference a symbolic variable in the text field of a settings list, it must be preceded by an ampersand (&).
- Variable names cannot include the period (.), equal sign (=), comma (,), space, ampersand (&) or left angle bracket (<) characters.
- Variable values cannot include the equal sign (=) or comma (,) characters.
- To use multiple variables together or use variables together with descriptive text, use a period to indicate the end of a variable name. The period is not displayed when the variable is resolved.

- You can override symbolic variables for a particular object if necessary after it is in the Defined View. See “Overriding assigned symbolic variables” on page 44
- The values of variables can reference other variables, but circular references are not supported. For example, the following variables are not supported:

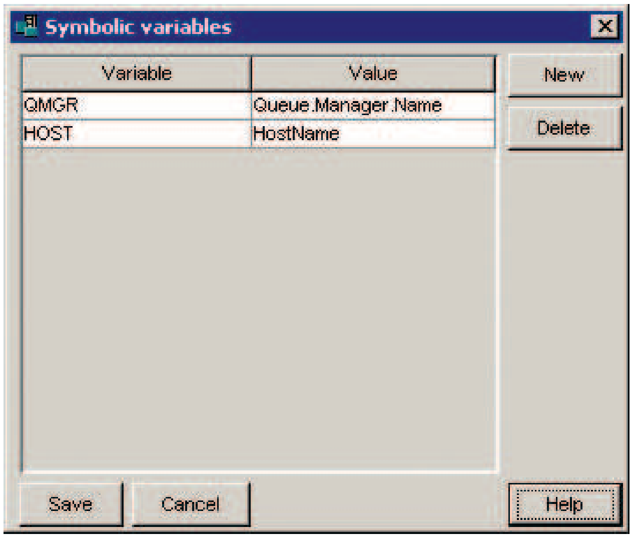
```
DESC1=&DESC2.1
DESC2=&DESC1.1
```

Example of adding symbolic variables to prototypes

In the following example, you create and use symbolic variables in prototype objects:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform the operations described in this example.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Create a queue manager prototype:
   a. Open the Defined and Prototype View.
   b. Right-click **Configured System Prototypes** and click **Create** > **Queue Manager**.
   c. When prompted for the name of the queue manager prototype, enter `Satellite.Queue.Manager.Proto`.
   d. Open the settings list of the queue manager prototype.
   e. Locate the **Symbolic variables** field and double-click its **Value** field. The Symbolic variables window opens as shown in Figure 23:



Variable	Value
QMGR	Queue.Manager.Name
HOST	HostName

Figure 23. Symbolic variables dialog

   f. Enter `QMGR` in the **Variable** field and `Queue.Manager.Name` in the **Value** field.
   g. Click **New**, enter `HOST` in the **Variable** field, and `HostName` in the **Value** field.
   h. Click **Save** to save your variable definitions and to close the Symbolic variables window.
3. Expand the **Manager** section in the settings list for the queue manager prototype.
4. Enter `&QMGR` in the **Name** field.

5. Enter `&HOST` in the **Host system name** field.
6. Complete the settings sections and click **Save** to save your changes.

   The queue manager prototype named Satellite.Queue.Manager.Proto is displayed in the prototype view tree.
7. Drag an instance of the prototype to the Defined View, the queue manager name is displayed as `HostName:Queue.Manager.Name`, based on the symbolic variables that you defined.

Overriding assigned symbolic variables

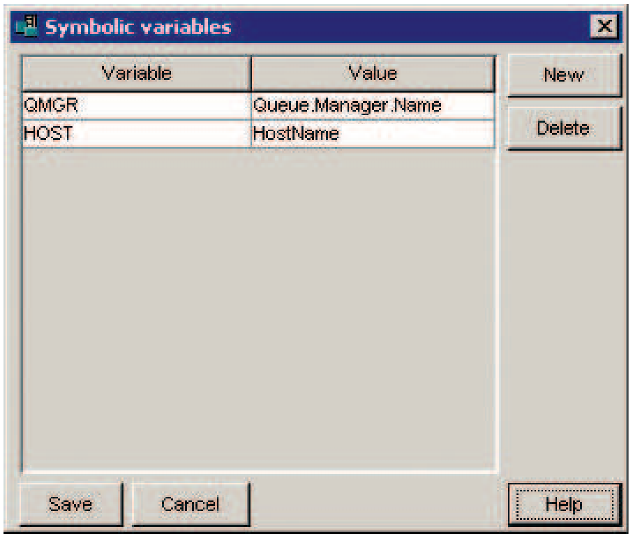
To override the assigned symbolic variables, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined View.
3. In the defined view tree, select the object that has symbolic variables that you want to override.

   The settings list for the object displays on the right side of the Defined View.
4. Expand the **Based On** section of the selected object.
5. Double-click the **Value** field in the **Symbolic variables** field.

   The Symbolic variables window opens, as shown in Figure 24.



Variable	Value
QMGR	Queue.Manager.Name
HOST	HostName

Figure 24. Override the assigned symbolic variables

6. Change the value of the variables as you need and click **Save** to save your changes and to close the Symbolic variables window.
7. Click **Save** to save your changes.

   The override affects the selected object only. None of the other defined objects that are based on the original prototype are affected.

Viewing resolved variables

If the current object is inherited from a prototype, the variables that are defined in the prototype are overridden by the global and symbolic variables that are defined with the same name. In this case, to view resolved variables:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Search for the variables in the symbolic variables that are defined at the current object to view the values.
2. If the current object has a parent resource group or queue manager, search for the variables in the symbolic variables that are defined at the parent resource group or queue manager, to view the values.
3. If the current object is inherited from a prototype, search for the variables in the symbolic variables that are defined at the prototype that it is inherited from, to view the values.
4. If you still cannot find the symbolic variables after doing the first three steps, search for the variables in the Global Variables workspace to view the values.

About using subsections of variables

You can reference a certain subsection of a global or symbolic variable using the following syntax:

```
&VariableName<iStart,iLen>
```

where *VariableName* is the global or symbolic variable name, *iStart* is the index within the variable at which the subsection begins (the index of the first character in the variable is 1), and *iLen* is the length of the subsection, in number of characters from the *iStart* position.

For example, if you have a global variable called GVTEST with the value ABCDEFGH, you can reference it using `&GVTEST<3:2>`. This resolves to CD. A field containing `&GVTEST<3:2>.Test` resolves to CDTest.

Viewing the settings of a prototype that an object is based on

You can view the settings of a prototype that an object is based on.

Do the following steps to view the settings of a prototype that an object is based on:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Open the Defined View.
2. Right-click an object that is based on a prototype and click **Select base object**. The prototype that this object is based on is highlighted in the Prototype View and its settings list is displayed on the right side of the Prototype View.

Reverting the settings of an object to its prototype

You can revert the settings of an object to the prototype that it is based on.

Do the following steps to revert the settings of an object to the prototype that it is based on:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined View.
3. In the Defined View, right-click an object whose settings you want to revert to the prototype on which it is based and click **Revert to base object**.

The settings of the object are now consistent with those of the prototype that this object is based on.

Determining which objects use a prototype

Do the following steps to see which objects are using a certain prototype:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Open the Prototype View.
2. Right-click the prototype in the prototype view tree and click **Show Using**.

   The Show Using window lists the following information about the prototype object:

   - The name of the configured system that uses this prototype
   - The name of the defined object (in the Defined View)
   - The resource type of the defined object

After you determine which prototype an object is using, you can use the Disinherit from Prototype function or the Disinherit function to break the prototype association. See "Breaking prototype associations."

Breaking prototype associations

You can either break prototype associations between a prototype and all objects using it or you can break prototype association between a prototype and a defined object that is using it.

Breaking the associations between a prototype and all objects that are using it

Do the following steps to break the association between a prototype and all objects that are using it:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Prototype View.

3. In the prototype view tree, right-click the prototype that you want to disassociate from all objects that are using it and click **Disinherit objects**.
4. Right-click **Defined View** in the Defined Tree window and click **Refresh** to refresh the objects whose association with the prototype is broken.

Breaking the association between a prototype and a defined object

To break the association between a prototype and a defined object that is using it, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Open the Defined View and select the defined object that is using the prototype.
3. Right-click the defined object and click **Disinherit**.
4. Right-click the defined object and click **Refresh**.

Example of planning with prototypes

If you want to create a new queue manager containing a set of queues, and you want to do this as easily as possible using prototypes, but still define certain properties, you can follow this example.

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform the operations described in this example.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Create a new configured system group to contain the resources.
   a. Open the Defined View.
   b. Right-click **Defined View** at the top of the defined view tree and click **Create Configured System Group**. You are prompted to supply a name for the new configured system group.
   c. Enter `group1`.
3. Create a standard queue manager inside the group1 configured system group.
   a. Open the Defined and Prototype View.
   b. Expand **Configured System Prototypes** in the Prototype View.
   c. Click the Standard.Queue.Manager prototype and drag it to the group1 configured system group in the Defined View. The new queue manager is now displayed in the Defined View.
   d. Enter `qm1` in the **Name** field of the settings list of the new queue manager, as shown in Figure 25 on page 48.

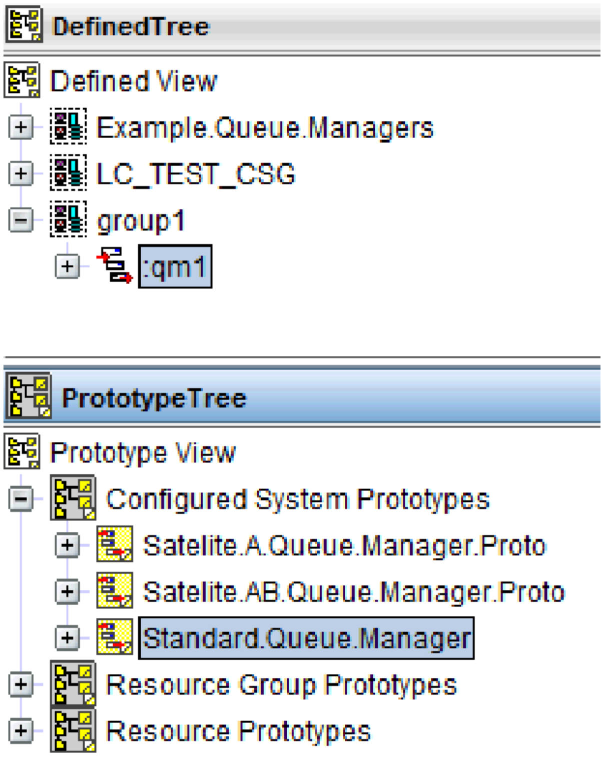


Figure 25. Creating a new queue manager from a prototype

e. Enter a host system name in the **Host system name** field of the settings list of the new queue manager. The host system name is the name of the host system on which you plan to create the queue manager.

4. Use prototypes to create a set of three queues inside the qm1 queue manager.

a. Open the Prototype View.

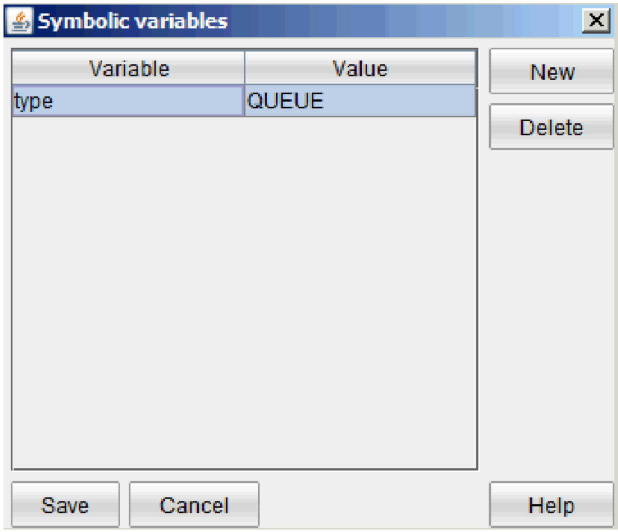
b. Right-click **Resource Prototypes** and click **Create** > **Queue:Local**. You are prompted to enter a name for the new queue prototype.

c. Enter `Qproto1` for the new queue prototype. Qproto1 is now displayed in the list of Resource Prototypes.

d. Create a global variable with the name `prefix` and the value `MYCO.MYDEPT`. See "Adding a global user variable" on page 40 for information about how to create a global variable.

e. Double-click the **Symbolic variables** field in the settings list of the queue prototype.

f. Enter a variable name of `type` and a value of `queue`, as shown in Figure 26 on page 49



Variable	Value
type	QUEUE

Figure 26. Defining symbolic variables

g. Open the **Common** section of the settings list of the queue prototype and enter `&prefix..&type` in the **Name** field. When referencing a variable, the variable name must be proceeded by an ampersand (&). The period (.) is used to separate variable names and is not displayed, but you actually want a period to be included between the two names, so you must use two periods.

h. Open the Defined and Prototype View.

i. Drag the Qproto1 prototype onto qm1 in the Defined View. A new queue named MYCO.MYDEPT.QUEUE is created. You can do this step multiple times to create more queues based on the Qproto1 prototype.

Chapter 4. Creating and defining objects in the defined view

You can create and define objects in the Defined View.

Objects in the Defined View represent WebSphere MQ resources that WebSphere MQ Configuration agent manages. These resources include all types of objects in an actual WebSphere MQ configuration, such as queue managers, queues, channels, processes, and namelists.

Each object in the Defined View has its own settings list that contains information specific to that object. Most of the information that you specify in the settings list corresponds to values that you would specify on the command line if you created objects manually using WebSphere MQ commands.

The objects that are displayed in the Defined View are defined in the configuration database and might be objects that do not yet exist in your actual WebSphere MQ environment.

You use settings lists to define object values in WebSphere MQ Configuration agent. Because you can use different methods to add objects to your Defined View, there might be times when you need to know the origin of object data. Typically, the color of the data that is displayed in the settings list for a defined object indicates the source of the data, as follows:

Black This data is explicitly defined for the object.

Green This data is a default value of WebSphere MQ or WebSphere MQ Configuration agent.

Blue This data is inherited from a prototype.

After you add objects to your configuration database, test the definitions to ensure that the objects were defined properly. The validation process checks the configuration database only; it does not query actual queue manager data in your WebSphere MQ environment. See Chapter 5, “Validating the configuration of your WebSphere MQ environment,” on page 75 for instructions.

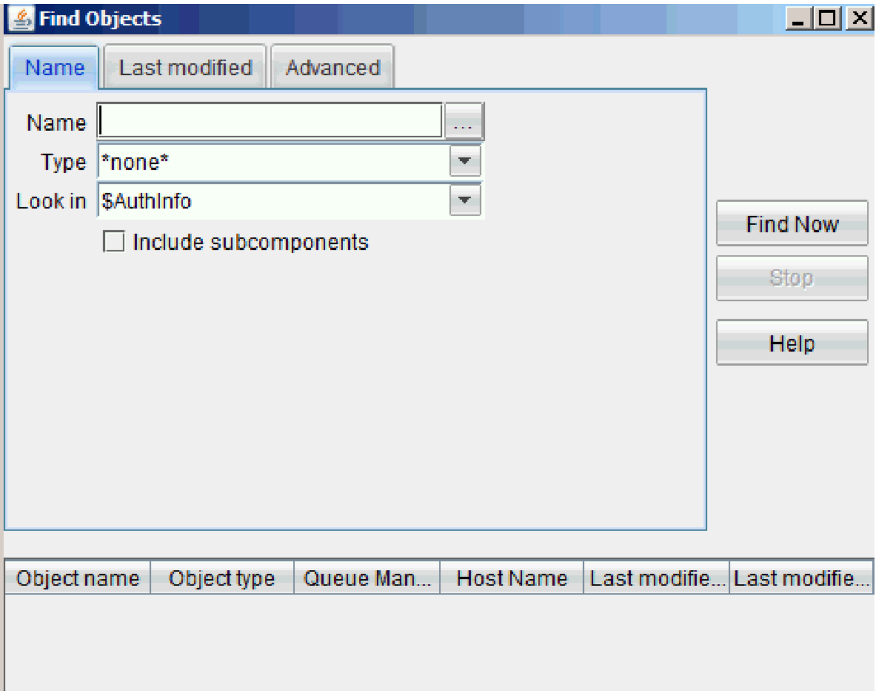
Searching for an object in the configuration database

You can use the search function that is provided by the WebSphere MQ Configuration agent to search for a particular object in the configuration database by name, object type, or object attributes. To search for an object in the configuration database, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Open the defined or prototype view, and select any object in the navigation tree.
2. Right-click the selected object and, from the menu, click **Find**.

   The Find Objects window opens.



Name

Type *none*

Look in $AuthInfo

□ Include subcomponents

Figure 27. Find Objects dialog

3. Use the Name page to specify the name and type of the object that you want to find.
   - Enter an expression representing the names or part of the names of the objects that you want to search for in the **Name** field. You can use the asterisk (*) or question mark (?) wildcard characters at the end of the search string. The asterisk represents any character or sequence of characters, and the question mark represents any single character. The wildcard character is regarded as a place holder when it is used in the search string.

     Tip: To enter a long name string, click the button next to this field. A small window is displayed for you to input the name. Click **Save** to close this window.
   - Select the type of object to search for. If you want to search all configuration objects, regardless of type, select ***none***.
   - Select the point in the object hierarchy at which to begin the search using the **Look in** list. The search includes only the descendants of the selected object. The items in this list depend on the object that was selected when you opened the Find Objects window. The object that was selected when the Find Objects window was first opened is selected by default in the **Look in** list. The list also contains ancestors of the object, which you can select as the start point of the search instead of the default object if required.
   - Indicate whether subcomponents should be included in the search. Select **Include subcomponents** to include the descendants of the object that is selected in the **Look in** list.

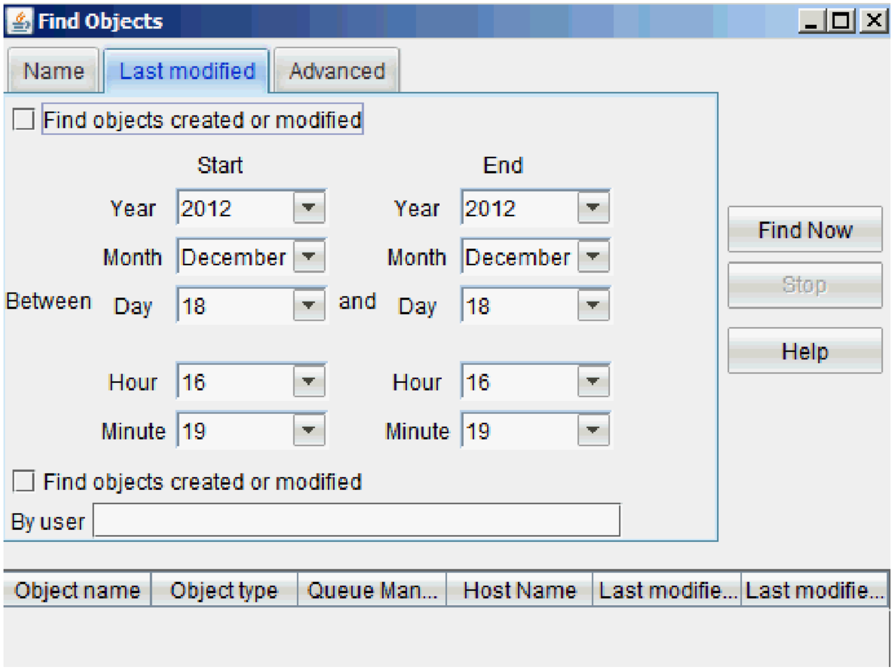
   Important:

   a. The search is not case sensitive and it returns all objects whose name includes the string that is specified in the **Name** field, for example, if you set the **Name** field to `test`, the objects that are named `testQueue`, `testQMGR`, and `Test` are all returned and listed in the results window.

b. All objects that are descendants of the object that are selected in **Look in** list are returned and listed in the result window if you only enter an asterisk (*) in the **Name** field or leave it as blank, and select **Include subcomponents**.

c. The queue manager name is considered to begin with the host name.

4. Optional: You can optionally include the date that the object was last modified or the name of the user who modified it in the search criteria. To do this, click the **Last Modified** tab and enter the search criteria as follows:
   - To search for objects that were created or modified between two specific dates, select the upper left **Find objects created or modified** check box, then enter the search criteria in the fields provided. Enter the start date and time in the fields located directly beneath the **Start** heading, and the end date and time in the fields located beneath the **End** heading.
   - To search for objects that were created or modified by a particular user, select the lower **Find objects created or modified** check box, then enter the name of the user who created or modified the objects that you want to search for.



□ Find objects created or modified

	Start		End
Year	2012	Year	2012
Month	December	Month	December
Between Day	18	and Day	18
Hour	16	Hour	16
Minute	19	Minute	19

□ Find objects created or modified

By user

Figure 28. Find objects by date, user ID, or both

5. Optional: You can specify advanced search criteria to perform more complex search operations. To do this, click the **Advanced** tab and enter search criteria as follows:

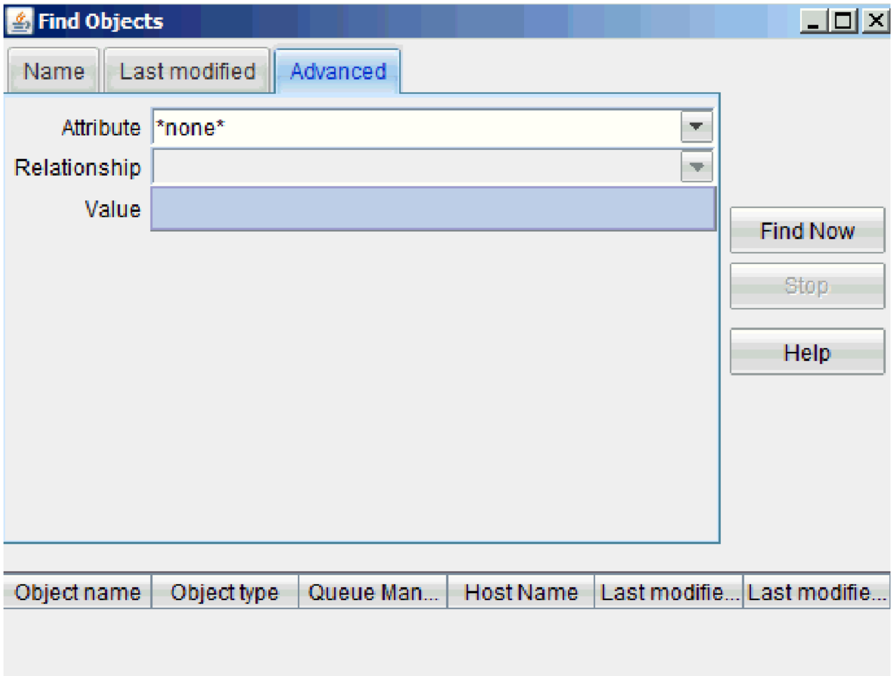


Figure 29. Advanced search options

- Use the **Attribute** menu to select an attribute of the object type that is specified in the **Type** field on the **Name** tab.
- Use the **Relationship** menu to select the type of comparison to perform against the specified value of the attribute. The types of comparison available depend on the type of value that the attribute can take. For example, six types of comparison (equal, not equal, greater than, less than, greater than or equal, less than or equal) are available for an attribute with a numeric value, but an attribute with a boolean value supports only two types of comparison (equal and not equal).
- Use the **Value** field to enter the value to compare the attribute against (if the attribute is a boolean variable, a list of possible values is provided).

6. Click **Find Now** to start searching.

After the search has begun, the results table in the lower section of the window is updated whenever a new object is discovered, so that each row represents a configuration object that matches the search criteria. The table contains the following columns:

- The name of the object
- The resource type of the object
- The name of the queue manager to which the object belongs
- The date and time that the object was last modified
- The name of the user who last modified the object
- The name of the host that the object is installed

Important:

- You can stop the search at any time by clicking **Stop**. All previously found objects are still displayed in the results table.
- All the search criteria that you specify in the Name, Last modified and Advanced tab pages are combined to form the final criteria of the search that determine which objects are returned and displayed in the results table.

7. Highlight an object in the results table to perform the following actions:
   - Click **Edit** to open the settings list for the object. You must be in update mode to perform this operation.
   - Click **Show in Tree** to locate the object in either the defined or prototype view (depending on the object type and where it is located). The display shows the view that you selected; the trees in the view are expanded so that you can see the item.

Displaying a filtered list of resources in a resource group

If you have a resource group that contains a large number of resources, it can be useful to filter those resources to view a certain subset of the whole group, or to search for resources of particular interest, for example, those resources that were updated over a particular period of time.

To display a filtered list of the resources that are contained within a particular resource group, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Open the defined view and select the resource group that you want to filter.
2. Right-click the resource group and click **Display Resources**.
3. In the Resource Filter window, enter the filter parameters as follows:
   - In the **Resource Name** field, enter a regular expression by which to filter resources by name. This field supports the asterisk (*) wildcard character to represent any character or sequence of characters. If you do not want to filter objects by name, leave this field blank.
   - In the **Resource Type** field, select an object type to include only objects of that type in the filtered list.
   - Select the **Recurse into lower level resource groups** option if you want the filtered list to include descendents of the children of the selected object; otherwise, only the children themselves are included in the filtered list.
   - Select the **Exclude Filtered Resources** option to apply an inverse filter to the resource group. The filtered list contains all objects that are typically excluded by the filter, and exclude the objects that are typically included.
   - Use the **Update date** option to include only objects that were last updated on, after, or before a particular date. Enter the date to filter by in the date field in the *yy/mm/dd* form.
4. Click **OK** to display the filtered list.

   The Resources window opens. It contains the following information about each resource:
   - Resource name
   - Resource type
   - Name of the user who last updated the resource
   - Date and time that the resource was last updated

From the Resources window you can do the following two operations:

- To view the settings list of a resource, select the resource and click **Edit**.
- To navigate to the location of a particular resource or resources in the defined view, select the resources (press Shift and click two resources if you want to

select these two resources and all resources between them. Press Ctrl and click the resources if you want to select multiple separate resources) and click **Show in tree**.

Creating a new queue manager definition

To create a new queue manager definition for a queue manager that does not yet exist in your actual WebSphere MQ environment, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined and Prototype View by clicking **Defined and Prototype** in the Configuration View.

   The defined view tree and prototype view tree are positioned and sized so that you can easily drag objects between them, as shown in Figure 30.

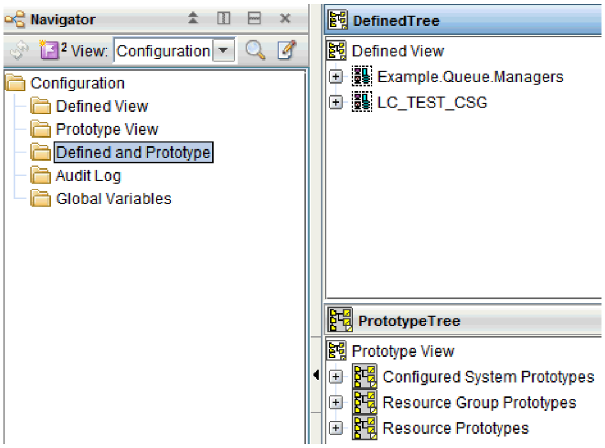


Figure 30. Defined and Prototype View

3. Right-click the configured system group to which you want to add the new queue manager in the defined view, and select **Create** > **Queue Manager**.
4. When prompted to provide a name, enter an alphanumeric name for the new queue manager, and click **OK**.

   The new queue manager object is added to the defined view tree.

   Remember:

   a. Do not use non-English characters for the new object name.
   b. SYSTEM should not be used as the prefix name that you assign to your own resource. WebSphere MQ Configuration agent identifies the resource whose prefix name is SYSTEM as a WebSphere MQ default resource and therefore skips the validation process.
   c. On z/OS systems with CCSID 1390, no WebSphere MQ objects support lowercase characters.
5. Select the new queue manager in the defined view tree.

The settings list for the queue manager is displayed on the right side of the Defined View.

6. In the **Manager** section of the settings list, click the arrow in the **Host system name** field and select the name of the host on which you want to create the queue manager. Do not type a host name manually in this field.
7. Complete the rest of the settings as necessary for your new queue manager.

   Click **Help** to display information about each parameter.
8. Add WebSphere MQ default resources as follows:
   a. In the Prototype View, expand **Resource Group Prototypes**.
   b. Locate the resource group named Default.MQSeries.Resources.
   c. Drag the Default.MQSeries.Resources icon to the appropriate queue manager icon in the defined view tree.

   Important: If you do not add default WebSphere MQ resources to new queue managers, when you perform a validating operation, you receive a validation error.

   An instance of the default resources is added to the new queue manager definition.
9. (For queue managers on systems other than z/OS systems) Select the **Auto create** check box in the **Auto Create** section of the queue manager settings list.

   Important: If you do not select **Auto create**, when you click **Update** > **Actual from defined**, the following error message is displayed.

   ```
   KMC0185E error: WebSphere MQ Configuration agent cannot create the actual queue
      manager
   ```

   When you select the **Auto create** check box and WebSphere MQ Configuration agent determines that this queue manager does not yet exist in your actual WebSphere MQ environment, it automatically creates the queue manager when you right-click it in the defined view and click **Update** > **Actual from defined**.
10. Click **Save** to save your changes.

Now the new queue manager definition is created in the Defined View and the configuration database. See “Creating resources in a resource group” on page 70 for information about how to create new resources in the queue manager.

You can also use the following ways to create queue managers in the defined view:

- Create an instance of a queue manager from a queue manager prototype in the Prototype View. See “Creating prototypes in the Prototype View” on page 32.
- Copy an existing queue manager from another configured system group in the Defined View. See “Copying an object to another location within the same view” on page 71.

Deploying a queue manager to the actual WebSphere MQ environment

After you create a queue manager definition in the Defined View, you can deploy the queue manager to the actual WebSphere MQ environment.

You need to create a queue manager definition in the Defined View. See “Creating a new queue manager definition” on page 56 for information about how to create a queue manager in the Defined View.

Do the following procedure to deploy a queue manager to the actual WebSphere MQ environment:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined and Prototype View by clicking **Defined and Prototype** in the Configuration view.

   The defined view tree and prototype view tree are positioned and sized so that you can easily drag objects between them, as shown in Figure 31.

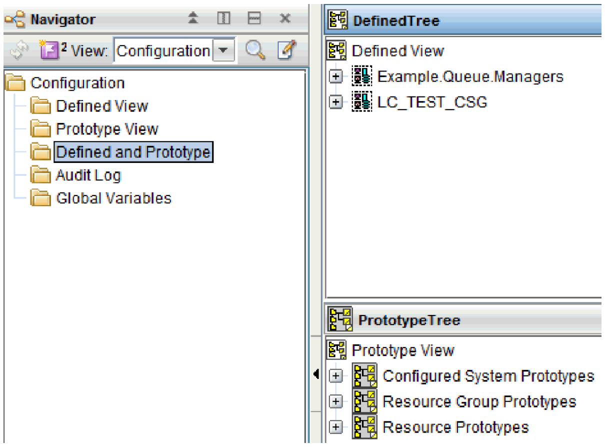


Figure 31. Defined and Prototype View

3. In the Defined View, click the queue manager that you want to deploy to your actual WebSphere MQ environment. The settings list for the queue manager is displayed on the right side of the Defined View.
4. Expand the **Auto Create** section. If the **Auto create** check box is enabled, go to step 11. If the **Auto create** check box is disabled, go to step 5.
5. Right-click the queue manager in the Defined View and click **Reset Actual Exists**. You are prompted to confirm the operation.
6. Click **Yes**. A message is displayed stating that the Reset Actual is completed successfully and you need to recycle the Tivoli Enterprise Portal to make the changes take effect.
7. Click **OK**.
8. Click **View** > **Refresh Now**. The **Auto create** check box in the **Auto Create** section is enabled and the **Name** field in the **Manager** section is editable.
9. Optional: In the **Manager** section of the settings list, enter a new alphanumeric name in the **Name** field. The queue manager that will be created in the WebSphere MQ environment will use the name that you specify in the **Name** field.
10. Optional: In the **Manager** section of the settings list, click the arrow in the **Host system name** field and select the host name on which you want to create the queue manager. Do not manually enter a host name in this field.
11. Ensure that the **Auto create** check box in the **Auto Create** section is selected.
12. Ensure that the **Auto start** check box in the **Auto Start** section is selected.

13. Click **Save** to save your changes.
14. Right-click the queue manager in the Defined View and click **Update** > **Actual from defined**. You are prompted to confirm the operation.
15. Click **Yes**. A message is displayed stating that your update request was completed successfully.
16. Click **OK**.

A queue manager with the name that you specified in the **Name** field is created on the host whose name is specified in the **Host system name** field.

Queue managers on z/OS systems

WebSphere MQ Configuration agent cannot create, delete, start, or stop queue managers running on z/OS systems, but it can perform all the other configuration functions that it provides for distributed systems. For example, after you create a queue manager on a z/OS system manually, you can use WebSphere MQ Configuration agent to discover the existing queues and channels for the queue manager and to add new queues and channels.

Starting queue managers automatically

The following actions require that the queue manager that they operate are started when they are performed:

- **Update** > **Actual from defined**
- **Update** > **Defined from actual**
- **View discrepancies**
- **View actual**

Do the following steps so that WebSphere MQ Configuration agent starts the queue manager automatically when you perform an action that requires the queue manager to be started:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

Restriction: This function is not available for z/OS queue managers.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. In the defined view tree, select the queue manager that you want WebSphere MQ Configuration agent to start automatically. The settings list for the queue manager is displayed on the right side of the Defined View.
3. Expand the **Auto Start** section and select the **Auto start** check box.
4. Complete the rest of the settings in the **Auto Start** section. You can also use the **Auto Start** section to start the WebSphere MQ listener and channel initiator.
5. Click **Save** to save your changes.

Sending commands to queue managers

You can start, stop, or send commands to a queue manager in your WebSphere MQ environment from your Defined View. Because these commands are sent to the queue manager through the WebSphere MQ Monitoring agent, you must configure the WebSphere MQ Monitoring agent to be able to issue MQSC commands before you can use this function. For information about how to configure the WebSphere MQ Monitoring agent to be able to issue MQSC commands, see *IBM Tivoli Composite Application Manager Agent for WebSphere MQ User's Guide*.

Remember: Make sure that the user ID that is used to interact with WebSphere MQ belongs to the **mqm** group. This user ID is specified by the **ACTIONACCOUNT** parameter in the configuration file of the WebSphere MQ Monitoring agent. Otherwise, an error message with error code 2035 is displayed.

Do the following steps to issue commands to a queue manager in your WebSphere MQ environment:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Select the queue manager in the defined view to which you want to send commands and right-click.
3. Depending on whether you want to start, stop, or submit MQ commands to the queue manager, click one of the following menu options. The menu options are shown in Figure 32.

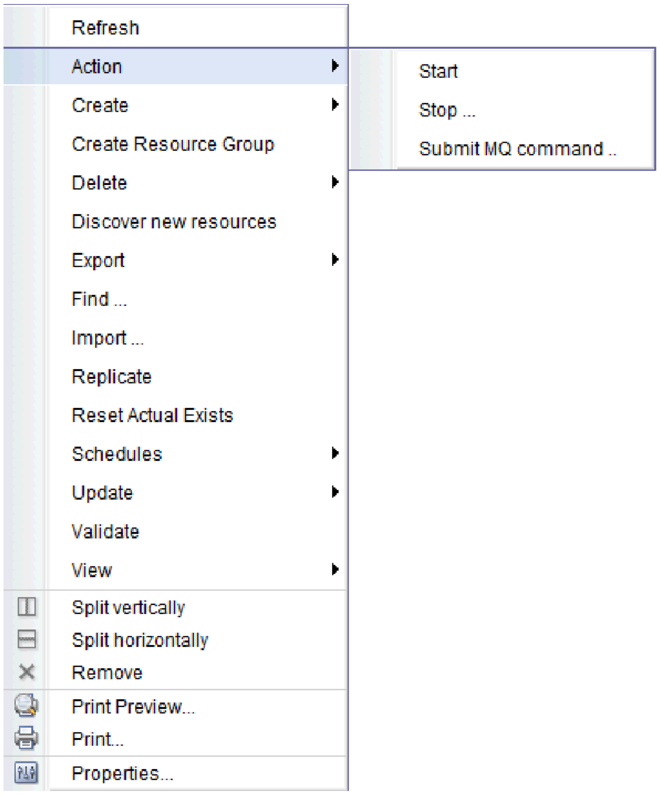


Figure 32. Action menu option

   a. **Action** > **Start**: To start the queue manager.
   b. **Action** > **Stop**: To stop the queue manager.

The Choose how to stop window opens. Depending on how you want to stop the queue manager, select one of the following options from the dropdown list:

Important: These options are equivalent to the options available on the WebSphere MQ **endmqm** command.

- **Controlled**: This is the default. If you select this mode, the queue manager is stopped, but only after all applications have disconnected. All MQI calls that are currently being processed are completed. Control is returned to you immediately.
- **Wait**: This type of shutdown is equivalent to a controlled shutdown, except that control is returned to you after the queue manager stops.
- **Immediate**: If you select this mode, the queue manager is stopped after it has completed all the MQI calls currently being processed.
- **Pre-emptive**: If you select this mode, the queue manager might stop without waiting for applications to disconnect or for MQI calls to complete. This can give unpredictable results for WebSphere MQ applications. Only use this type of shutdown under exceptional circumstances.

c. **Action** > **Submit MQ command**: Enter the MQ command that you want to issue to the queue manager in the **Command to submit** field and click **OK**.

Sending commands to channels

You can start, stop, retrieve the status of, or send commands to a channel in your WebSphere MQ environment from your Defined View. Because these commands are sent to the channel through the WebSphere MQ Monitoring agent, you must configure the WebSphere MQ Monitoring agent to be able to issue MQSC commands before you can use this function. For information about how to configure the WebSphere MQ Monitoring agent to be able to issue MQSC commands, see *IBM Tivoli Composite Application Manager Agent for WebSphere MQ User's Guide*.

Remember: Make sure that the user ID that is used to interact with WebSphere MQ belongs to the **mqm** group. This user ID is specified by the **ACTIONACCOUNT** parameter in the configuration file of the WebSphere MQ Monitoring agent. Otherwise, an error message with error code 2035 is displayed.

Do the following steps to issue commands to a channel in your WebSphere MQ environment:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Select the channel in the defined view to which you want to send commands and right-click.
3. Depending on whether you want to start, stop, retrieve the status, or submit MQ commands to the channel, select one of the following menu options as shown in Figure 33 on page 62.

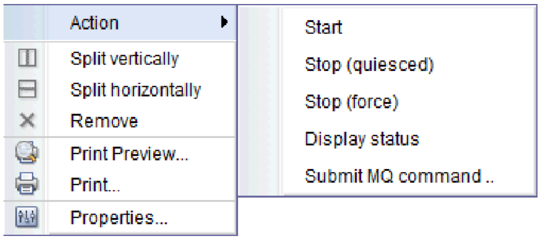


Figure 33. Action options for channels

- **Action** > **Start**: To start the channel.
- **Action** > **Stop (quiesced)**: If you select this stop mode, the channel stops when the current message is completed and the batch is then ended, even if the batch size value is not reached and there are messages already waiting on the transmission queue.
- **Action** > **Stop (force)**: If you select this stop mode, the channel stops immediately. If a batch of messages is in progress, an indoubt situation might result.
- **Action** > **Display status**: If you want to display the status of the channel.
- **Action** > **Submit MQ command**: Enter the MQ command that you want to issue to the channel in the **Command to submit** field and click **OK**.

Specifying OAM security authorizations for WebSphere MQ objects

You can configure object authority manager (OAM) security authorizations that control access authority for the following WebSphere MQ objects:

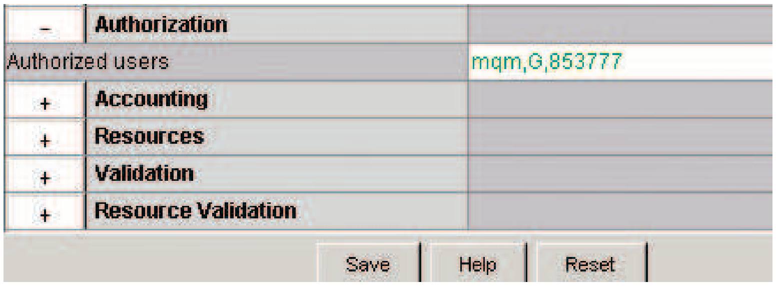
- Authentication information
- Channel
- Listener
- Namelist
- Queue
- Queue manager
- Service

Restriction: Setting OAM access authority for WebSphere MQ objects is not supported on z/OS systems.

To specify OAM security authorizations for WebSphere MQ objects:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Open the Defined View. The settings list for the object is displayed on the right side of the Defined View.
3. In the defined view tree, select the namelist, queue, or queue manager that has security authorizations that you want to set.
4. Expand the **Authorization** section.



– Authorization

Authorized users: mqm,G,853777

+ Accounting

+ Resources

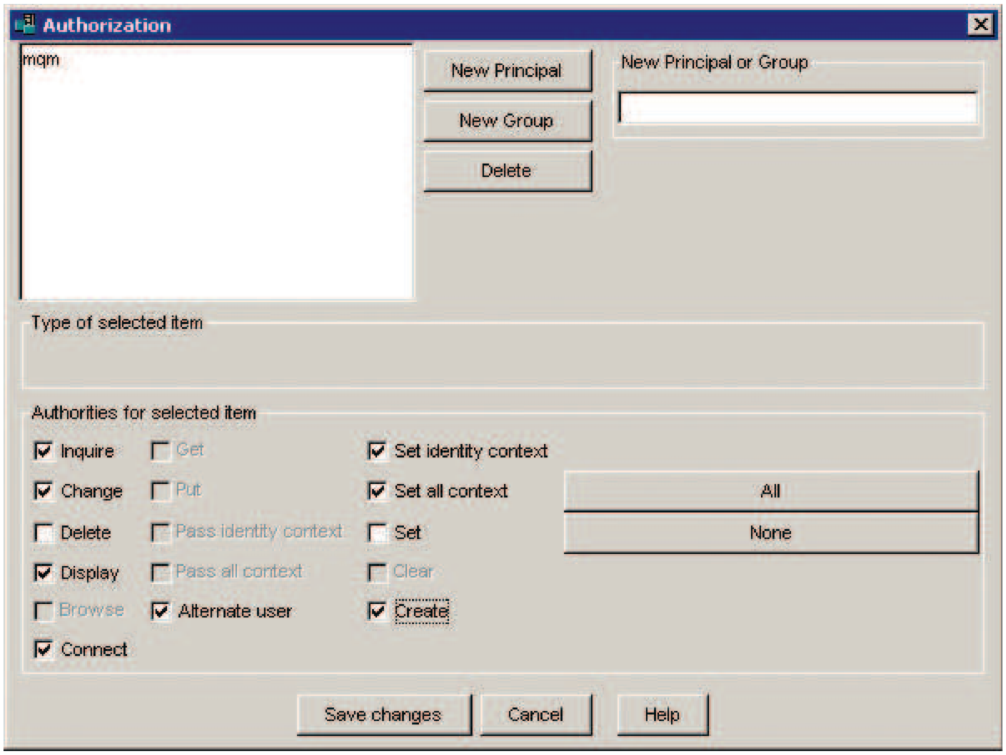
+ Validation

+ Resource Validation

Figure 34. Expand the Authorization section

The **Authorized users** field lists users (U) or user groups (G) that are authorized to use this resource. (This example shows that users who belong to the mqm user group are authorized to use this resource.) Each 3-item comma-delimited string sequence that is in this field ends with a number that is created by WebSphere MQ Configuration agent, which you can ignore.

5. Double-click the **Authorized users** field to edit this value. The Authorization window opens as shown in Figure 35:



Authorization

mqm

New Principal or Group:

Type of selected item:

Authorities for selected item

☑ Inquire □ Get ☑ Set identity context

☑ Change □ Put ☑ Set all context

□ Delete □ Pass identity context □ Set

☑ Display □ Pass all context □ Clear

□ Browse ☑ Alternate user ☑ Create

☑ Connect

Figure 35. Authorization dialog

Use this window to add, delete, or alter principals or groups; you can also specify authorities for a specific user or group. When you select an entry from the list area on the left, the **Authorities** check boxes are set according to the defined authority settings that are associated with the selected user or group. For details about using this window, click **Help**.

6. Use this window to add, delete, or alter principals or groups that are authorized to use this resource and click **Save changes** to save your change.
7. Select the **Configure WebSphere MQ Authorization** check box in the **Auto Start** section of the queue manager settings list. If you are specifying the access

authority of a queue or a namelist, you must open the settings list of the queue manager that it belongs to and select the **Configure WebSphere MQ Authorization** check box.

8. Click **Save** to save your changes.

Viewing OAM security authorizations for WebSphere MQ objects

You can view OAM security authorizations for WebSphere MQ objects in the Defined View.

Do the following steps to view OAM security authorizations for WebSphere MQ objects:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined View.
3. In the defined view tree, right-click the queue manager that has the objects whose security authorizations you want to view and click **View** > **Authorities**.

The View Authorities window is displayed, listing the users, user groups and the authorities that they have on the resources in the queue manager.

Creating links between two queue managers

You can use WebSphere MQ Configuration agent to quickly and easily create links between two queue managers. When you drag queue manager objects in the interface, WebSphere MQ Configuration agent automatically creates the necessary channels and transmission queues.

To create links between two queue managers:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined View, and expand the defined view tree as necessary.
3. Locate the first queue manager that you want to connect.
4. Locate the second queue manager.
5. Click the first queue manager that you want to connect.
6. Drag the icon of the first queue manager to the second queue manager. A resource group is automatically added to each queue manager. The resource group that is added is based on the value specified in the **Autoconnect prototype resource group** field in the **Auto Start** section of the queue manager settings list.

WebSphere MQ Configuration agent creates the necessary transmission queues and channels to link the two queue managers. They are added to the automatically created resource group for each queue manager.

Resource group

A resource group is a unit of organization within WebSphere MQ Configuration agent. Resource groups make it easy to organize queue manager resources (queues, channels, namelists, processes, and other objects) by the business purpose that they serve. For example, you can put all the resources that are associated with a particular application into a single resource group. Or you can use resource groups to logically group resources in a way that is meaningful in your environment. For example, you might want to organize the queues that are discovered on a particular queue manager into ProdQueues and TestQueues resource groups. After you organize resources into groups, you can take actions on all of the resources in the group in one step instead of issuing commands on individual resources.

Tip: If a resource group contains a large number of resources, you might experience a degradation in performance. To avoid this situation, decrease the number of resources in a resource group and create more resource groups.

$Default_Group resource group

When you use the discovery function to populate a configured system group in the Defined View, resources that are associated with each active queue manager are put into a $Default_Group resource group. Each active queue manager that you discover has its own $Default_Group resource group. After the discovery process is complete, you can use this pool of definitions to populate resource groups that you create.

The discovery process (or alternatively, the Auto Discover product option or the Discover New Resources option for Configured Systems) separates the $Default_Group resources into sub-resource group types. This process reduces potential performance issues because you have smaller resource groups, which require less client processing time.

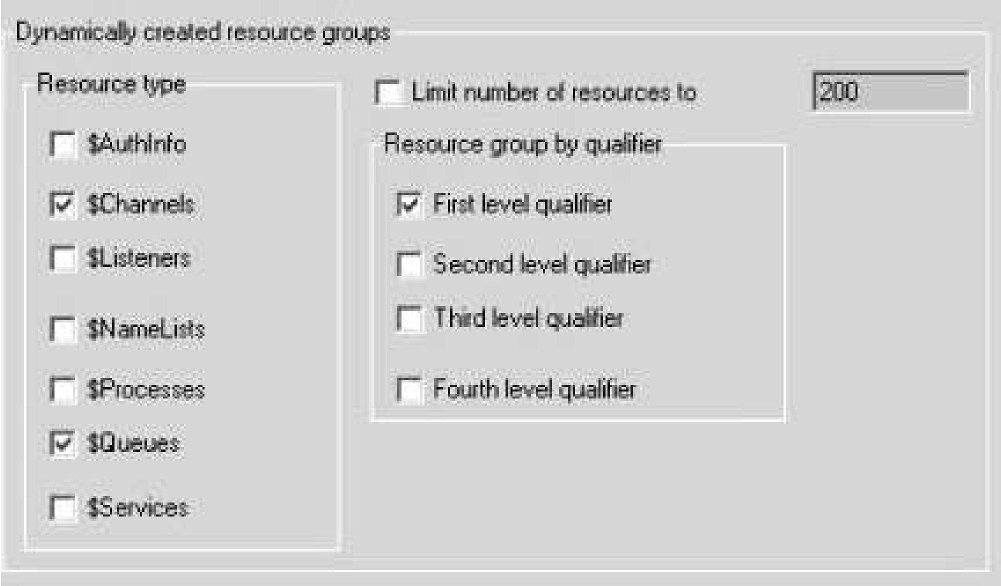
In each $Default_Group resource group, the resources are separated into the following subgroups:

- *$AuthInfo* contains all WebSphere MQ authentication information objects.
- *$Channels* contains all channels.
- *$Listeners* contains all channel listeners.
- *$Namelists* contains all namelists.
- *$Processes* contains all processes.
- *$Queues* contains all queues.
- *$StorageClasses* contains all storage classes.
- *$Service* contains all services.

For dynamic resources (permanent dynamic queues), the $DynamicResources resource group also contains sub-groups for each resource type. However, only the $Queues resource group exists, because queues are the only type of dynamic resource that is supported. Permanent dynamic queue definitions are not created in the configuration database, unless you enabled the **Configure permanent dynamic queues** option in the **Auto Start** section of the queue manager settings list.

Automatic grouping of discovered resources

The **Dynamically created resource groups** area in the Product Options area of the Configuration workspace provides the options for controlling how discovered resources are grouped. Figure 16 on page 25 shows the options for controlling how discovered resources are grouped.



Dynamically created resource groups

Resource type

☐ $AuthInfo
☑ $Channels
☐ $Listeners
☐ $NameLists
☐ $Processes
☑ $Queues
☐ $Services

☐ Limit number of resources to 200

Resource group by qualifier

☑ First level qualifier
☐ Second level qualifier
☐ Third level qualifier
☐ Fourth level qualifier

Figure 36. Controlling how discovered resources are automatically grouped

With the dynamically created resource groups function, you can control the number of resources that are automatically put into a resource group and the number of resource groups for each resource type that you select, you can also refine the classification of discovered resources by selecting different prefix level of the resource name.

The **Resource type** area includes the following resource types:

- AuthInfo
- Channels
- Listeners
- NameLists
- Processes
- Queues
- Services

The **Limit number of resources to** and **Resource group by qualifier** functions are only available after you select one or more of the resource types.

Select the **Limit number of resources to** check box to indicate that the number of resources that are placed into a resource group during discovery and the number of resource groups for each resource type that you select in the **Resource Type** area should be limited to the number that you specify. Use the entry field to indicate the maximum size (it is set to 200 in Figure 16 on page 25). If the number of resources or resource groups exceeds the number that you specify, a new resource group is created and a numeric suffix (starting with 0001) is added to the resource group name to make it unique.

By default, WebSphere MQ Configuration agent limits the number of resources that are placed into a resource group to 200. To achieve better performance, set this value to a number between 50 and 300. The number that you specify in the entry field also affects the number of resource groups that are contained in the $Default_Group resource group. If the number of discovered resource groups exceeds the number that you specify, a new default group is created.

The **Resource group by qualifier** area provides four prefix levels of the resource name for classifying discovered resources to create distinct resource groups.

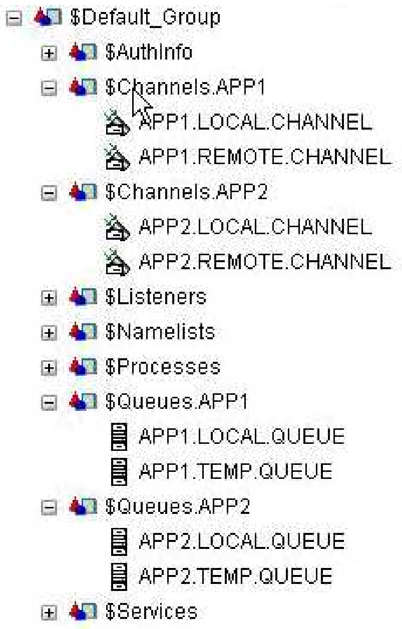
If you select the **First level qualifier** check box, the discovered resources that are of the same resource type and have the same first level qualifier are added to the same resource group, which is named using the selected resource type name and the first level qualifier name separated by a period. If you select the **Second level qualifier**, **Third level qualifier** or **Fourth level qualifier** check box, the discovered resources are added to separate resource groups in a similar way as when the **First level qualifier** is selected.

You can also select multiple level qualifier check boxes. For example, if you select both the **First level qualifier** and **Second Level qualifier** check boxes, the discovered resources that are of the same resource type and have the same first and second level qualifiers are added to the same resource group, which is named using the selected resource type, the first and the second level qualifier names separated by periods.

In the following example, it is assumed that you have the following four queues and four channels on the queue manager that you want to discover, and the **$Queues** and **$Channels** resource types are selected in the **Resource Type** area:

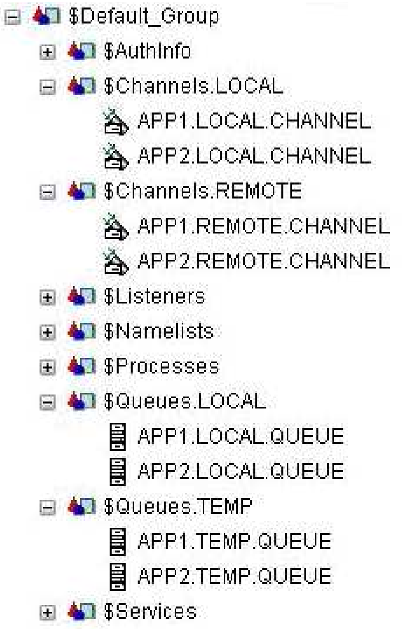
- APP1.LOCAL.QUEUE
- APP2.LOCAL.QUEUE
- APP1.TEMP.QUEUE
- APP2.TEMP.QUEUE
- APP1.LOCAL.CHANNEL
- APP2.LOCAL.CHANNEL
- APP1.REMOTE.CHANNEL
- APP2.REMOTE.CHANNEL

If you select **$Queues** and **$Channels** in the **Resource Type** section and the **First level qualifier** check box in the **Resource group by qualifier** section, two resource groups named $Queues.APP1 and $Queues.APP2 are created for the four queues in the previous list and another two resource groups named $Channels.APP1 and $Channels.APP2 are created for the four channels in the previous list during the discovery process, which are shown in the figure below:



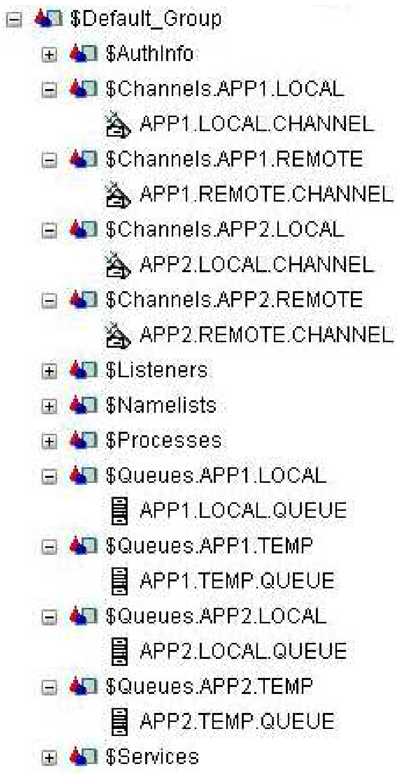
```
⊟ $Default_Group
    ⊞ $AuthInfo
    ⊟ $Channels.APP1
          APP1.LOCAL.CHANNEL
          APP1.REMOTE.CHANNEL
    ⊟ $Channels.APP2
          APP2.LOCAL.CHANNEL
          APP2.REMOTE.CHANNEL
    ⊞ $Listeners
    ⊞ $Namelists
    ⊞ $Processes
    ⊟ $Queues.APP1
          APP1.LOCAL.QUEUE
          APP1.TEMP.QUEUE
    ⊟ $Queues.APP2
          APP2.LOCAL.QUEUE
          APP2.TEMP.QUEUE
    ⊞ $Services
```

If you select **$Queues** and **$Channels** in the **Resource Type** section and the **Second level qualifier** check box in the **Resource group by qualifier** section, two resource groups named $Queues.LOCAL and $Queues.TEMP are created for the four queues in the previous list and another two resource groups named $Channels.LOCAL and $Channels.REMOTE are created for the four channels in the previous list during the discovery process, which are shown in the figure below:



```
⊟ $Default_Group
    ⊞ $AuthInfo
    ⊟ $Channels.LOCAL
          APP1.LOCAL.CHANNEL
          APP2.LOCAL.CHANNEL
    ⊟ $Channels.REMOTE
          APP1.REMOTE.CHANNEL
          APP2.REMOTE.CHANNEL
    ⊞ $Listeners
    ⊞ $Namelists
    ⊞ $Processes
    ⊟ $Queues.LOCAL
          APP1.LOCAL.QUEUE
          APP2.LOCAL.QUEUE
    ⊟ $Queues.TEMP
          APP1.TEMP.QUEUE
          APP2.TEMP.QUEUE
    ⊞ $Services
```

If you select **$Queues** and **$Channels** in the **Resource Type** section, and **First level qualifier** and **Second Level qualifier** in the **Resource group by qualifier** section, four resource groups named $Queues.APP1.LOCAL, $Queues.APP2.LOCAL, $Queues.APP1.TEMP and $Queues.APP2.TEMP are created for the four queues in the previous list and another four resource groups named $Channels.APP1.LOCAL, $Channels.APP2.LOCAL, $Channels.APP1.REMOTE and $Channels.APP2.REMOTE are created for the four channels in the previous list during the discovery process, which are shown in the figure below:



```
⊟ $Default_Group
    ⊞ $AuthInfo
    ⊟ $Channels.APP1.LOCAL
          APP1.LOCAL.CHANNEL
    ⊟ $Channels.APP1.REMOTE
          APP1.REMOTE.CHANNEL
    ⊟ $Channels.APP2.LOCAL
          APP2.LOCAL.CHANNEL
    ⊟ $Channels.APP2.REMOTE
          APP2.REMOTE.CHANNEL
    ⊞ $Listeners
    ⊞ $Namelists
    ⊞ $Processes
    ⊟ $Queues.APP1.LOCAL
          APP1.LOCAL.QUEUE
    ⊟ $Queues.APP1.TEMP
          APP1.TEMP.QUEUE
    ⊟ $Queues.APP2.LOCAL
          APP2.LOCAL.QUEUE
    ⊟ $Queues.APP2.TEMP
          APP2.TEMP.QUEUE
    ⊞ $Services
```

Creating a new resource group

To create a new resource group, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Open the Defined View. The defined view tree is displayed on the left side of the Defined View.
3. Right-click the queue manager for which you want to create a new resource group and select **Create Resource Group**.

   Tip: You can also create a resource group within another resource group.
4. When prompted to provide a name, enter an alphanumeric name for the new resource group and click **OK**. The new resource group is added to the defined view tree.

   Remember:
   a. Do not use non-English characters for the new object name.
   b. SYSTEM should not be used as the prefix name that you assign to your own resource. WebSphere MQ Configuration agent identifies the resource whose prefix name is SYSTEM as the WebSphere MQ default resource and therefore skips the validation process.
   c. On z/OS systems with CCSID 1390, no WebSphere MQ objects support lowercase characters.

5. Select the new resource group in the defined view tree. The settings list for the object are displayed on the right side of the Defined View.
6. Complete the settings list as necessary.
7. Click **Save** to save your changes.

Creating resources in a resource group

You can use the menu options in the defined view to create and define new resources in an existing resource group. You can create the following resources:

- Alias queue
- Authentication Information object
- Client connection channel
- Cluster receiver channel
- Cluster sender channel
- Coupling facility (z/OS systems only)
- Listener
- Local queue
- Model queue
- Namelist
- Process
- Receiver channel
- Remote queue
- Requester channel
- Sender channel
- Server channel
- Server connection channel
- Service
- Storage class (z/OS systems only)

To create a new resource in a resource group:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Open the Defined View. The defined view tree is displayed on the left side of the Defined View.
3. Right-click the resource group to which you want to add the new resource, click **Create**, and then select the type of resource that you want to create.
4. When prompted to provide a name, enter an alphanumeric name for the new resource and click **OK**. The new resource is added to the defined view tree.

   Remember:

   a. Do not input non-English characters for the new object name.
   b. SYSTEM should not be used as the prefix name that you assign to your own resource. WebSphere MQ Configuration agent identifies the resource whose prefix name is SYSTEM as the WebSphere MQ default resource and therefore skips the validation process.

c. On z/OS systems with CCSID 1390, no WebSphere MQ objects support lowercase characters.

5. In the defined view tree, select the new resource. The settings list for the object is displayed on the right side of the Defined View.
6. Complete the settings list as necessary. Click **Help** to display information about each parameter.
7. Click **Save** to save your changes.

New resources that you create with this method are not based on a prototype, therefore you need to either specify all the required parameters or accept the default settings. To base an object on a prototype, see "Creating prototypes in the Prototype View" on page 32.

Copying objects

You can copy objects from one location to another in the same view. You can select one or more objects at a time to copy to a new location.

This information also applies to the Prototype View.

Guidelines for copying objects

Use these guidelines when copying objects within the same view:

- You can copy existing queue managers from one configured system group only to another configured system group.
- You can copy an existing resource group from one queue manager to another resource group in the same queue manager or a different queue manager, or to another queue manager.
- You can copy existing resources (queues, channels, and other objects) from one resource group to another resource group, or to another queue manager.
- If you copy an object that is based on a prototype, the new copy is based on the same prototype.

Copying an object to another location within the same view

Do the following steps to copy an object to another location within the same view:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined View or the Prototype View.
3. Select the object that you want to copy.
4. Press Ctrl and drag the object to the new location. Do not release the Ctrl key until the object is dropped to the new location.

   Important:

   a. You can copy existing queue managers from one configured system group only to another configured system group, or within the same group.
   b. You can copy an existing resource group from one queue manager only to another queue manager, or in the same queue manager, or to another resource group in the same queue manager or a different queue manager.

c. You can copy existing resources (queues, channels, and other objects) from one resource group to another resource group, or to another queue manager.
d. If you copy an object that is based on a prototype, the new copy is based on the same prototype.

Copying prototypes

When you are dragging one prototype object to another (for example, copying a local queue prototype to a resource group prototype), you can make a copy of the object that you are dragging or you can create a reference object in the target object, which then refers back to the object that you are dragging. The default is to copy the object.

To create a prototype reference object, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. In the Configuration view, ensure that Prototype copy semantics is set to **Create reference**.
3. Open the Prototype View and expand the prototype view tree as necessary, so that you can see both the object that you want to drag and the target object.
4. Select the object that you want to drag.
5. Drag the object to the target object.

A prototype reference object is created in the target object. This prototype reference object points back to the original prototype.

Creating multiple copies of a configuration object

You can use the Replicate option to create multiple copies of a configuration object without having to drag the object for each copy that you want to create. This option is available for copying all configuration objects, including prototypes.

To create multiple copies of a configuration object, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the defined or prototype view.
3. Select the object or objects that you want to replicate. Press Shift and click two objects if you want to select these two objects and all objects between them. Press Ctrl and click objects if you want to select multiple separate objects.
4. After you select the objects, right-click one of the selected objects and click **Replicate**. The Object Replication window opens as shown in Figure 37 on page 73:

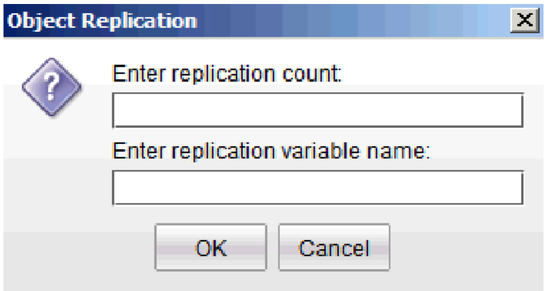


Figure 37. Using the Replication Option

5. Enter the number of copies of each object that you want to create in the **Enter replication count** field.
6. Optional: Enter the name of a symbolic variable that is already associated with the object being copied in the **Enter replication variable name** field. A unique number is assigned to this variable for each new instance of the object that is created. If you do not specify a symbolic variable name, a numerical suffix is appended to the name of each object that is created, to ensure that object names are unique.
7. Click **OK** to replicate the objects.

The newly created copies are added to the view.

Suppose that you have a resource named LOCAL.QUEUE.&NUM that has a symbolic variable NUM. The NUM symbolic variable has the value 0 defined in the **Based On** section of its settings list. The resolved name of the resource is LOCAL.QUEUE.0. If you select the **Replicate** option and enter the value `50` in the **Enter replication count** field to create 50 copies of the object, and you enter `NUM` in the **Enter replication variable name** field, 50 copies of the resource are created under the parent object.

The NUM variable of the first copy has the value 1, and so the resource is named LOCAL.QUEUE.1. Likewise, the second object is named LOCAL.QUEUE.2 because its NUM variable has the value 2. The NUM variables of other objects have values in the range 3 - 50. By default, variables are assigned values starting with the value 1. The exception to this is if the NUM variable of the object that is being copied is already assigned a value; in this case, numbering starts from that value plus one.

Chapter 5. Validating the configuration of your WebSphere MQ environment

You can ensure that the defined objects that you create using WebSphere MQ Configuration agent are valid before you add them to your WebSphere MQ environment.

Validating objects in the Defined View

Before you add defined objects to your actual WebSphere MQ environment, you can validate their definitions to ensure that they are defined correctly. For example, you can use WebSphere MQ Configuration agent to create a sender channel that references a transmit queue that does not yet exist in your WebSphere MQ configuration. WebSphere MQ Configuration agent notifies you if the validation test detects this error.

When you choose the validation feature, a group of default validation functions are performed on all objects. You can, however, control the amount of validation testing that you want to perform on specific objects.

WebSphere MQ Configuration agent provides two ways to control validation testing:

- Use the **Validation** settings of the object to enable or disable validation options. The validation options apply to individual objects only and cannot be inherited by subordinate objects.
- Use the **Resource Validation** settings of the queue manager to enable or disable validation options for the subordinate resources of a queue manager. All subordinate resources inherit the queue manager validation options by default.

Remember: Validation processes objects in the configuration database only; it does not process actual queue manager data that is in your WebSphere MQ environment.

Default validation options

By default, WebSphere MQ Configuration agent performs the following validation tests on all objects, unless you change the validation options:

- Queue manager validation
  - Ensures that no resources with the same name exist within a queue manager
  - Ensures that default resources are defined within the queue manager
  - Ensures that referenced dead-letter queues and default transmit queues are defined correctly
- Queue validation
  - Ensures that a sender or server channel exists on the same queue manager that references the queue when a local queue is defined as a transmit queue
  - Ensures that the remote queue manager referenced by the remote queue is defined within the same queue manager as a transmission queue when the XMITQ field is blank
  - Ensures that if triggering is enabled for a queue, the process and initiation queue exist within the queue manager

- Channel validation
  - Ensures that a sender or server channel references a transmit queue
  - Ensures that the transmit queue is properly defined within the queue manager
  - Ensures that there is a receiver or requester channel properly defined on the connected queue manager for each sender or server channel on the local queue manager

  Remember: When you create a new channel, if another channel with the same name already exists on the same queue manager, a suffix is automatically appended to the channel name to distinguish it from the existing channel. However, if the channel is part of a pair of sender/receiver channels, the channel name is different from the other channel in the pair and validation fails. In this case you must rename the channels so that their names are identical and there are no other channels with the same name on the same queue manager.
- Process validation
  - Ensures that defined processes are referenced by local queues within the queue manager
- Namelist validation (z/OS systems only)
  - Ensures that each name referenced within a namelist is defined as a queue within the queue manager

Validating objects in the Defined View

Do the following steps to validate objects in the Defined View before you use the Update function.

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined View.
3. Select the object or objects that you want to validate (press Shift and select two objects if you want to select these two objects and all objects between them. Press Ctrl and select objects if you want to select multiple separate objects) and right-click them.
4. Select **Validate** from the displayed menu.

If there are no validation errors, a message indicates that the validation request completed successfully. If there are validation errors, the Validate window lists the object name and type, its location in the defined view tree, and a description of the error found. When the objects contain no errors, you can use the objects to update your WebSphere MQ configuration. See "Updating your actual configuration from defined objects" on page 85 for information about how to update your WebSphere MQ configuration.

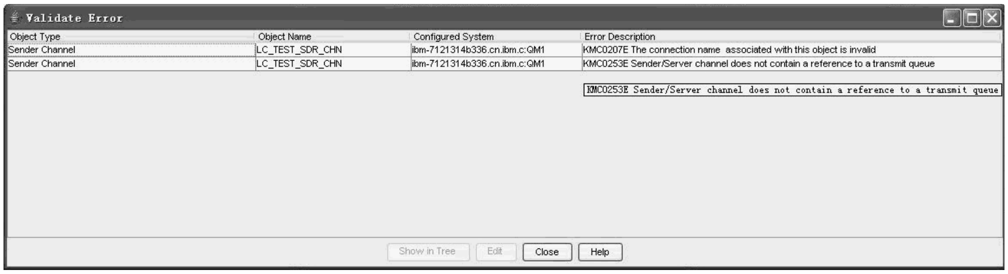
Example of validating objects

After creating and defining a new sender channel, you want to validate it to ensure that it is defined correctly before deploying it to your environment:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform the operations described in this example.

1. Ensure that you are in update mode (See “Entering update mode” on page 18 for information about how to enter update mode)
2. Right-click the channel in the defined view and click **Validate**.

The window shown in Figure 38 is displayed.



Validate Error

Object Type	Object Name	Configured System	Error Description
Sender Channel	LC_TEST_SDR_CHN	ibm-7121314b336.cn.ibm.c:QM1	KMC0207E The connection name associated with this object is invalid
Sender Channel	LC_TEST_SDR_CHN	ibm-7121314b336.cn.ibm.c:QM1	KMC0253E Sender/Server channel does not contain a reference to a transmit queue

KMC0253E Sender/Server channel does not contain a reference to a transmit queue

Figure 38. Validation errors

Validation has detected the following two errors:

- `KMC0207E The connection name associated with this object is invalid`
- `KMC0253E Sender/Server channel does not contain a reference to a transmit queue`

The first error occurs because the address of the receiver channel to which the new sender channel will connect is not specified in the **Connection Name** field. In this case you want to connect to a receiver channel running on the same host system, so you open the **Transport** section of the settings list of the channel and enter `127.0.0.1(1918)`, where 127.0.0.1 is the loopback address and 1918 is the port to connect on.

The second error occurs because the name of the transmission queue that is used by the channel is not specified. To fix this error, you open the **Transmit** section of the setting list of the channel and select the transmission queue that you want to use from the **Transmit queue name** list.

You now try validating the channel again. A message is displayed stating that validation completed and that no problems were found.

Controlling the rules of validation testing

You can change the validation rules for single objects or for the subordinate objects of a queue manager.

In the Validation section for a resource object, you can enable or disable validation options for individual objects. The options that you select apply to the individual object only and cannot be inherited by other objects.

In the Validation section for a queue manager, you can enable or disable validation options for queue manager subordinate objects. All subordinate objects inherit the validation options of the queue manager, unless you specifically change a resource setting.

You can also set validation options for prototype objects. Any object that you create from the prototype inherits its validation rules.

Setting validation rules for individual objects

You can enable or disable validation options for individual objects by doing the following steps:

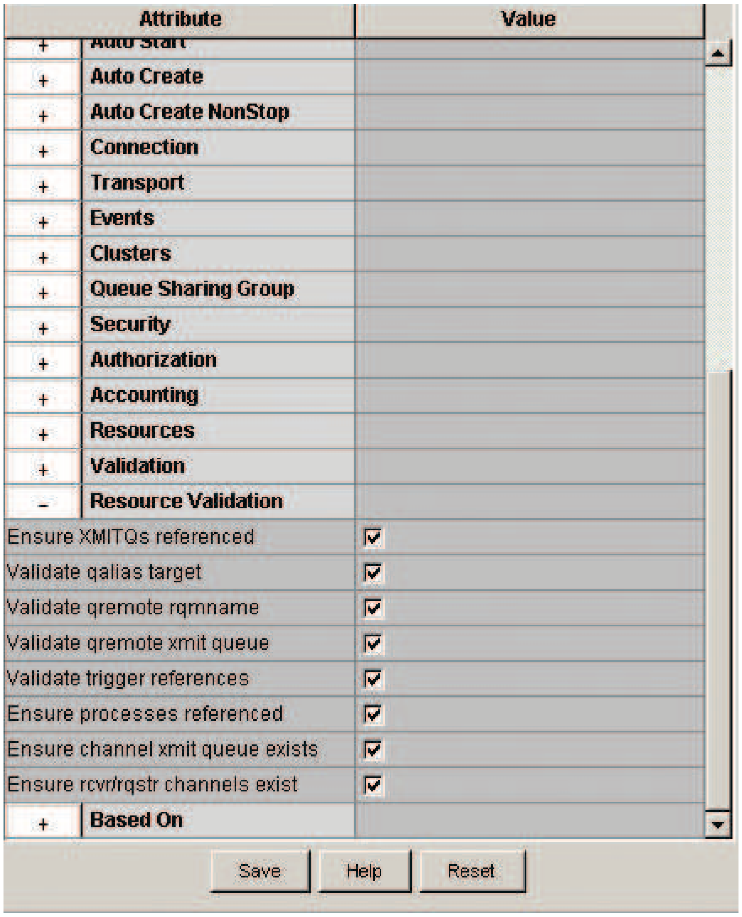
Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. In the Defined View select a resource object or in the Prototype View select a resource object prototype. The settings list for the object is displayed.
3. Expand the **Validation** section of the settings list.
4. To disable a particular validation option, select **Disabled** from the list of available options or clear the check box. To enable a particular validation option, select **Enabled** from the list of available options or select the check box.
5. Click **Save** to save your changes.

When you validate this object, WebSphere MQ Configuration agent performs only the validation options that are activated.

Setting validation rules for resources in a queue manager

You can use the **Resource Validation** section of a queue manager to enable or disable validation options for queue manager subordinate objects. Figure 39 on page 79 shows the **Resource Validation** section of a queue manager.



	Attribute	Value
+	Auto Start	
+	Auto Create	
+	Auto Create NonStop	
+	Connection	
+	Transport	
+	Events	
+	Clusters	
+	Queue Sharing Group	
+	Security	
+	Authorization	
+	Accounting	
+	Resources	
+	Validation	
-	Resource Validation	
Ensure XMITQs referenced		☑
Validate qalias target		☑
Validate qremote rqmname		☑
Validate qremote xmit queue		☑
Validate trigger references		☑
Ensure processes referenced		☑
Ensure channel xmit queue exists		☑
Ensure rcvr/rqstr channels exist		☑
+	Based On	

Figure 39. Setting validation rules for resources within a queue manager

To set validation rules for resources in a queue manager:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. In the Defined View select a queue manager or in the Prototype View select a prototype queue manager. The settings list for the object is displayed.
3. Expand the **Resource Validation** section. All options are selected by default.
4. To disable an option, click the option to clear the check box.
5. Click **Save** to save your changes.

If you want to be sure that a resource inherits the validation rules of the queue manager, make sure that the **Inherit** option is selected in the **Validation** section of the settings list of the resource.

Configuring validation to ignore resources with a particular prefix

You can also use the **Validation** section of a queue manager (or a prototype queue manager) to specify that validation is not performed on objects that have a name that begins with a particular prefix. By default, validation ignores all objects that use the prefix SYSTEM., which represents the objects that are provided by IBM. You can delete the default option and enter a prefix that you prefer, or enter several prefixes that are separated by commas.

Do the following steps to configure validation to ignore resources with a particular prefix:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. In the Defined View select a queue manager or in the Prototype View select a prototype queue manager. The settings list for the object is displayed.
3. Expand the **Validation** section.
4. In the **Don't check resources prefixed with** field, enter the prefix names that you want to exclude from validation. You can enter multiple prefixes, separated by commas.
5. Click **Save** to save your changes.

When you use the validation feature, objects that have the selected prefixes are ignored.

Chapter 6. Maintaining the configuration of your WebSphere MQ environment

When you use the discovery feature, you add a matching set of WebSphere MQ objects to the configuration database and to the defined view tree. You now have corresponding objects in two separate places: one set in the configuration database and one set in your actual WebSphere MQ configuration. When you create new objects or modify existing objects in either location, the changes are *not* automatically added to the corresponding objects.

WebSphere MQ Configuration agent provides the following options to help you keep corresponding objects synchronized:

- The **View discrepancies** option checks for differences between the defined configuration objects and the corresponding objects in your WebSphere MQ configuration after the last update.
- The **Update** > **Defined from actual** option changes the defined resource to match the actual resource.
- The **Update** > **Actual from defined** option changes the actual resource to match the defined version.
- The **Discover new resources** option for queue managers searches the queue manager and adds newly discovered resources to the configuration database and to the defined view tree. Any newly discovered permanent dynamic queues are saved in a $DynamicResources resource group; all other newly discovered resources are saved in $Default_Group resource group. Permanent dynamic queue definitions are not created in the configuration database unless you enabled the **Configure permanent dynamic queues** option in the Auto Start section of the queue manager settings list.

Viewing discrepancies

Use the **View discrepancies** menu option to evaluate the difference between the defined and actual resource definitions for an object and to display any conflicts. If you select this option for an object that contains other objects, the action is also applied to the contained objects. If there are differences between the objects, you can make the appropriate changes before you use one of the update options.

To view discrepancies between the defined and actual resource definitions for an object:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Open the Defined View.
2. In the Defined View, right-click the object that you want to compare to its corresponding object in your WebSphere MQ configuration and select **View** > **discrepancies**

WebSphere MQ Configuration agent checks the defined object against the corresponding object in your WebSphere MQ configuration. If no discrepancies are detected, a message is displayed stating that no discrepancies have been found. If discrepancies are found, the Discrepancy Display window lists them. Use this window to locate resource definitions that do not meet system requirements or conventions before updating your actual configuration from your defined configuration. You can resolve discrepancies for individual objects or for an object and its subordinates.

Guidelines for viewing discrepancies

Use these guidelines when viewing discrepancies:

- When you use the **View discrepancies** option at the resource group level, you cannot use the option to add or delete resource definitions for objects at that level. The **Update defined from actual** operation, when used at the resource group level, only updates resources that already exist in the selected resource group.
- When you use the **View discrepancies** option on a resource group, the difference between the defined and actual resource definitions only for the existing objects are evaluated.
- To add or delete resource definitions for objects that are in your defined configuration or your actual configuration, use the **View discrepancies** option at the configured system level.

Resolving discrepancies

The Discrepancy Display window lists the discrepancies that are found between resource definitions that are defined in your configuration database and the corresponding resource definitions in your actual configuration. Discrepancies found is an error condition.

If you are authorized to do so, you can use the Discrepancy Display window to resolve these discrepancies.

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

You must be in update mode to perform an Update operation from this window.

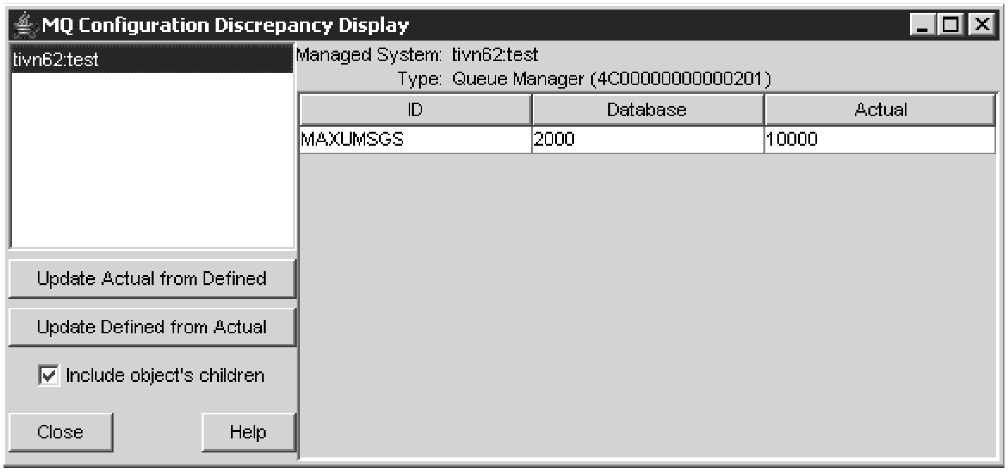
When you are in update mode, the window displays buttons and check boxes that list the actions you can take to resolve the discrepancy, either in favor of the configuration database or in favor of the actual WebSphere MQ configuration.

Certain attributes of WebSphere MQ objects must be defined. If such attributes have no value in the defined view, when you perform the **Update** > **Actual from defined** operation, instead of being cleared completely in your actual environment, attributes of the actual object are reset to WebSphere MQ default values. The object in the defined view is unchanged, and so even after the operation is complete, the actual and defined object are still different. If the default values that are assigned by WebSphere MQ to the actual object are correct, you can perform the **Update** > **Defined from actual** operation to update these values in the defined object, making the attributes of the two objects the same.

Example of resolving discrepancies

Assume that you have a queue manager deployed in your environment with a maximum uncommitted messages value of 10 000 messages. However, in the defined view, the queue manager has a maximum uncommitted messages value of 2000. If you right-click the queue manager in the defined view and select **View** >

Discrepancies, a list of differences between the queue manager in the defined view and the queue manager in your actual environment is displayed, as shown in Figure 40.


MQ Configuration Discrepancy Display
tivn62:test
Update Actual from Defined
Update Defined from Actual
Close
Help

Managed System: tivn62:test
Type: Queue Manager (4C00000000000201)

ID	Database	Actual
MAXUMSGS	2000	10000

☑ Include object's children

Figure 40. Discrepancies between objects in the defined view and the actual WebSphere MQ environment

You must now decide whether the maximum uncommitted messages value used by the deployed queue manager or the value specified in the defined view is correct.

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform the operations described in this example.

In this case, you want to use the value of 2000 that is specified in the defined view.

Click **Update** > **Actual from Defined** to set the value in the deployed queue manager to 2000, the value that is specified in the queue manager settings list in the defined view.

If you want to use the value that is specified in the actual queue manager, you click **Update** > **Defined from Actual** to copy the value from the actual queue manager to the queue manager definition in the defined view.

A message is displayed stating that the update is completed. You now close this message and the window listing discrepancies. If you right-click the queue manager and select **View** > **Discrepancies** again, a message is displayed stating that no discrepancies exist.

Updating the configuration database from your actual WebSphere MQ configuration

Use the **Update** > **Defined from actual** menu option to update your defined configuration to match your actual configuration.

This option changes the defined resource to match the actual definition. If any differences exist, the defined resource is changed to match the actual version. When you use this option at the configured system level, if an actual resource exists that has no defined counterpart, a new defined resource is created; if a defined resource exists that has no actual counterpart, the defined resource is deleted.

You can use this operation on a configured system group, queue manager, resource group, or resource.

This operation affects only the objects that you select. For example, if you make changes to a queue manager in your WebSphere MQ environment whose corresponding object is already part of the configuration database, WebSphere MQ Configuration agent updates the selected object in the configuration database and in the display. Now, the object in the Defined View and its corresponding object in the WebSphere MQ configuration are identical.

Guidelines for updating the configuration database

Use these guidelines when updating the configuration database:

- Use the **View discrepancies** option before you use the **Update** > **Defined from actual** option to ensure that you know what changes WebSphere MQ Configuration agent will implement.
- If you changed any object that is currently in the defined configuration, the **Update** > **Defined from actual** option overwrites the current parameters of the object that is defined in the configuration database.
- When you use the **Update** > **Defined from actual** option at the resource group level, only resources that already exist in that group are updated. If you want to add new resources that are found in the actual WebSphere MQ configuration, perform the **Discover new resources** option at the configured system group level.

Adding objects and changes to the configuration database

To add actual WebSphere MQ objects and changes to the configuration database and the Defined View, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Open the Defined View.
3. Select the object or objects that you want to update (Press Shift and select two objects if you want to select these two objects and all objects between them. Press Ctrl and select objects if you want to select multiple separate objects), and then right-click them.
4. Click **Update** > **Defined from actual**. You are prompted to confirm the update.
5. Click **Yes** to confirm the update. Any new WebSphere MQ objects or changes to corresponding objects are added to the configuration database.

   Tip: If you add a WebSphere MQ queue manager that has resources attached, you must first create a resource group in the defined configuration to hold the resources. If you do not create this resource group, one $Default_Group resource group is created.

If the update is successful, the WebSphere MQ objects and changes to these objects are added to the configuration database and the Defined View, and an update successful message is displayed. If there are problems, an error message is displayed. Correct the problems, then use the **Update defined from actual** option again.

Backing up queue managers in your WebSphere MQ environment

You should make a backup copy of the original queue manager definition in your actual WebSphere MQ environment before you make any changes to it with the **Update actual from defined** option.

To back up queue managers in your actual WebSphere MQ environment:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined View. The defined view tree is displayed on the left side of the Defined View.
3. Right-click **Defined View** (the root-level item) and select **Create Configured System Group**. You are prompted to supply a name for the new object.
4. Enter a name (for example, Backup) for the new configured system group and click **OK**. The new backup configured system group is added to the defined view tree.
5. Copy the queue managers that you want to back up from the configured system group in which they are defined to the new configured system group.
6. Rename each of the backup queue managers. For example, you might add the suffix _bak to the name of each queue manager.
7. Right-click the backup configured system group and click **Update** > **Defined from actual**.

You now backed up the configuration for one or more queue managers in your existing configuration by storing in the backup configured system group the definitions of the queue managers. If you ever need to restore the original configuration for a queue manager from the backup that you created using this procedure, right-click the name of the duplicate queue manager in the backup configured system group and select **Update** > **Actual from defined**.

Updating your actual configuration from defined objects

The **Update** > **Actual from defined** option changes the actual WebSphere MQ resource to match the defined version in the configuration database and the Defined View. If any differences exist, the actual resource is changed to match the defined version. If an actual resource exists that has no defined counterpart, the actual resource is deleted; if a defined resource exists that has no actual counterpart, the actual resource is created.

You can use the **Update** > **Actual from defined** option to add new objects to your WebSphere MQ configuration or to update corresponding objects in your WebSphere MQ configuration.

The **Update** > **Actual from defined** option automatically runs validation tests on defined objects; it does not add objects or changes to objects that are not defined correctly to your WebSphere MQ configuration.

Objects that you copy from the configuration database to your actual WebSphere MQ configuration perform as if they were originally created in the WebSphere MQ environment.

Tip: If you delete a resource of a queue manager that is in your Defined View, and then you use the **Update** > **Actual from defined** option on the queue manager, the resource is deleted from the queue manager in your actual WebSphere MQ configuration.

Updating objects in your actual WebSphere MQ configuration

Use the **View Discrepancies** option before you use the **Update** > **Actual from defined** option to ensure that you know what changes WebSphere MQ Configuration agent will implement to your actual WebSphere MQ configuration. You can make a backup copy of the actual queue managers before you make any changes to them. See "Backing up queue managers in your WebSphere MQ environment" on page 85.

To update objects in your actual WebSphere MQ configuration:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Open the Defined View.
3. Select the object or objects that you want to update in your WebSphere MQ environment (Press Shift and select two objects if you want to select these two objects and all objects between them. Press Ctrl and select objects if you want to select multiple separate objects.) and then right-click them.
4. Click **Update** > **Actual from defined**. You are prompted to confirm the update.
5. Click **Yes** to confirm the update. If the update is successful, the corresponding objects in your WebSphere MQ environment are changed and an `update successful` message is displayed. If there are problems, an error message is displayed.
6. If there are problems, correct them, then use the **Update** > **Actual from defined** option again.

Working with queue-sharing groups (z/OS systems only)

In an existing queue-sharing group environment on z/OS systems, you can use WebSphere MQ Configuration agent to define the following resource objects:

- Authentication Information
- Channels (all types)
- Namelist
- Process
- Queues (all types)
- Storage Class

You can also update a queue manager that already belongs to a queue-sharing group, or convert an existing WebSphere MQ for z/OS queue manager to be part of an existing queue-sharing group.

Remember: Queue sharing groups are only available on z/OS systems.

Before you can use WebSphere MQ Configuration agent to work with queue-sharing groups, you need to ensure the following items:

- Your queue-sharing group environment must already exist.

  WebSphere MQ Configuration agent cannot create or start queue managers on z/OS systems, but it can perform all the other configuration functions that it provides for distributed systems.
- Your queue-sharing group environment must be defined in WebSphere MQ Configuration agent.

  You must have used WebSphere MQ Configuration agent to discover the queue managers in your queue-sharing group. The queue managers are visible in the Defined View and your defined configuration matches your actual WebSphere MQ configuration.

Defining a new resource in a queue-sharing group environment

To add a new resource in a queue-sharing group environment, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. In the defined view tree, right-click a queue manager that belongs to the queue-sharing group, click **Create**, and select the type of the resource that you want to create.
3. Define your new resource and specify GROUP as the disposition.
4. Enter the parameters as required, and save the definition.
5. Right-click the resource that you just defined and click **Validate**.
6. Right-click the resource that you just defined and click **Update** > **Actual from defined**.

WebSphere MQ Configuration agent issues the necessary WebSphere MQ commands to define the resource on every queue manager in your queue-sharing group.

Example of adding a new local queue to a queue-sharing group

Assume that you have three queue managers, QMG1, QMG2, and QMG3, defined in your queue-sharing group and these queue managers are displayed in the Defined View.

To add a new local queue to be used by all queue managers in this queue-sharing group, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform the operations described in this example.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.

2. In the defined view tree, right-click the QMG1 queue manager (any queue manager in the group would do, you select QMG1 for this example) and click **Create** > **Queue:Local**.
3. Define your new local queue, name it *mynewqueue*, with the disposition of GROUP.
4. Enter all parameters as required, and save the definition.
5. Right-click the local queue, and select **Validate**.
6. Right-click the local queue, and select **Update** > **Actual from defined**.

   WebSphere MQ Configuration agent creates the following objects on QMG1, QMG2, and QMG3 in the Defined View:

   - A local queue object named `mynewqueue` with the disposition COPY

     This is the local copy that belongs to each queue manager.
   - A local queue object named `mynewqueue` with the disposition GROUP

     This is the actual definition of the local queue object that has the disposition group that is maintained in the shared DB2® repository.

If present in the Defined View, the background color of a resource object icon indicates its queue-sharing group information as follows:

Blue The object is a group resource.

Turquoise
The object is a copy.

Green (local and model queues only) The local queue or model queue is shared.

Updating a queue manager in a queue-sharing group environment

To update a queue manager in a queue-sharing group:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
2. Select the queue manager that you want to update in the defined view tree, and complete the queue-sharing group section of its settings list as required.
3. Click **Save** to save your changes to the queue manager definition.
4. Right-click the queue manager that you just updated and click **Validate**.
5. Right-click the queue manager that you just updated and click **Update** > **Actual from defined**.

Exporting and importing WebSphere MQ resources

You can export data from and import data to the configuration database in XML (Extensible Markup Language) format.

This feature is useful for the following purposes:

- Batch reporting (using an independent software-vendor report generator)
- Offline data manipulation

WebSphere MQ Configuration agent provides three different options for exporting data from the configuration database:

- **Partial Export**: Use this option to export resources and their attributes that exist in your actual WebSphere MQ environment from the configuration database of WebSphere MQ Configuration agent. Both defined view and prototype view objects can be exported.
- **Extended Export**: Use this option to export resources and their attributes from the configuration database of WebSphere MQ Configuration agent, regardless of whether they exist in your actual WebSphere MQ environment. Both defined view and prototype view objects can be exported.
- **Export All**: Use this option to export the entire configuration database of WebSphere MQ Configuration agent. The exported data can be useful in analyzing your configuration database, but it cannot be imported back into a database.

If invalid, unknown, or out-of-sequence data is found in an imported XML file, the import process is stopped. The point at which the error was found is identified by an error message.

Exporting data using the partial export option

Use the partial export option to export a single resource or group of resources. Exported resources can be either defined or prototype resources.

Only WebSphere MQ resources and attributes that are supported by WebSphere MQ are included in the exported data. Resources, such as configured system groups, and attributes, such as the host system name, that exist only in the defined view and have no correspondent in the actual WebSphere MQ environment, are not exported.

Resources that are based on prototypes are effectively disinherited in the exported XML file and global variables are resolved to their values.

Do the following steps to export a resource using the partial export option:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Right-click the resource that you want to export in the defined or prototype view and select **Export** > **Partial**.

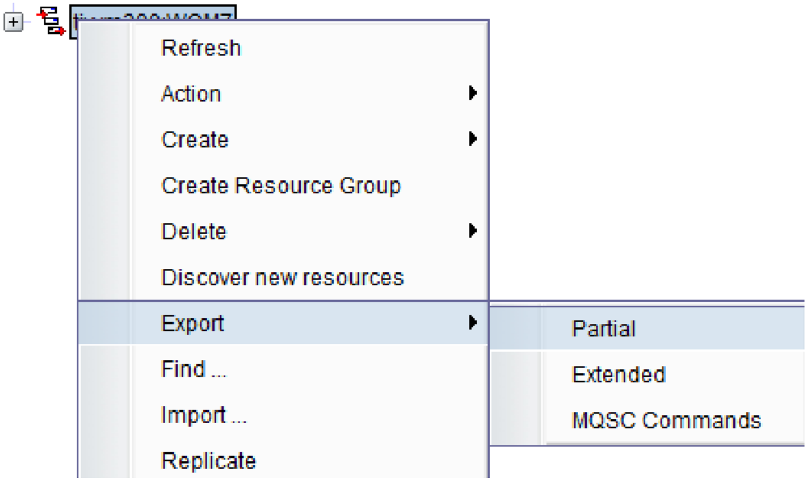


Figure 41. Using the Partial export option

2. In the **Save** window, enter the name of the XML file in which to store the exported XML data and click **OK**. A message is displayed reminding you that if you want to be able to import a previously exported resource, you must not delete its prototype.
3. Click **OK** to continue. A message is displayed indicating that the XML file is exported.
4. Click **OK** to close it.

An XML file that contains information about all the resources that you selected is created. Other resources contained within selected resources are also exported. For example, if you selected a queue manager, all the objects that it contains, such as queues and channels, are also exported.

Exporting data using the extended export option

Use the extended export option to export a single resource or group of resources. Exported resources can be either defined or prototype resources.

The extended export option differs from the partial export option in that the XML file generated contains all resources and attributes, including ones that exist only in the configuration database of WebSphere MQ Configuration agent. For example, resource groups, which are used to organize resources in the defined view and do not have a counterpart in the actual WebSphere MQ environment, are exported when the extended export option is used. In contrast, an XML file created using the partial export option only contains attributes of WebSphere MQ resources that exist in the real WebSphere MQ environment, so resources such as resource groups are not exported in partial export.

Do the following steps to export a resource using the extended export option:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Do one of the following steps:
   - Right-click the resource that you want to export in the Defined View and click **Export** > **Extended**.

- Right-click the resource that you want to export in the Prototype View and click **Export** > **Extended**.

2. In the **Save** window, enter the name of the XML file in which to store the exported XML data and click **OK**. A message is displayed reminding you that if you want to be able to import a previously exported resource, you must not delete its prototype.
3. Click **OK** to close it and to continue. A message is displayed indicating that the XML file is exported.
4. Click **OK** to close it.

An XML file that contains information about all the resources that you selected is created. Other resources contained within selected resources are also exported. For example, if you selected a queue manager, all the objects that it contains, such as queues and channels, are also exported.

Exporting data using the export all option

Use the export all option to export the entire configuration database, including global variables, defined resources, and prototype resources, to a single XML file. This file can be viewed using standard XML utilities to examine the properties of resources and their attributes. However, because the file contains mixed resource types, it cannot be imported into the configuration database of WebSphere MQ Configuration agent. To back up the entire database, click **Backup Configuration Database** in the Configuration View.

The export all option is available from the top-level icon in the defined or prototype view tree. No matter which of these nodes you select, the resulting XML file is the same.

Do the following steps to export your entire configuration database to an XML file:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. In the Defined View, right-click the Defined View node (or right-click the Prototype View node in the Prototype View).

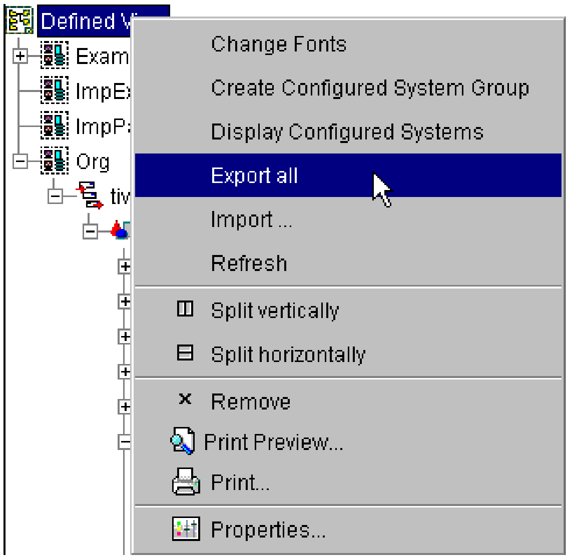


Figure 42. Using the Export All option

2. In the Save window, enter the name of the XML file where you want to store the exported XML data.
3. A message is displayed indicating that the XML file is exported. Click **OK** to close it.

An XML file is created that contains information about the entire configuration database.

Importing resources

You can import XML data that was previously exported using the partial export or extended export option. The resources that are imported depend on which method was used to export the data. If data was exported using the partial export option, objects and attributes that existed in your configuration database but are not supported by WebSphere MQ, such as resource group information, were not exported, and so are not displayed after importing the data. If data was exported using the extended export option, all objects from the configuration database are imported. For example, you might have a queue manager with objects organized into several resource groups in the defined view. If you used the partial export option when exporting the data, when you import it, these resource groups are not created. All objects that were inside the resource groups are placed directly under the queue manager.

Do the following steps to import resources that are defined in an XML file:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Select a resource under which you want the resources that are defined in the XML file to be imported into the defined view. You must select a resource that can contain the type of resource that you want to import. For example, if you want to import a queue manager, you must select a configured system group. If you want to import a queue, channel, or other queue manager resource, you must select a queue manager or resource group. If you are importing a

prototype, you must import it to the appropriate category of prototypes in the prototype view. For example, if you are importing a queue prototype, you must import it to Resource Prototypes group.

2. Right-click the resource and then click **Import**.

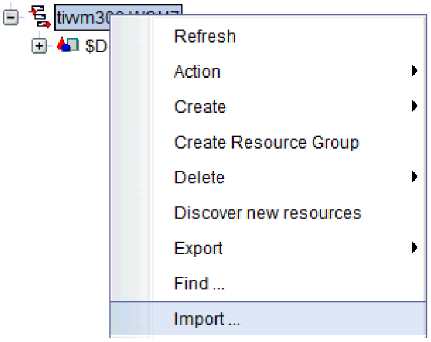


Figure 43. Importing a resource to the configuration database

Remember: When you import a new managed cluster, make sure the name of the cluster is unique. if another managed cluster with the same name already exists under a different configured system group, the two clusters might have different status records, none of which reflects the real situation of the cluster queue managers.

3. Select the file that contains the XML data that you want to import, and click **Open**.
4. A message is displayed reminding you that if you want to be able to import a previously exported resource, you must not delete its prototype. Click **OK** to close it.

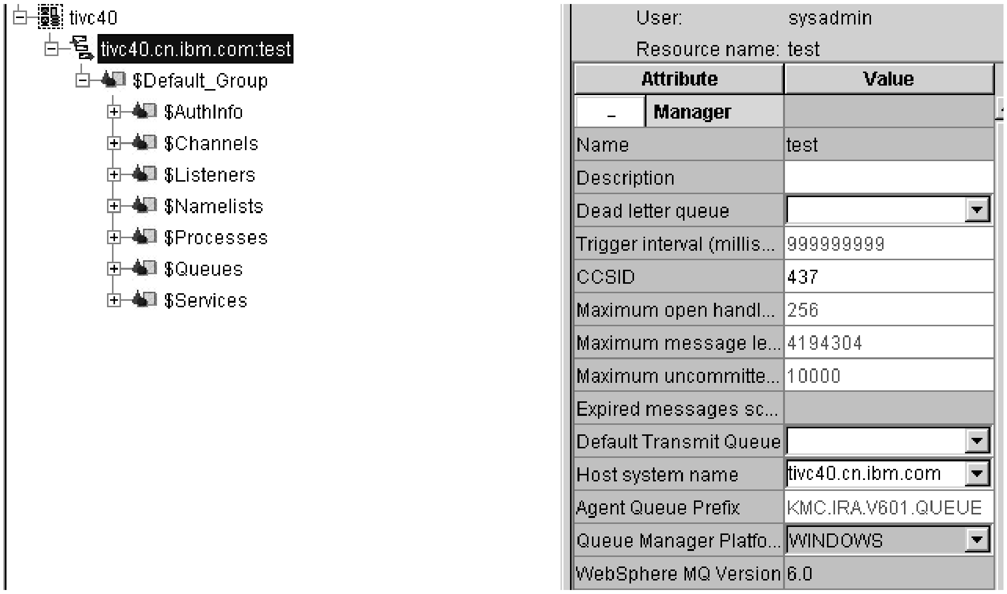
The resources in the imported XML file are placed under the selected resource in the defined view tree.

Restriction:

1. An XML file that is created by performing the export extended operation on configured system prototypes, resource group prototypes, or resource prototypes cannot be imported into a configuration database.
2. An XML file that is created using the export all option cannot be imported into a configuration database.
3. To enhance the portability of XML data exported from WebSphere MQ Configuration agent, after importing data from an XML file, the MQ version attribute is always set to UNKNOWN.

Example of importing a queue manager

Assume that you have a queue manager with seven resource groups containing different types of objects, as shown in figure Figure 44 on page 94.



User: sysadmin

Resource name: test

Attribute	Value
– Manager	
Name	test
Description	
Dead letter queue	
Trigger interval (millis...	999999999
CCSID	437
Maximum open handl...	256
Maximum message le...	4194304
Maximum uncommitte...	10000
Expired messages sc...	
Default Transmit Queue	
Host system name	tivc40.cn.ibm.com
Agent Queue Prefix	KMC.IRA.V601.QUEUE
Queue Manager Platfo...	WINDOWS
WebSphere MQ Version	6.0

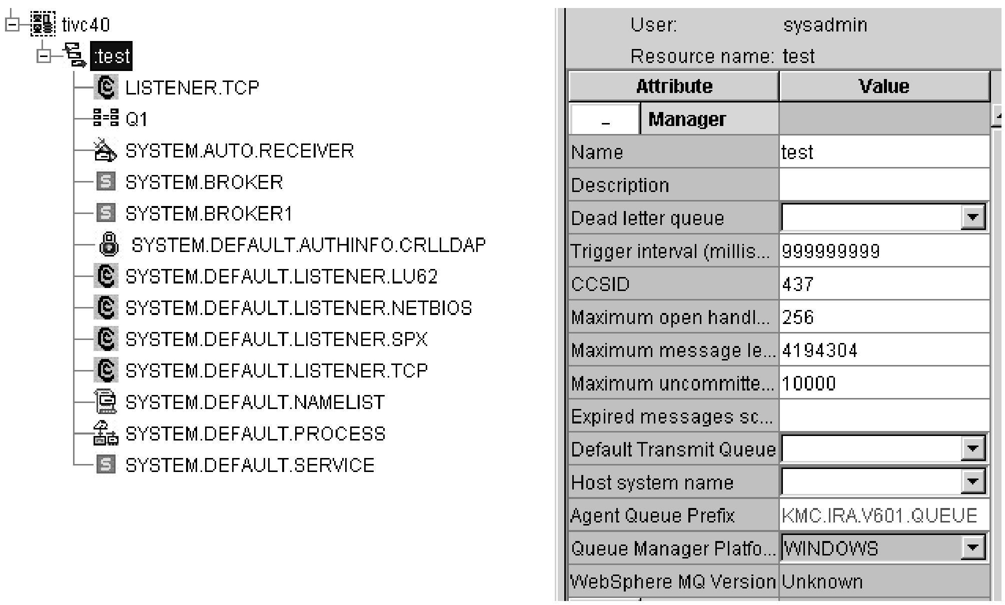
Figure 44. Queue manager with resource groups and host system name variable before performing partial export

The queue manager has various defined attributes, including host system name, which is an attribute supported by the WebSphere MQ Configuration agent but not by WebSphere MQ itself. You export this queue manager using the partial export option, which only exports WebSphere MQ resources and attributes that are supported by the actual WebSphere MQ environment. You then import the queue manager into the configuration database used by another WebSphere MQ environment, performing the following procedure:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform the operations described in this example.

1. Right-click the configured system group where you want to import the queue manager and click **Import**.
2. In the open file window select the file that contains the XML data that you want to import, and click **Open**.
3. A message is displayed reminding you that if you want to be able to import a previously exported resource, you must not delete its prototype. Click **OK** to close this message. The object queue manager is imported from the file.

The imported queue manager is different from the original queue manager because you exported the original queue manager using the partial export option. The result is that resources are no longer organized by resource groups, and attributes such as the host system name do not contain any data, because the partial export option does not export that information. The imported queue manager is shown in figure Figure 45 on page 95.



- tivc40
  - :test
    - LISTENER.TCP
    - Q1
    - SYSTEM.AUTO.RECEIVER
    - SYSTEM.BROKER
    - SYSTEM.BROKER1
    - SYSTEM.DEFAULT.AUTHINFO.CRLLDAP
    - SYSTEM.DEFAULT.LISTENER.LU62
    - SYSTEM.DEFAULT.LISTENER.NETBIOS
    - SYSTEM.DEFAULT.LISTENER.SPX
    - SYSTEM.DEFAULT.LISTENER.TCP
    - SYSTEM.DEFAULT.NAMELIST
    - SYSTEM.DEFAULT.PROCESS
    - SYSTEM.DEFAULT.SERVICE

User: sysadmin
Resource name: test

Attribute	Value
– **Manager**	
Name	test
Description	
Dead letter queue	
Trigger interval (millis...	999999999
CCSID	437
Maximum open handl...	256
Maximum message le...	4194304
Maximum uncommitte...	10000
Expired messages sc...	
Default Transmit Queue	
Host system name	
Agent Queue Prefix	KMC.IRA.V601.QUEUE
Queue Manager Platfo...	WINDOWS
WebSphere MQ Version	Unknown

Figure 45. Imported queue manager without resource groups or host system name variable

If you want to export information about resources and attributes that are not supported by the partial export option, use the extended export option, which supports exporting all resources and attributes.

Tip: If you export a configured system group using the partial export option, its contents (the queue managers and other resources that are under the configured system group) are exported, but the configured system group is not because it is an organization unit and is not supported by WebSphere MQ. When you import the contents of the group, they must be imported into another configured system group.

Example of exporting and importing a queue based on a prototype

You have a queue named q1 that is based on a queue prototype named pt1. You want to export both the queue and its prototype and import them to another WebSphere MQ environment (you cannot import the queue without its prototype). The order in which resources that are based on prototypes are exported is not important, but if they are imported in the wrong order, they do not work correctly. Before importing any resources based on a prototype, you must first import its prototype.

Do the following steps to export the q1 queue and then import it to a queue manager or a resource group:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform the operations described in this example.

1. Export q1 and pt1 separately to different files. The order in which the resources are exported is not important.

   Important: Do not export multiple prototypes to the same file.
2. In the environment to which you want to import the resources, right-click **Resource Prototypes** and click **Import**.

3. In the open file window select the file that contains the XML data for the pt1 prototype and click **Open**.
4. A message is displayed reminding you that if you want to be able to import a previously exported resource, you must not delete its prototype. Click **OK** to close this message.
5. Right-click the queue manager or resource group where you want to import the queue and click **Import**.
6. In the open file window select the file that contains the XML data for q1 and click **Open**.
7. A message is displayed reminding you that if you want to be able to import a previously exported resource, you must not delete its prototype. Click **OK** to close this message.

If the prototype of your queue is based on another prototype, before importing the queue prototype, you must first import the prototype on which it is based. For example, if you have the q2 queue based on the pt1 queue prototype, and pt1 is based on another prototype pt2, you must first import pt2, then pt1 and finally q2.

Important:

1. A queue manager might contain objects that are based on prototypes. If you are importing a queue manager, you must first ensure that all the prototypes that are used by the resources of the queue manager have been imported.
2. When importing resources based on prototypes, ensure that the environment to which the resource is imported does not already contain any prototypes with the same names as those used by the imported resource. If prototypes with the same names but different properties exist, the properties of the object are incorrect.

Example of exporting and importing resources

The following example is intended to display the difference between importing resources from an exported XML file using the partial export option and one using the extended export option.

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform the operations described in this example.

Step 1: creating a queue manager in the defined view

Do the following procedure to export a queue manager using the partial export option:

1. Click the Defined and Prototype node in the Configuration View to open the Defined and Prototype View.
2. Drag the Standard.Queue.Manager node under Configured System Prototypes in the Prototype View to the Example.Queue.Managers node in the Defined View to create a new queue manager.
3. Click the new queue manager in the Defined View. Its setting list is opened on the right side of the window.
4. Change the queue manager name to QM1 and click **Save** to save your changes.

A queue manager named QM1 is created in the Defined View.

Related reference:

"Step 2: exporting a queue manager using the partial export option" on page 97

Step 2: exporting a queue manager using the partial export option

Do the following procedure to export the queue manager using the partial export option:

1. Right-click the QM1 queue manager in the Defined View, and click **Export** > **Partial**.
2. In the Save File window, enter the file name `export_partial.xml`.
3. A message is displayed reminding you that if you want to be able to import a previously exported resource, you must not delete its prototype. Click **OK** to close this message.
4. A message is displayed indicating that the XML file is exported. Click **OK** to close it.

The partial export operation is complete, and the `export_partial.xml` file is created.

Related reference:

"Step 3: exporting a queue manager using the extended export option"

"Step 1: creating a queue manager in the defined view" on page 96

Step 3: exporting a queue manager using the extended export option

Use the following procedure to export a queue manager using the extended export option:

1. Right-click the QM1 queue manager in the Defined View, and select **Export** > **Extended**.
2. In the Save File window, enter the file name `export_extended.xml`.
3. A message is displayed reminding you that if you want to be able to import a previously exported resource, you must not delete its prototype. Click **OK** to close this message.
4. A message is displayed indicating that the XML file has been exported. Click **OK** to close it.

The extended export operation is completed, and the `export_extended.xml` file is created.

Related reference:

"Step 4: importing the export_partial.xml file"

"Step 2: exporting a queue manager using the partial export option"

Step 4: importing the export_partial.xml file

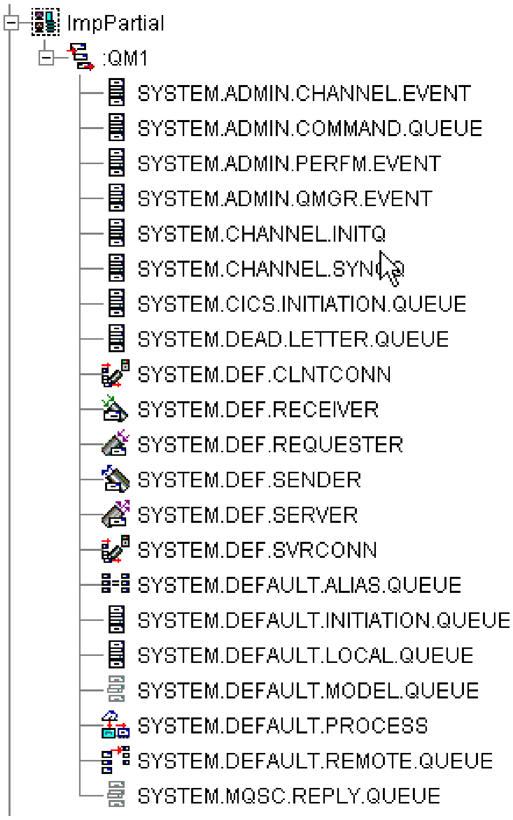
Use the following procedure to import the `export_partial.xml` file to the configuration database:

1. Right-click the **Defined View** node in the Defined View tree, and select **Create Configured System Group**.
2. Enter `ImpPartial` in the **New Resource Name** window and click **OK**.

   A configured system group named ImpPartial is created in the Defined View.
3. Right-click the configured system group named ImpPartial in the Defined View, and click **Import**.
4. Select `export_partial.xml` in the Open window and click **Open**.

5. A message is displayed reminding you that if you want to be able to import a previously exported resource, you must not delete its prototype. Click **OK** to close this message.

Resources saved in the `export_partial.xml` file are imported, and a queue manager named QM1 is created under the ImpPartial configured system group.



ImpPartial
:QM1
SYSTEM.ADMIN.CHANNEL.EVENT
SYSTEM.ADMIN.COMMAND.QUEUE
SYSTEM.ADMIN.PERFM.EVENT
SYSTEM.ADMIN.QMGR.EVENT
SYSTEM.CHANNEL.INITQ
SYSTEM.CHANNEL.SYNCQ
SYSTEM.CICS.INITIATION.QUEUE
SYSTEM.DEAD.LETTER.QUEUE
SYSTEM.DEF.CLNTCONN
SYSTEM.DEF.RECEIVER
SYSTEM.DEF.REQUESTER
SYSTEM.DEF.SENDER
SYSTEM.DEF.SERVER
SYSTEM.DEF.SVRCONN
SYSTEM.DEFAULT.ALIAS.QUEUE
SYSTEM.DEFAULT.INITIATION.QUEUE
SYSTEM.DEFAULT.LOCAL.QUEUE
SYSTEM.DEFAULT.MODEL.QUEUE
SYSTEM.DEFAULT.PROCESS
SYSTEM.DEFAULT.REMOTE.QUEUE
SYSTEM.MQSC.REPLY.QUEUE

Figure 46. QM1 queue manager created by importing the export_partial.xml file

Related reference:

"Step 5: importing the export_extended.xml file"

"Step 3: exporting a queue manager using the extended export option" on page 97

Step 5: importing the export_extended.xml file

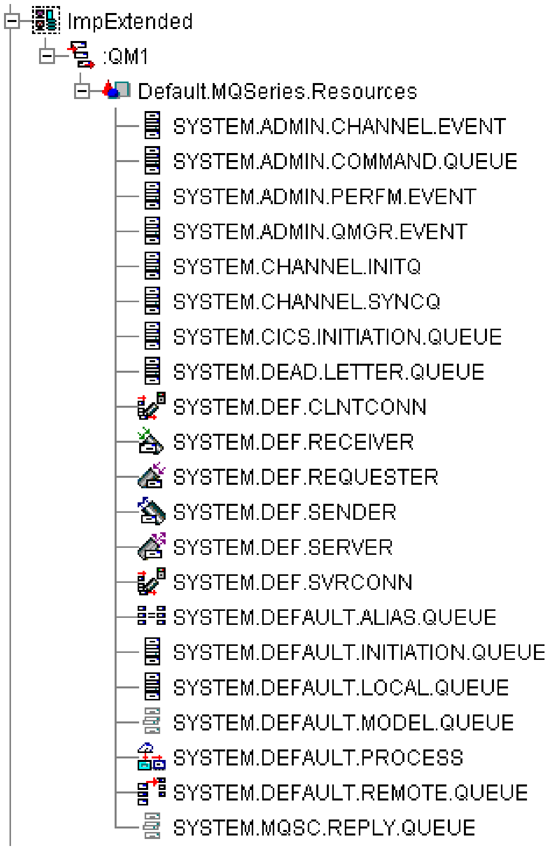
Use the following procedure to import the `export_extended.xml` file to a configuration database:

1. Right-click the **Defined View** node in the Defined View tree, and select **Create Configured System Group**.
2. Enter `ImpExtended` in the **New Resource** window and click **OK**.

   A configured system group named ImpExtended is created in the Defined View.
3. Right-click the configured system group named ImpExtended in the Defined View and click **Import**.
4. Select `export_extended.xml` in the Open window and click **Open**.

5. A message is displayed reminding you that if you want to be able to import a previously exported resource, you must not delete its prototype. Click **OK** to close this message.

Resources saved in the `export_extended.xml` file are imported, and a queue manager named QM1 is created under the ImpExtended configured system group.



```
ImpExtended
  :QM1
    Default.MQSeries.Resources
      SYSTEM.ADMIN.CHANNEL.EVENT
      SYSTEM.ADMIN.COMMAND.QUEUE
      SYSTEM.ADMIN.PERFM.EVENT
      SYSTEM.ADMIN.QMGR.EVENT
      SYSTEM.CHANNEL.INITQ
      SYSTEM.CHANNEL.SYNCQ
      SYSTEM.CICS.INITIATION.QUEUE
      SYSTEM.DEAD.LETTER.QUEUE
      SYSTEM.DEF.CLNTCONN
      SYSTEM.DEF.RECEIVER
      SYSTEM.DEF.REQUESTER
      SYSTEM.DEF.SENDER
      SYSTEM.DEF.SERVER
      SYSTEM.DEF.SVRCONN
      SYSTEM.DEFAULT.ALIAS.QUEUE
      SYSTEM.DEFAULT.INITIATION.QUEUE
      SYSTEM.DEFAULT.LOCAL.QUEUE
      SYSTEM.DEFAULT.MODEL.QUEUE
      SYSTEM.DEFAULT.PROCESS
      SYSTEM.DEFAULT.REMOTE.QUEUE
      SYSTEM.MQSC.REPLY.QUEUE
```

Figure 47. QM1 queue manager created by importing the export_extended.xml file

In Figure 46 on page 98 and Figure 47, you can see that the two queue managers that are created from importing XML files have the same set of resources. However, the resources under QM1 that are created by importing the `export_extended.xml` file are grouped under the resource group named Default.MQSeries.Resources, while resources under QM1 that are created by importing the `export_partial.xml` file are not grouped. The reason is that the Default.MQSeries.Resources resource group that is created by WebSphere MQ Configuration agent for grouping usage is not a real resource in the WebSphere MQ environment and so is not exported when you export data using the partial export option.

Related reference:

"Step 4: importing the export_partial.xml file" on page 97

Security (z/OS systems only using external security)

The following security measures are required:

- For partial export or partial import operations, you must have update authority to the resource that you select to export the data from or that you select to import the data to.

- For export operations, you must have read authority to the resources that are being exported.
- For import operations, you must have update authority to the target resource.

Exporting data from the configuration database

You can export data from the configuration database and store it in MQSC commands script format. The MQSC commands script that is produced and saved in a file can be directly used to create WebSphere MQ resources on your actual queue manager.

To use an MQSC commands script to create WebSphere MQ resources on your actual queue manager, you must also use WebSphere MQ command processors.

The following example shows how to use the MQSC commands in the `mqsc.tst` file to create resources in the QMGR queue manager:

```
runmqsc  QMGR < mqsc.tst
```

where `mqsc.tst` is an MQSC commands script that is exported from a queue manager.

For details about the **runmqsc** command provided by WebSphere MQ, see the *WebSphere MQ System Administration Guide*.

On z/OS systems, use the **CSQUTIL** batch utility program to create resources on your actual queue manager using the exported MQSC commands script.

On i5/OS™ systems, use the **STRMQMMQSC** command to create resources on your actual queue manager using the exported MQSC commands script.

Exporting MQSC commands

You can use the MQSC commands export option to export a single defined resource or a group of defined resources. The exported data are MQSC commands that can be used to create resources in your WebSphere MQ environment.

The MQSC commands export option is available from the defined view tree. Do the following steps to export a resource, a resource group, a queue manager or a configured system group:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. In the Defined View, right-click the resource that you want to export and click **Export** > **MQSC Commands**. To select multiple resources, press the Ctrl key when you select the resources.
2. In the standard Save file window, enter the name of the file to save the MQSC commands. The suggested file extension for an MQSC commands script is `.tst`. The file is created if it does not already exist.
3. A message is displayed indicating that the requested action is completed successfully. Click **OK**.

The MQSC commands that are used to create all subordinate resources to the selected resource are included in the export file. This is an example export file:

```
* <CNFG Ver="06.00.00" Appl="MQ" Type="MQSC" Level="2" Date="08/01/07"
  Time="22:53:49">

DEFINE QLOCAL  ('GQL.1') DEFPRTY( 0 ) DEFPSIST( NO ) DESCR('A local queue ')-
 PUT( ENABLED ) BOTHRESH( 0 ) DEFSOPT( SHARED ) DISTL( NO ) GET( ENABL-
ED ) MAXDEPTH( 5000 ) MAXMSGL( 4194304 ) MSGDLVSQ( PRIORITY )  HARDENB-
O  SHARE  NOTRIGGER NPMCLASS( NORMAL ) QDEPTHHI( 80 ) QDEPTHLO( 20 ) Q-
DPHIEV( DISABLED ) QDPLOEV( DISABLED ) QDPMAXEV( ENABLED ) QSVCIEV( NO-
NE ) QSVCINT( 999999999 ) RETINTVL( 999999999 ) SCOPE( QMGR ) TRIGDPTH-
( 1 ) TRIGMPRI( 0 ) TRIGTYPE( FIRST ) USAGE( NORMAL ) DEFBIND( OPEN ) -
CLWLPRTY( 0 ) MONQ( QMGR ) ACCTQ( QMGR ) STATQ( QMGR ) CLWLUSEQ( QMGR -
) CLWLRANK( 0 )

DEFINE SERVICE ('SYSTEM.DEFAULT.SERVICE') DESCR(' ') CONTROL( MANUAL ) -
SERVTYPE( COMMAND )
```

Only application attributes are included. Resources that are based on prototypes are effectively disinherited in the export operation; global variables are resolved in the output file.

After the export operation, the original object remains unchanged in the configuration database.

MQSC command notes

Exporting resources using MQSC commands generates a commands script for creating WebSphere MQ resources that are within the scope of the export.

To make scripts portable, the significant length of generated MQSC commands is restricted to 72 characters. If a command exceeds 72 characters, it is continued on the next line.

- If the MQSC commands script was generated for a queue manager that is running on an operating system (for example, a z/OS system) different from the operating system of the target queue manager (for example, a UNIX system), syntax errors can result when you run the **runmqsc** command with the generated commands script. This is because some attributes or resources are valid only on certain systems. Syntax errors can also result if the source object and target object are running on different versions of WebSphere MQ.
- When you run the **runmqsc** command with the generated commands script, duplicate default resources cause duplicate resource errors; this is expected.
- Queue manager definitions are not exported. The command to create a queue manager is outside the scope of the **runmqsc** command. Only the resources that are stored in the queue manager are exported.
- If the system type of the defined queue manager is unknown, all attributes that belong to the resource are exported. For example, for a resource with the type local queue, the QSGDISP attribute is exported. If this script is used as an input to a queue manager that is running on UNIX or Linux systems, it causes a syntax error. In this case, you must edit the generated commands script to make sure that the syntax errors do not occur on the target system.
- Lines in the file containing the commands must not exceed the maximum line length for the system on which you are running the commands. If a line is too long, you must open the file containing the commands and divide the commands across multiple lines that do not exceed the maximum line length of the system. The maximum line lengths for different systems are as follows:
  - Windows systems, AIX systems, HP-IA systems, i5/OS systems, Solaris systems, and all versions of Linux systems: maximum line length of 2048 characters.

- Other versions of UNIX and HP OpenVMS systems: maximum line length of 80 characters.
- Compaq NSK systems: maximum line length of 72 characters.
- z/OS systems: maximum line length of 72 characters. Although scripts are held in a fixed-format data set, with a record length of 80 characters, Characters 73 - 80 are ignored.

Chapter 7. Protect resources from unauthorized access using the granular security function (distributed systems only)

As a security administrator, you can implement security control by using the granular security function. With this function, you can grant staff appropriate access authorities to resources in the configuration database and resources in the WebSphere MQ environment. As a result, resources in the configuration database and resources in the WebSphere MQ environment can be properly protected.

By default, the sysadmin ID is used as the security administrator. However, you can abandon the sysadmin ID and use another user ID for administration. For information about how to create another user ID with equivalent authorities as sysadmin, see Appendix C, "Creating another user ID with equivalent authorities as sysadmin," on page 263.

Important: The granular security function is applicable only when the hub monitoring server runs on a distributed system. For information about the similar security available when the hub monitoring server runs on a z/OS system, see *IBM Tivoli OMEGAMON XE for Messaging for z/OS: Planning and Configuration Guide*.

Before you start to use the granular security function, do the following things:

- Understand the following concepts:
  - "Inheritance of security authority" on page 104
  - "Security checking level" on page 105
  - "Default access level" on page 108
  - "Different levels of access authorities" on page 111
- Familiarize yourself with the procedure that WebSphere MQ Configuration agent uses to determine if a specific user ID has the required access authorities to perform a certain operation. See "How the WebSphere MQ Configuration agent checks authority settings" on page 109.

To use the granular security function, you must complete the following tasks:

1. Enable the granular security function in your environment.
2. Set security checking level for a configured system group.
3. Grant authorities for an object to a user ID or Grant authorities for an object to a group ID (In this way, all users that belong to this group have the same access authorities for the object.)

When you use the granular security function, use the guidelines that are described in "Best practices when the granular security function is used" on page 120 to help you implement security control in your environment.

To grant authorities for backing up the configuration database, accessing audit log, global variables, and schedules, see the following topics:

- Grant authorities for backing up the configuration database
- Grant authorities for adding, deleting, or modifying global variables
- Grant authorities for accessing the audit log
- Grant authorities for viewing, deleting, or modifying schedules

To view authority settings for backing up the configuration database, global variables, audit log, and scheduled actions, see the following topics:

- View authority settings for backing up the configuration database
- View authority settings for global variables
- View authority settings for accessing audit log
- View authority settings for scheduled actions

To change authority settings for an object, see change authority settings for an object.

To check what authorities are required for performing a specific operation, see access authorities required for different operations.

Remember: When a user wants to operate a defined object that is based on a prototype, the WebSphere MQ Configuration agent does not check the authority settings for the prototype on which the defined object is based. The operation is approved if the user has appropriate authority for the defined object.

Inheritance of security authority

In an environment that is implemented with security policy, a secure object is the object with explicitly defined security authority. A non-secure object is the object without explicitly defined security authority. To protect the configuration data, each object must be protected by the security authority in one of the following ways:

- Use the default security authority for the entire configuration tree hierarchy (including the Prototype View)
- Specify an explicit security authority for an object
- Allow the non-secure object to inherit the security authority from the first preceding secure object in the configuration tree hierarchy

Adopting an inherited security authority can greatly reduce the administration tasks for a security administrator.

The power of security authority inheritance is based on this principle: Any object without an explicitly defined security authority inherits the authority of its nearest preceding object with an explicitly defined security authority. The inheritance chain is broken when an object has an explicitly defined security authority.

Security authority inheritance simplifies the administration tasks of setting and maintaining access control on a large protected configuration data space. In a typical configuration data space, you must specify only a few security authorities at key locations to secure the entire configuration data.

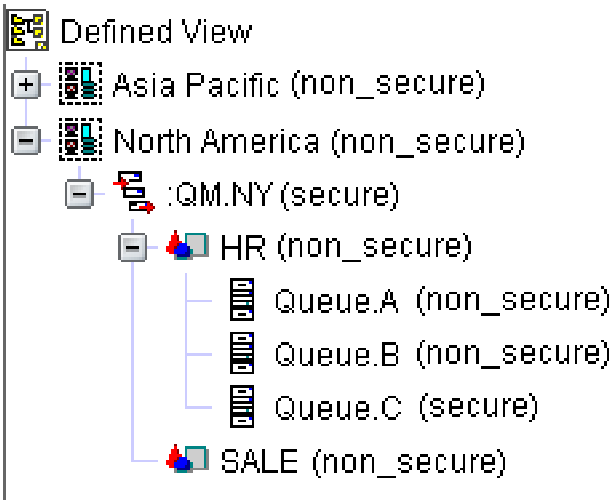
A typical configuration data space begins with a single explicit security authority that is defined to the root of the configuration data, such as the root of the Defined View and the Prototype View. The root authority must always exist. Typically, the root authority is set to the authority with the strictest restriction, NONE. All descendent objects in the configuration tree hierarchy inherit the authority implicitly.

When a subtree in the configuration data space requires different access control restrictions, you can define an explicit security authority at the root object of that subtree. This explicit authority interrupts the flow of inherited security authorities from the root node to that subtree. A new chain of inheritance begins from this newly created explicit security authority.

The WebSphere MQ Configuration agent checks inheritance beginning with the root node of the configuration data. If you do not explicitly set a security authority on any other object in the tree, the objects in the entire tree inherit this root security authority.

An example of the configuration tree structure is displayed in the following figure. The Asia Pacific and North American configured system groups are non-secure objects. The QM.NY configured system is secure object. The HR and SALE resource groups are non-secure objects. The Queue.A and Queue.B queues are non-secure objects, and the Queue.C queue is a secure object.

The Queue.A queue, Queue.B queue, HR resource group, and SALE resource group inherit the security authority from the QM.NY queue. The North American and Asia Pacific configured system groups inherit the security authority from the root node of the configuration data space (default access level).



Security checking level

With security authority inheritance, a non-secure object inherits the authority settings of the first secure object that is above it in the configuration tree. It greatly reduces the administration tasks for security administrators; however, security checking can be slow if the non-secure object is at a relatively low level in the object hierarchy and the WebSphere MQ Configuration agent has to check multiple objects above it. To solve this problem, security checking level is used at the configured system group level to improve the performance of security checking.

Security checking level is an attribute that is associated with a configured system group. It is used to determine the starting point of security checking when you attempt to operate an object in the Defined View. For information about how the WebSphere MQ Configuration agent determines if a user has the required access authorities to perform a specific operation, see "How the WebSphere MQ Configuration agent checks authority settings" on page 109.

Security checking level affects the performance of security checking; it should be modified only by security administrators.

Table 1 contains information about the five security checking levels and how the WebSphere MQ Configuration agent uses the security checking level to determine if your user ID has the required access authorities for the operation.

Table 1. Security checking level

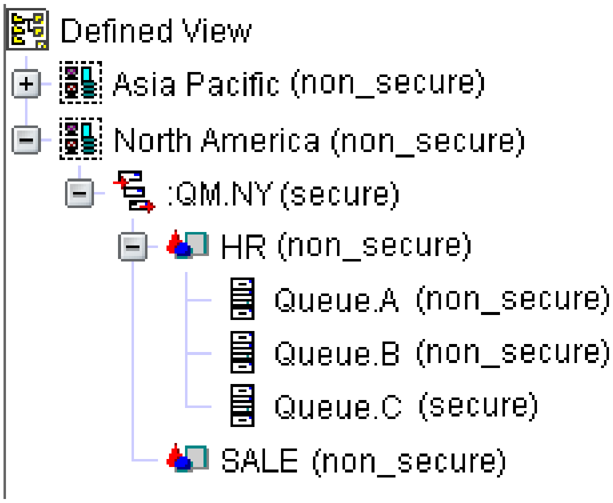
Security checking level	Hierarchy level	Description
None	Top	All objects in the configured system group are protected according to the default access level that is defined in the hub Tivoli Enterprise Monitoring Server. The WebSphere MQ Configuration agent uses the default access level to determine if a user has the required access authorities to perform a specific operation. When the security checking level is set to None, security checking has the best performance but the least flexibility.
Configured system group	Second	All objects in the configured system group are protected according to the access authority settings that are associated with the configured system group. When configured system group is specified as the security checking level, the WebSphere MQ Configuration agent begins to search from its access authority settings, even if access authority settings that are associated with lower security checking levels exist.
Configured system	Third	All objects that belong to the configured system are protected according to the access authority settings that are associated with the configured system. When configured system is specified as the security checking level, the WebSphere MQ Configuration agent begins to search from its access authority settings, even if access authority settings that are associated with lower security checking levels exist.

Table 1. Security checking level (continued)

Security checking level	Hierarchy level	Description
Resource group	Fourth	Each resource in the configured system group is protected according to the access authority settings that is associated with the resource group. When resource group is specified as the security checking level, the WebSphere MQ Configuration agent begins to search from the access authority settings that are associated with the resource group, even if access authority settings that are associated with lower security checking levels exist.
Resource	Bottom	Each resource that belongs to the configured system group is protected according to the access authority settings that are associated with the resource. When resource is specified as the security checking level, the WebSphere MQ Configuration agent begins to search from the access authority settings that are associated with this resource. When the security checking level is set to None, security checking has the worst performance but the most flexibility.

The following figure shows how security checking level improves the performance of security checking. In this example, security checking level is set to configured system. When you operate the Queue.C queue, which is a secure object, the WebSphere MQ Configuration agent starts security checking from the configured system, which in this example is the QM.NY queue manager, and skips checking

Queue.C, even though it is a secure object.


Defined View
Asia Pacific (non_secure)
North America (non_secure)
:QM.NY (secure)
HR (non_secure)
Queue.A (non_secure)
Queue.B (non_secure)
Queue.C (secure)
SALE (non_secure)

To determine the appropriate security checking level for your environment, consider the following factors:

- Efficiently protect your configuration data. Keep in mind that security checking level affects performance. If you set the security checking level to the top level, security checking has the best performance and the least flexibility. If you set the security checking level to the bottom level, security checking has the worst performance and the most flexibility.
- Align with your business needs. For example, if you have queue managers that contain objects that are used by different groups of users, you can set the security checking level to configured system or higher.
- Consider the security checking level together with access authority settings. Security checking level is closely related to access authority settings. Changing the security checking level to a higher level might invalidate existing access authority settings of some objects and cause potential security risks. To simplify the administration tasks of a security administrator, you can define access authority settings only on those objects that are of the type that is specified as the value of the security checking level .

Default access level

In granular security, access level is the level of authority that is required to access a protected object. As a system administrator, you can grant different access authorities for a certain object to a user ID or a group ID. Also, you can decide to use the default access level that applies to all the objects in the configuration database or in the WebSphere MQ environment. The default access level for the configuration database and for the WebSphere MQ environment are specified when you enable the granular security function.

The WebSphere MQ Configuration agent uses the default access level to determine whether the operation should be approved in one of the following circumstances:

- The security checking level is set to NONE.
- The security checking level is not set to NONE, but no authority for the target object is specified for the user ID that wants to use the operation or for the group ID that the user ID belongs to.

For information about different access levels for the configuration database and for objects in the WebSphere MQ environment, see "Different levels of access authorities" on page 111.

How the WebSphere MQ Configuration agent checks authority settings

When a user wants to use some operation on an object, the WebSphere MQ Configuration agent checks the authority settings for the user to determine whether the operation can be approved.

Remember: The process of checking authority settings that is described in this section is done by the WebSphere MQ Configuration agent. No human interaction is required in the this process.

Important: The process of checking authority settings is bypassed for a security administrator user ID. All operations are automatically approved for a security administrator.

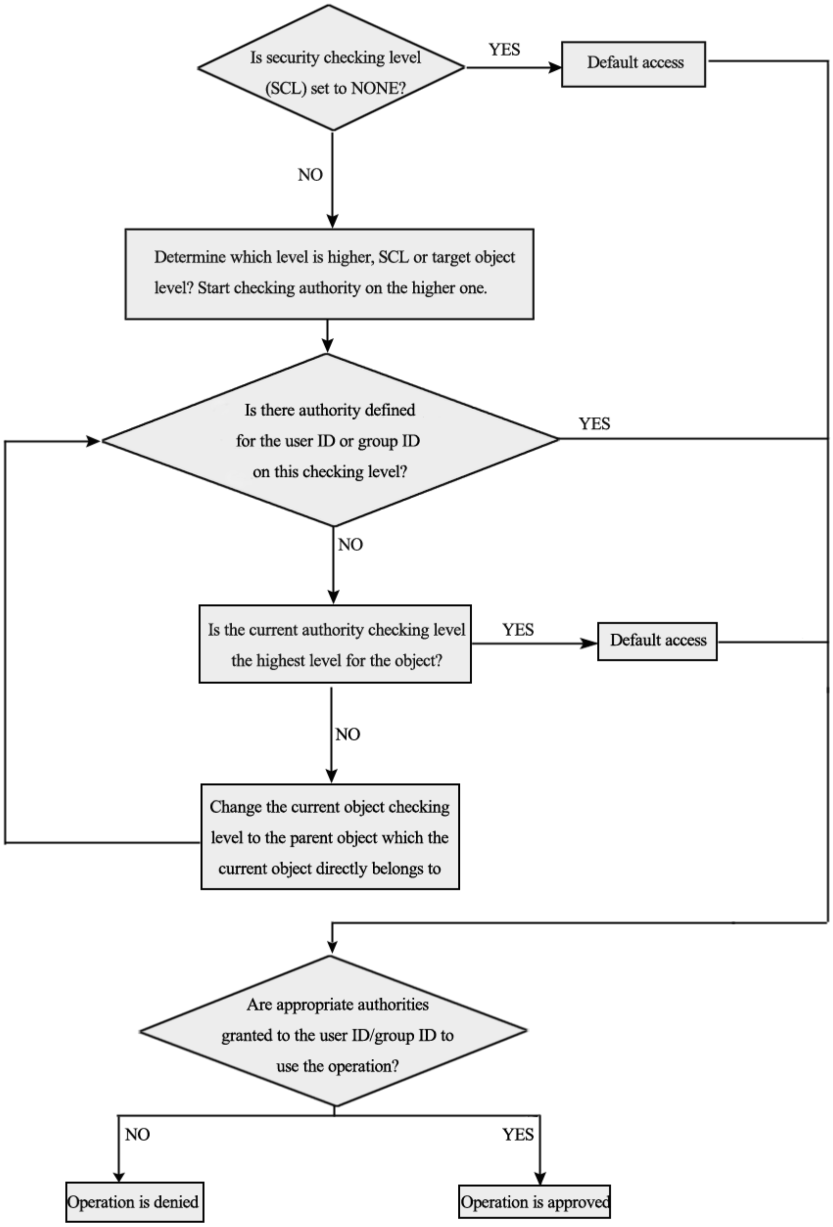
If the security checking level that is associated with a configured system group is set to NONE, the default access level is used to determine whether the user has appropriate authority to use the operation. Otherwise, the WebSphere MQ Configuration agent first compares the security checking level and the target object level and starts authority checking for the user from the higher level. If there is no authority specified on the current checking level for the user or the group that the user belongs to, the WebSphere MQ Configuration agent checks whether there is authority specified on a higher level for the user or the group that the user belongs to, until the checking level is the highest level. See Table 2 for the highest checking levels for different objects. If there is still no authority specified on the highest level for the user or the group that the user belongs to, the default access level is used to determine whether the user has appropriate authority to use the operation.

The highest checking level is different for different objects, as shown in Table 2:

Table 2. Highest checking level for different objects

Objects	Highest checking level
Objects in the Defined View	Configured system group
Objects in a configured system prototype	Configured system
Objects in a resource group prototype	Resource group
Objects in a resource prototype	Resource

The authority checking process is illustrated in Figure 48 on page 110.



Is security checking level (SCL) set to NONE?
YES
Default access
NO
Determine which level is higher, SCL or target object level? Start checking authority on the higher one.
Is there authority defined for the user ID or group ID on this checking level?
YES
NO
Is the current authority checking level the highest level for the object?
YES
Default access
NO
Change the current object checking level to the parent object which the current object directly belongs to
Are appropriate authorities granted to the user ID/group ID to use the operation?
NO
YES
Operation is denied
Operation is approved

Figure 48. Authority checking flow

1. The WebSphere MQ Configuration agent checks whether the security checking level is set NONE, and does one of the following things, depending on the checking result:
   - If the security checking level is set to NONE, the default access level is used to determine whether appropriate authorities are granted to the user ID or the group ID that the user ID belongs to and skip to Step 4.

- If the security checking level is not set to NONE, the WebSphere MQ Configuration agent compares the security checking level with the target object level, determines which level is higher, and starts the authority checking on this higher level.

  Remember: If the operation is to create an object, the WebSphere MQ Configuration agent compares the security checking level with the level of the parent object that the newly created object belongs to, instead of the target object level.

  Exception: The concept of security checking level is applicable only to objects in the Defined View. For objects in the Prototype View, the WebSphere MQ Configuration agent skips this step, and checks authority settings on the current object level directly.

2. The WebSphere MQ Configuration agent checks whether the authority is specified on the current checking level for the user ID or the group ID that the user ID belongs to, and does one of the following things depending on the checking result:
   - If there is authority specified for the user ID or the group ID, skip to Step 4.
   - If there is no authority specified for the user ID or the group ID, proceed to the next step.
3. The WebSphere MQ Configuration agent does one of the following things depending on whether the current checking level is on the highest level for the target object:
   - If the current authority checking is on the highest level, the WebSphere MQ Configuration agent uses the default access level to determine whether appropriate authorities are granted to the user ID or the group ID, and skip to Step 4.
   - If the current authority checking is not on the highest level, the WebSphere MQ Configuration agent changes the current checking level to the level of the parent object to which the current object directly belongs in the hierarchical tree structure. Go back to Step 2 and repeat Step 2 andStep 3, until the current authority checking level is the highest level for the object.
4. The WebSphere MQ Configuration agent checks whether required authorities are granted to the user ID or the group ID to use the operation.
   - If the user ID or the group ID has the appropriate authority, the user operation is approved.
   - If the user ID or the group ID does not have the appropriate authority, the user operation is denied.

Different levels of access authorities

Table 3 and Table 4 on page 112 list the different levels of access authorities to objects in the configuration database and in the WebSphere MQ environment, and what you can do with these access authorities.

Table 3. Access authorities to objects in the configuration database

Access authority	What you can do with this access authority
NONE	You cannot view the settings list of the object and cannot change the object in the configuration database.

Table 3. Access authorities to objects in the configuration database (continued)

Access authority	What you can do with this access authority
READ	You can view the settings list of the object but cannot change it in the configuration database.
UPDATE	UPDATE inherits the authority of READ. With this authority, you can make changes to the object in the configuration database.
CREATE	CREATE inherits the authority of UPDATE. With this authority, you can create new objects in the configuration database.
DELETE	DELETE inherits the authority of CREATE. With this authority, you can delete objects from the configuration database.

Table 4. Access authorities to objects in the actual WebSphere MQ environment

Access authority	What you can do with this access authority
NONE	You cannot view the information about the object in the WebSphere MQ environment.
READ	You can view information about the object in the WebSphere MQ environment, but you cannot change it.
EXECUTE	EXECUTE inherits the authority of READ. With this authority, you can change the object in the actual WebSphere MQ environment, including creating a new object and modifying or deleting an existing object.

Enabling the granular security function

By default, the granular security function is disabled after installation. You must customize the environment file of the hub Tivoli Enterprise Monitoring Server to enable the granular security function.

Before you enable the granular security function, do the following steps:

1. Ensure that there is a Lightweight Directory Access Protocol (LDAP) server in your environment. The LDAP servers that the WebSphere MQ Configuration agent can work with include IBM Tivoli Directory Server 6.2 or later, and Novell e-Directory Server 8.8 or later.
2. Import the `mc_itds.schema` file (for Tivoli Directory Server) or the `mc_edir.schema` file (for Novell e-Directory Server) to the LDAP server. The schema files are created when you install the application support for WebSphere MQ Configuration agent on the Tivoli Enterprise Monitoring Server. Do the following steps to import the schema file to the LDAP server:
   a. Ensure that the LDAP server is running and the LDAP bind ID that you use to log on to the LDAP server has the authority to modify the schema.
   b. Copy the `mc_itds.schema` file or the `mc_edir.schema` file from the following directory on the hub Tivoli Enterprise Monitoring Server to the LDAP server:
      - Windows systems: *`install_dir`*`\CMS\RKCFLDAP`
      - UNIX and Linux systems: *`install_dir`*`/tables/`*`tems_name`*`/RKCFLDAP`

where *install_dir* is the installation directory of IBM Tivoli Monitoring, and *tems_name* is the name of hub Tivoli Enterprise Monitoring Server.

c. Run one of the ldapmodify commands to import the schema file, depending on the LDAP server that you are using:
   - Tivoli Directory Server:

     ```
     ldapmodify -h hostname -p port -a -c -D binddn -w password -i
        mc_itds.schema
     ```
   - Novell e-Directory Server:

     ```
     ldapmodify -h hostname -p port -r -c -D binddn -w password -f
        mc_edir.schema
     ```

   where *hostname* is the host name of the directory server; *port* is the port number for accessing the directory server host; *binddn* is the bind ID of the LDAP server for accessing your directory; and *password* is the password for the LDAP bind ID.

   Tip:
   - You can find the ldapmodify tool in the following directory, where *install_dir* is installation directory of the directory server:
     - Windows systems: `install_dir\bat`
     - UNIX and Linux systems: `install_dir/bin`
   - For more information about how to use the ldapmodify tool, such as the Secure Sockets Layer (SSL) options, refer to the documents of Tivoli Directory Server or Novell e-Directory Server.

3. Define a base Distinguished Name (DN) for the LDAP server. This DN will be used when you enable the granular security function.

To enable the granular security function, do one of the following procedures, depending on the operating system where the hub Tivoli Enterprise Monitoring Server is installed:

- If the hub Tivoli Enterprise Monitoring Server is installed on a Windows system, see “Enabling the granular security function on Windows systems.”
- If the hub Tivoli Enterprise Monitoring Server is installed on a UNIX or Linux system, see “Enabling the granular security function on UNIX and Linux systems” on page 115.

Enabling the granular security function on Windows systems

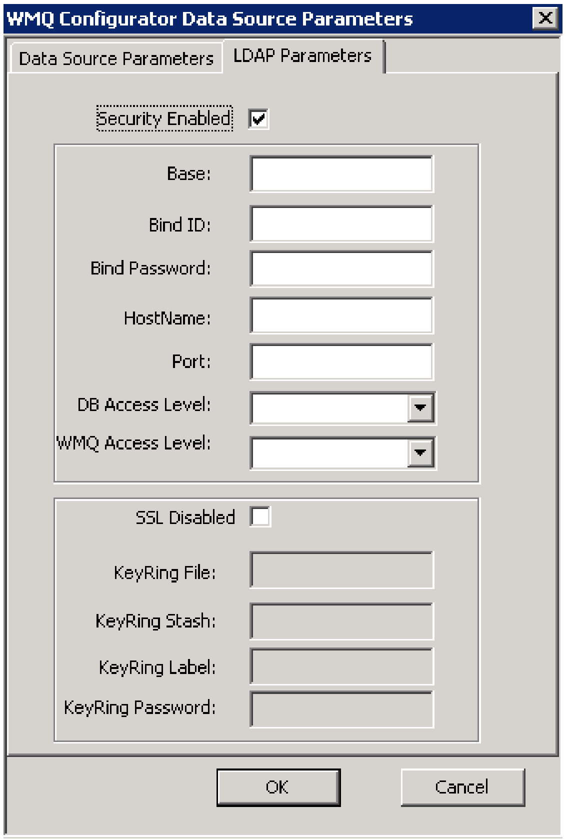
By default, the granular security function is disabled after installation. You must customize the environment file of the hub Tivoli Enterprise Monitoring Server to enable the granular security function.

Ensure that there is an LDAP server in your environment. The LDAP servers that the WebSphere MQ Configuration agent can work with include Tivoli Directory Server 6.2 or later, and Novell e-Directory Server 8.8 or later.

If the hub Tivoli Enterprise Monitoring Server is running on a Windows system, to enable the granular security function, do the following steps:

1. Log on to the system where the hub monitoring server is installed.
2. Go to the `install_dir\CMS` directory, where *install_dir* is the IBM Tivoli Monitoring installation directory. The default is `C:\IBM\ITM`.
3. Double-click the `KCFDataSource.exe` file. The WMQ Configurator Data Source Parameters window opens.

4. Open the **LDAP Parameters** tab page. The LDAP parameters are displayed in the window, as shown in Figure 49.



Security Enabled ☑

SSL Disabled ☐

Figure 49. LDAP parameters

5. To enable the granular security function, select **Security Enabled** .
6. Do the following steps to enter information about the LDAP server:
   a. In the **Base** field, enter the base DN that you defined previously.
   b. In the **Bind ID** field, enter the bind ID of the LDAP server.
   c. In the **Bind Password** field, enter the password of the LDAP bind ID.
   d. In the **Host name** field, enter the host name of LDAP server.
   e. In the **Port** flied, enter the port number of the LDAP server.
   f. In the **DB Access Level**, click the arrow to set the default access level for the configuration database.
   g. In the **WMQ Access Level** list, select the default access level for objects in the WebSphere MQ environment.
7. To use Secure Socket Layer (SSL) communication between the Tivoli Enterprise Monitoring Server and the LDAP server, do the following steps:
   a. Select **SSL Enabled**.
   b. In the **Key Ring File** field, enter the name of the key ring file.
   c. In the **Key Ring Stash** field, enter the key ring stash.
   d. In the **Key Ring Label** field, enter the key ring label.
   e. In the **Key Ring Password** field, enter the key ring password.
8. Click **OK**.

9. For the changes to take effect, restart the hub Tivoli Enterprise Monitoring Server .

Tip: If you want to check if the granular security function is enabled successfully, find related log information in the Tivoli Enterprise Monitoring Server log file. The monitoring server log file can be found in the `install_dir\logs` directory, where *install_dir* is the directory where the IBM Tivoli Monitoring is installed.

Enabling the granular security function on UNIX and Linux systems

By default, the granular security function is disabled after installation. You must customize the environment file of the hub Tivoli Enterprise Monitoring Server to enable the granular security function.

Ensure that there is a LDAP server in your environment. The LDAP servers that the WebSphere MQ Configuration agent can work with include Tivoli Directory Server 6.2 or later, and Novell e-Directory Server 8.8 or later.

To enable the granular security function at the hub Tivoli Enterprise Monitoring Server that is running on UNIX or Linux systems, do the following steps:

1. Log on to the system where the hub monitoring server is installed.
2. If the configuration database is a DB2 database, run the following command:

   ```
   . DB2_instance_home/sqllib/db2profile
   ```

   where *DB2_instance_home* is the home directory of the DB2 instance.
3. To customize the environment file of the hub Tivoli Enterprise Monitoring Server, use the KCFDataSourceU database configuration tool. Run the following commands:
   - For AIX systems:

     For a 32-bit monitoring server, run the following commands:

     ```
     export KEYFILE_DIR=install_dir/keyfiles
     export ICCRTE_DIR=install_dir/arch_gs/gs
     export KBBENV_HOME=install_dir/tables/tems_name
     export KBBENVINI_HOME=install_dir/config
     export LIBPATH=install_dir/arch_gs/gs/lib:$LIBPATH
     cd install_dir/arch/ms/bin
     ./KCFDataSourceU -s (Y|N) -b LDAPBaseDN -B LDAPBindID
     -P LDAPBindPassword -h LDAPHostName -T LDAPPort -D LDAPDBAccessLevel
     -W LDAPWMQAccessLevel -S (Y|N) -F KeyRingFile -H KeyRingStash -L KeyRingLabel
     -A KeyRingPassword
     ```

     For a 64-bit monitoring server, run the following commands:

     ```
     export KEYFILE_DIR=install_dir/keyfiles
     export ICCRTE_DIR=install_dir/arch_gs/gs
     export KBBENV_HOME=install_dir/tables/tems_name
     export KBBENVINI_HOME=install_dir/config
     export LIBPATH=install_dir/arch_gs/gs/lib64:$LIBPATH
     cd install_dir/arch/ms/bin
     ./KCFDataSourceU -s (Y|N) -b LDAPBaseDN -B LDAPBindID
     -P LDAPBindPassword -h LDAPHostName -T LDAPPort -D LDAPDBAccessLevel
     -W LDAPWMQAccessLevel -S (Y|N) -F KeyRingFile -H KeyRingStash -L KeyRingLabel
     -A KeyRingPassword
     ```
   - For Linux systems:

     ```
     export KEYFILE_DIR=install_dir/keyfiles
     export ICCRTE_DIR=install_dir/arch_gs/gs
     export KBBENV_HOME=install_dir/tables/tems_name
     ```

```
export KBBENVINI_HOME=install_dir/config
cd install_dir/arch/ms/bin
./KCFDataSourceU -s (Y|N) -b LDAPBaseDN -B LDAPBindID
-P LDAPBindPassword -h LDAPHostName -T LDAPPort -D LDAPDBAccessLevel
-W LDAPWMQAccessLevel -S (Y|N) -F KeyRingFile -H KeyRingStash -L KeyRingLabel
-A KeyRingPassword
```

- For HP-IA systems:

  ```
  export KEYFILE_DIR=install_dir/keyfiles
  export ICCRTE_DIR=install_dir/arch_gs/gs
  export KBBENV_HOME=install_dir/tables/tems_name
  export KBBENVINI_HOME=install_dir/config
  cd install_dir/arch/ms/bin
  ./KCFDataSourceU -s (Y|N) -b LDAPBaseDN -B LDAPBindID
  -P LDAPBindPassword -h LDAPHostName -T LDAPPort -D LDAPDBAccessLevel
  -W LDAPWMQAccessLevel -S (Y|N) -F KeyRingFile -H KeyRingStash -L KeyRingLabel
  -A KeyRingPassword
  ```

- For Solaris systems:

  ```
  export KEYFILE_DIR=install_dir/keyfiles
  export ICCRTE_DIR=install_dir/arch/ms/lib/gskit
  export KBBENV_HOME=install_dir/tables/tems_name
  export KBBENVINI_HOME=install_dir/config
  cd install_dir/arch/ms/bin
  ./KCFDataSourceU -s (Y|N) -b LDAPBaseDN -B LDAPBindID
  -P LDAPBindPassword -h LDAPHostName -T LDAPPort -D LDAPDBAccessLevel
  -W LDAPWMQAccessLevel -S (Y|N) -F KeyRingFile -H KeyRingStash -L KeyRingLabel
  -A KeyRingPassword
  ```

where:

- *install_dir* is the installation directory of IBM Tivoli Monitoring.
- *arch* is the architecture code of your operating system (See Appendix B, “Architecture codes,” on page 261 for reference).
- *arch_gs* is the architecture code of the operating system where the `gs` directory locates. Use the following examples as reference:
  - For a 32-bit monitoring server on the AIX systems, use `aix523`.
  - For a 64-bit monitoring server on the AIX systems, use `aix526`.
  - For the monitoring server on the Linux for xSeries systems, use `li6243`.
  - For the monitoring server on the Linux for zSeries systems, use `ls3266`.
  - For the monitoring server on the HP-IA systems, use `hpi113`.
- *tems_name* is the name of the hub Tivoli Enterprise Monitoring Server.
- the -s option specifies whether to enable the granular security function. Y indicates yes and N indicates no.
- *LDAPBaseDN* is the based DN that you defined previously.
- *LDAPBindID* is the bind ID of the LDAP server.
- *LDAPBindPassword* is the password of the LDAP bind ID.
- the -h option specifies the host name of the LDAP server.
- *LDAPHostName* is the host name of the LDAP server.
- *LDAPPort* is the port number of the LDAP server.
- *LDAPDBAccessLevel* is the default access level for the configuration database. Valid values are NONE, READ, UPDATE, CREATE, and DELETE.
- *LDAPWMQAccessLevel* is the default access level for the WebSphere MQ environment. Valid values are NONE, READ, and EXECUTE.
- the -S option specifies whether the Secure Socket Layer (SSL) option is enabled. Y indicates yes and N indicates no.
- *KeyRingFile* is the key ring file.

- *KeyRingStash* is the key ring stash.
- *KeyRingLabel* is the key ring label.
- *KeyRingPassword* is the key ring password.

Remember:

- The options for the **KCFDataSourceU** command must be entered in the order that is indicated previously in the *install_dir*/*arch*/ms/bin/KCFDataSourceU line, and they are case-sensitive.
- The options for the key ring are effective only when the SSL option is enabled.

The following example enables the granular security function and disables the SSL option. The root user ID is used to access the LDAP server at the tivc31.cn.ibm.com host. The default access level is set to READ for the configuration database and EXECUTE for the WebSphere MQ environment.

```
export KEYFILE_DIR=/opt/IBM/ITM/keyfiles
export ICCRTE_DIR=/opt/IBM/ITM/sol283/ms/lib/gskit
export KBBENV_HOME=/opt/IBM/ITM/tables/TEMS1
export KBBENVINI_HOME=/opt/IBM/ITM/config
cd /opt/IBM/ITM/sol283/ms/bin
./KCFDataSourceU -s Y -b ou=tivoli,o=ibm -B cn=root
-P password -h tivc31.cn.ibm.com -T 3890 -D READ -W EXECUTE -S N
```

4. For the changes to take effect, restart the hub Tivoli Enterprise Monitoring Server.

Tip: If you want to check if the granular security function is enabled successfully, find related log information in the Tivoli Enterprise Monitoring Server log file. The monitoring server log file can be found in the *install_dir*/logs directory, where *install_dir* is the directory where the IBM Tivoli Monitoring is installed.

Setting security checking level

To set security checking level for a configured system group, do the following steps:

1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, “Creating another user ID with equivalent authorities as sysadmin,” on page 263.
2. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
3. In the Defined View, click the configured system group that you want to set security checking level for. The settings list for the configured system group is displayed on the right side of the workspace.
4. Click the arrow in the **Security Checking Level** field and select the appropriate value. Valid options are `None`, `Configured system group`, `Configured system`, `Resource group`, and `Resource`. The default selection is `Configured system`.
5. To save your changes, click **Save**.

Granting access authorities for an object to a user ID

To grant access authorities for an object to a user ID, do the following steps:

1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, “Creating another user ID with equivalent authorities as sysadmin,” on page 263.
2. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
3. In the Configuration view, click **Defined and Prototype**. The Defined and Prototype View opens.
4. Right-click the object for which you want to grant access authorities to the user ID and click **Granular Security** > **Grant authorization**. The Grant authorization window is displayed.
5. Enter the user ID in the field on the right side of the window, as shown in Figure 50.

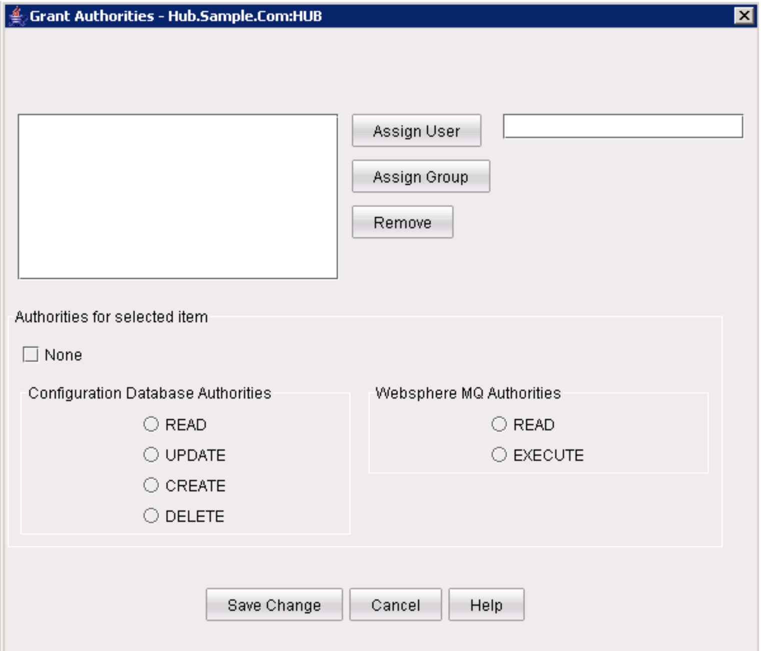


Figure 50. The Grant authorization window

6. Click **Assign User**. The user ID is added to the list on the left side of the window.
7. Depending on the access authorities that you want to grant to this user ID, do one of the following steps:
   a. Select **None** if you do not want to give the user ID any access authority to this object.
   b. Select **READ**, **UPDATE**, **CREATE**, or **DELETE** in the **Configuration Database Authorities** section, and select **READ**, or **EXECUTE** in the **WebSphere MQ Authorities** section. See “Different levels of access authorities” on page 111 for the definition of access authority and what you can do with different access authorities. See “Access authorities required for different operations” on page 180 for the access authorities that are required for performing different operations.
8. Click **Save Change**.

Information about the access authorities that the user has on this object is saved in the LDAP server in your environment.

Granting access authorities for an object to a group ID

To grant access authorities for an object to a group ID, do the following steps:

1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, “Creating another user ID with equivalent authorities as sysadmin,” on page 263.
2. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
3. In the Configuration view, click **Defined and Prototype**. The Defined and Prototype View opens.
4. Right-click the object for which you want to grant access authorities to the group ID and click **Granular Security** > **Grant authorization**. The Grant authorization window is displayed.
5. Enter the group ID in the field on the right side of the window, as shown in Figure 51.

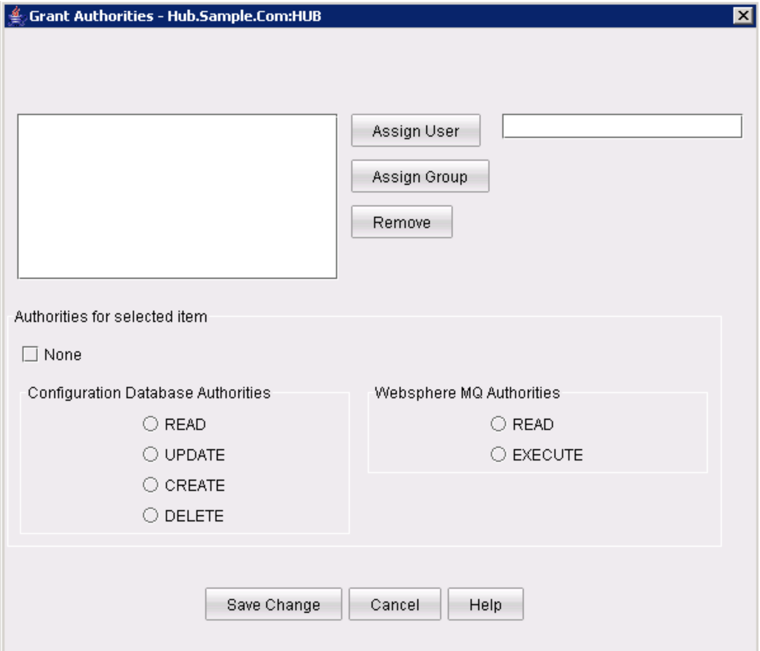


Figure 51. The Grant authorization window

6. Click **Assign Group**. The group ID is added to the list on the left side of the window.
7. Depending on the access authorities that you want to grant to this group ID, do one of the following steps:
   a. Select **None** if you do not want to give the group ID any access authority to this object.
   b. Select **READ**, **UPDATE**, **CREATE**, or **DELETE** in the **Configuration Database Authorities** section, and select **READ**, or **EXECUTE** in the **WebSphere MQ Authorities** section. See “Different levels of access authorities” on page 111 for the definition of access authority and what can

be done with different access authorities. See “Access authorities required for different operations” on page 180 for the access authorities that are required for performing different operations.

8. Click **Save Change**.

Information about the access authorities that users in this group have on this object is saved in the LDAP server in your environment.

Best practices when the granular security function is used

When you use the granular security function, use the following best practice guidelines to help you with implementing security control in your environment:

- The security checking level that you specify for a configured system group affects product performance. The lower the level that you specify for the security checking level, the longer it takes for the WebSphere MQ Configuration agent to check the authority settings for an operation. For performance consideration, set the security checking level as high as possible that best suits your environment.

  Remember: The highest level of the security checking level is NONE. However, when the security checking level is set to NONE, it does not mean that the WebSphere MQ Configuration agent does not check the authority settings at all. Instead, the WebSphere MQ Configuration agent does not check the authority settings for the related object, but checks the default access level that is specified for the configuration database or WebSphere MQ environment, to determine whether an operation is authorized for the related object.
- Group the user IDs in your environment, and use the group IDs as much as possible when you grant authorities. In this way, you do not have to modify the authority settings due to a change of an individual user ID.

  Exception: For the following operations, you must grant authorities to the user ID, regardless of the group ID that the user ID belongs to:
  - Run the **`MCExport`** and **`MCImport`** commands
  - Enable a scheduled action to run
- Group the queue managers into configured system groups for more convenient management. Specify the common security settings at the configured system group level as much as possible, even if the security checking level is not set to Configured system group. In this way, you can save effort in specifying authority settings for objects at lower levels. And the use of a configured system group can facilitate many operations, such as the Discover operation.
- Group the resources, such as queues and channels, into resource groups for more convenient management. In most cases, when the objects are grouped appropriately into resource groups, it is probable to avoid setting the security checking level to Resource. In this way, the performance can be improved, because no authority setting checking is required for each involved resource. And, the category of resources can benefit the users who need to manage these resources.
- When an object is moved or copied, the defined security settings for this object and the resources that this object contains are also propagated. However, the defined security settings for the parent object that contains this object are not propagated.
- Be cautious when you grant the EXECUTE authority for WebSphere MQ to an ID. The queue managers in actual WebSphere MQ environment can be updated with this EXECUTE authority.

- Always use the Tivoli Enterprise Portal GUI to modify the security settings in LDAP.
- By default, the sysadmin ID is provided as a security administrator. A security administrator can define security and has full security access to the whole environment. However, you can use another user ID as the security administrator (see Appendix C, "Creating another user ID with equivalent authorities as sysadmin," on page 263). Be careful when you use a security administrator ID that is not sysadmin to grant authorities. The WebSphere MQ Configuration agent does not check security settings for a security administrator ID. A security administrator ID has full access to the configuration database and actual WebSphere MQ environment, and can manage the authority profiles that are in LDAP.

User scenarios

Common user scenarios are described in this section for the granular security function. As a system administrator, you can use these scenarios to get an overview of how the granular security function can secure the real environment.

User scenario: setting the security checking level to configured system group

In this scenario, assume that there are three groups of queue managers in your environment and that they are used by the Payroll, Accounting, and Warehouse department respectively. The security requirements are as follows:

- WebSphere MQ administrators of each department have full access to the queue managers that are used by their department.
- Operators of each department can change only existing objects in actual queue managers that are used by their department.
- Application users of each department can create, delete, and change objects in queue managers that are used by their department in the configuration database, but they cannot create, delete, or change objects in these queue managers in the real WebSphere MQ environment.

Do the following steps to secure your environment:

1. Create three configured system groups to contain the queue managers for each department, and name them Payroll, Accounting, and Warehouse.
2. In the TEP User Administration window, create the following three user ID groups for the WebSphere MQ administrators of each department:
   - MQAdminPR is a group of users who have full access to administer the queue managers in the Payroll configured system group.
   - MQAdminAC is a group of users who have full access to administer the queue managers in the Accounting configured system group.
   - MQAdminWH is a group of users who have full access to administer the queue managers in the Warehouse configured system group.
3. In the TEP User Administration window, create the following three user ID groups for operators of each department:
   - MQOperPR is a group of users who can update existing objects in actual queue managers in the Payroll configured system group.
   - MQOperAC is a group of users who can update existing objects in actual queue managers in the Accounting configured system group.

- MQOperWH is a group of users who can update existing objects in actual queue managers in the Warehouse configured system group.

4. In the TEP User Administration window, create the following three user ID groups for application users of each department:
   - AppUserPR is a group of application users who can create, delete, and change objects in queue managers in the Payroll configuration system group in the configuration database, but not in the real WebSphere MQ environment.
   - AppUserAC is a group of application users who can create, delete, and change objects in queue managers in the Accounting configured system group in the configuration database, but not in the real WebSphere MQ environment.
   - AppUserWH is a group of application users who can create, delete, and change objects in queue managers in the Warehouse configured system group in the configuration database, but not in the real WebSphere MQ environment.
5. Set the security checking level of each configured system group to **Configured system group**.
6. Grant access authorities to the user groups as follows:
   - In the security settings for the Payroll configured system group, grant the DELETE authority to the configuration database and the EXECUTE authority to the WebSphere MQ environment to the MQAdminPR group.
   - In the security settings for the Payroll configured system group, grant the UPDATE authority to the configuration database and the EXECUTE authority to the WebSphere MQ environment to the MQOperPR group.
   - In the security settings for the Payroll configured system group, grant the DELETE authority to the configuration database and the READ authority to the WebSphere MQ environment to the AppUserPR group.
   - In the security settings for the Accounting configured system group, grant the DELETE authority to the configuration database and the EXECUTE authority to the WebSphere MQ environment to the MQAdminAC group.
   - In the security settings for the Accounting configured system group, grant the UPDATE authority to the configuration database and the EXECUTE authority to the WebSphere MQ environment to the MQOperAC group.
   - In the security settings for the Accounting configured system group, grant the DELETE authority to the configuration database and the READ authority to the WebSphere MQ environment to the AppUserAC group.
   - In the security settings for the Warehouse configured system group, grant the DELETE authority to the configuration database and the EXECUTE authority to the WebSphere MQ environment to the MQAdminWH group.
   - In the security settings for the Warehouse configured system group, grant the UPDATE authority to the configuration database and the EXECUTE authority to the WebSphere MQ environment to the MQOperWH group.
   - In the security settings for the Warehouse configured system group, grant the DELETE authority to the configuration database and the READ authority to the WebSphere MQ environment to the AppUserWH group.
7. Make sure that the default access level for the configuration database and the default access level for the WebSphere MQ objects are set to NONE. The default access level is set when you enable the granular security. For instructions about how to set the default access level, see “Enabling the granular security function” on page 112.

User scenario: setting the security checking level to configured system

In this scenario, assume that there are three queue managers that are named Qmgr_Sales, Qmgr_HR, and Qmgr_TS. They are used by the Sales, HR, and Technical Support application group respectively. The security requirements are as follows:

- Administrators of each application group have full access to administer the queue manager that is used by their application group.
- Users of each application group can change only the queue manager that is used by their application group in the configuration database, they cannot change the real queue manager in the WebSphere MQ environment.
- A central operation group can make changes to objects in all queue managers.

Do the following steps to secure your environment:

1. Create a configured system group to contain the three queue managers.
2. In the TEP User Administration window, create the following three user groups for WebSphere MQ administrators of each application group:
   - SalesAdmin is a group of users who have full access to administer the queue manager that is used by the Sales application group.
   - HRAdmin is a group of users who have full access to administer the queue manager that is used by the HR application group.
   - TSAdmin is a group of users who have full access to administer the queue manager that is used by the Technical Support application group.
3. In the TEP User Administration window, create the following three user groups for users of each application group:
   - SalesUser is a group of Sales application users who can create and change objects in the queue manager in the configuration database, but cannot change the actual queue manager.
   - HRUser is a group of HR application users who can create and change objects in the queue manager in the configuration database, but cannot change the actual queue manager.
   - TSUser is a group of Technical Support application users who can create and change objects in the queue manager in the configuration database, but cannot change the actual queue manager.
4. In the TEP User Administration window, create the MQOper user group to update objects in any queue managers.
5. Set the security checking level of the configured system group to **Configured System**.
6. Grant access authorities to the user groups as follows:
   - In the security settings for the Qmgr_Sales queue manager, grant the DELETE authority to the configuration database and the EXECUTE authority to the WebSphere MQ environment to the SalesAdmin group.
   - In the security settings for the Qmgr_Sales queue manager, grant the CREATE authority to the configuration database and the READ authority to the WebSphere MQ environment to the SalesUser group.
   - In the security settings for the Qmgr_HR queue manager, grant the DELETE authority to the configuration database and the EXECUTE authority to the WebSphere MQ environment to the HRAdmin group.

- In the security settings for the Qmgr_HR queue manager, grant the CREATE authority to the configuration database and the READ authority to the WebSphere MQ environment to the HRUser group.
- In the security settings for the Qmgr_TS queue manager, grant the DELETE authority to the configuration database and the EXECUTE authority to the WebSphere MQ environment to the TSAdmin group.
- In the security settings for the Qmgr_TS queue manager, grant the CREATE authority to the configuration database and the READ authority to the WebSphere MQ environment to the TSUser group.

7. In the security settings for the configured system group, grant the UPDATE authority to the configuration database and the EXECUTE authority to the WebSphere MQ environment to the MQOper group.
8. Make sure that the default access level for the configuration database and the default access level for the WebSphere MQ objects are set to NONE. The default access level is set when you enable the granular security. For instructions about how to set the default access level, see "Enabling the granular security function" on page 112.

User scenario: setting the security checking level to resource group

In this scenario, assume that there is one queue manager that is shared by the Finance, Investment, and Insurance departments. The security requirements are as follows:

- One user group can administer the queue manager in the configuration database, but cannot change the actual queue manager.
- One user group can update existing objects in the queue manager in the configuration database, but cannot change the actual queue manager.
- One user group can update the actual queue manager, but cannot change it in the configuration database.
- Users of each department can change only resources that are used by their department in the configuration database.
- One user from each department can change resources that are used by their department in the configuration database by using the command line interface function.

Do the following steps to secure your environment:

1. Create a configured system group to contain the queue manager.
2. Create three resource groups to contain the resources that are used by the Finance, Investment, and Insurance department, and name them RG_Finance, RG_Investment, and RG_Insurance respectively.
3. In the TEP User Administration window, create the following three user groups for WebSphere MQ administrators:
   - MQAdmin is a group of users who have full access to administer the queue manager in the configuration database, but cannot change the actual queue manager.
   - MQOper is a group of users who can update existing objects in the queue manager in the configuration databases, but cannot change the actual queue manager.
   - MQExec is a group of users who can update the actual queue manager, but cannot change it in the configuration database.

4. In the TEP User Administration window, create the following three user groups for users of each department:
   - FinGrp is a group of users who can update only those objects in the RG_Finance resource group.
   - InvGrp is a group of users who can update only those objects in the RG_Investment resource group.
   - InsGrp is a group of users who can update only those objects in the RG_Insurance resource group.
5. In the TEP User Administration window, create the following user IDs:
   - FinUser is a user who can update only those objects in the RG_Finance resource group by using the command line interface function.
   - InvUser is a user who can update only those objects in the RG_Investment resource group by using the command line interface function.
   - InsUser is a user who can update only those objects in the RG_Insurance resource group by using the command line interface function.
6. Set the security checking level of the configured system group to **Resource Group**.
7. Grant access authorities to the user groups as follows:
   - In the security settings for the configured system group, grant the DELETE authority to the configuration database and the READ authority to the WebSphere MQ environment to the MQAdmin group.
   - In the security settings for the configured system group, grant the UPDATE authority to the configuration database and the READ authority to the WebSphere MQ environment to the MQOper group.
   - In the security settings for the configured system group, grant the READ authority to the configuration database and the EXECUTE authority to the WebSphere MQ environment to the MQExec group.
   - In the security settings for the RG_Finance resource group, grant the UPDATE authority to the configuration database and the READ authority to the WebSphere MQ environment to the FinGrp group.
   - In the security settings for the RG_Investment resource group, grant the UPDATE authority to the configuration database and the READ authority to the WebSphere MQ environment to the InvGrp group.
   - In the security settings for the RG_Insurance resource group, grant the UPDATE authority to the configuration database and the READ authority to the WebSphere MQ environment to the InsGrp group.
8. Grant access authorities to the user IDs as follows:
   - In the security settings for the RG_Finance resource group, grant the UPDATE authority to the configuration database and the READ authority to the WebSphere MQ environment to the FinUser user.
   - In the security settings for the RG_Investment resource group, grant the UPDATE authority to the configuration database and the READ authority to the WebSphere MQ environment to the InvUser user.
   - In the security settings for the RG_Insurance resource group, grant the UPDATE authority to the configuration database and the READ authority to the WebSphere MQ environment to the InsUser user.
9. Make sure that the default access level for the configuration database and the default access level for the WebSphere MQ objects are set to NONE. The default access level is set when you enable the granular security. For instructions about how to set the default access level, see “Enabling the granular security function” on page 112.

Granting authorities for backing up the configuration database to a user or group

To back up the configuration database, the user ID or the group ID must have READ or higher authority for the configuration database. To grant the authority for backing up the configuration database to a user ID or a group ID, do the following steps:

1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, “Creating another user ID with equivalent authorities as sysadmin,” on page 263.
2. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
3. To the left of the **Update mode** check box, click **Grant Backup Authorities**. The Grant Authorization window is displayed.
4. In the Grant Authorization window, do one of the following steps, depending on whether the ID already exists in the list on the left side of the window:
   - If the user ID or the group ID exists, click the ID in the list.
   - If the user ID or the group ID does not exist, do the following steps to add the ID to the list:
     a. In the field on the right side of the window, enter the user ID or group ID that you want to grant authority to.
     b. Click **Assign User** or **Assign Group** depending on what type of ID you entered in the previous step. The user ID or the group ID is added to the list on the left side of the window.
5. Ensure that the **None** check box is not selected.
6. Grant configuration database authority to the user ID or the group ID by selecting the authority name in the **Configuration Database Authorities** section. The minimum authority requirement for backing up the configuration database is READ.
7. Click **Save Change**.

Now, the user ID or the group ID has the required authority to back up the configuration database.

Related tasks:

“Viewing authority settings for backing up the configuration database” on page 129

Granting authorities for adding, deleting, or modifying global variables to a user or group

Different authorities are required for an ID to create, modify, or delete a global variable. To grant the authority for adding, deleting, or modifying global variables to a user ID or a group ID, do the following steps:

1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, “Creating another user ID with equivalent authorities as sysadmin,” on page 263.
2. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.

3. In the Configuration view, click **Global Variables**. The Global Variables workspace is displayed on the right side of the Configuration view.
4. Click **Authorities**. The Grant Authorization window is displayed.
5. In the Grant Authorization window, do one of the following steps, depending on whether the ID already exists in the list on the left side of the window:
   - If the user ID or the group ID exists, click the ID in the list.
   - If the user ID or the group ID does not exist, do the following steps to add the ID to the list:
     a. In the field on the right side of the window, enter the user ID or group ID that you want to grant authority to.
     b. Click **Assign User** or **Assign Group** depending on what type of ID you entered in the previous step. The user ID or the group ID is added to the list on the left side of the window.
6. Ensure that the **None** check box is not selected.
7. Grant configuration database authority to the user ID or the group ID by selecting the authority name in the **Configuration Database Authorities** section. The minimum authority requirement for the adding, deleting, or modifying global variables is UPDATE.
8. Click **Save Change**.

Authority for global variables is granted to the user ID or the group ID.

Related tasks:

"Viewing authority settings for global variables" on page 130

Granting authorities for accessing audit log to a user or group

To grant the authority for accessing audit log to a user ID or a group ID, do the following steps:

1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, "Creating another user ID with equivalent authorities as sysadmin," on page 263.
2. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
3. In the Configuration view, click **Audit Log**. The Audit Log workspace is displayed on the right side of the Configuration view.
4. Click **Grant Authorities**. The Grant Authorization window is displayed.
5. In the Grant Authorization window, do one of the following steps, depending on whether the ID already exists in the list on the left side of the window:
   - If the user ID or the group ID exists, click the ID in the list.
   - If the user ID or the group ID does not exist, do the following steps to add the ID to the list:
     a. In the field on the right side of the window, enter the user ID or group ID that you want to grant authority to.
     b. Click **Assign User** or **Assign Group** depending on what type of ID you entered in the previous step. The user ID or the group ID is added to the list on the left side of the window.
6. Ensure that the **None** check box is not selected.

7. Grant configuration database authority to the user ID or the group ID by selecting the authority name that is listed in the **Configuration Database Authorities** section. The minimum authority requirement for accessing the audit log is READ.
8. Click **Save Change**.

The user ID or the group ID has required authority to use appropriate operations on the audit log.

Related tasks:

"Viewing authority settings for accessing audit log" on page 131

Granting authorities for viewing, deleting, or modifying schedules to a user or group

To grant the authority for viewing, deleting, or modifying schedules to a user ID or a group ID, do the following steps:

1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, "Creating another user ID with equivalent authorities as sysadmin," on page 263.
2. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
3. In the Defined View, right-click the configured system group that is associated with the scheduled action and click **Schedules** > **View**. The Scheduled Action Report window is displayed.

   For information about how to create a schedule, see "Scheduling an action" on page 198.
4. Select a scheduled action by clicking the row where the action is listed in the report, and click **Grant Authorities**. The Grant Authorization window is displayed.
5. In the Grant Authorization window, do one of the following steps, depending on whether the ID already exists in the list on the left side of the window:
   - If the user ID or the group ID exists, click the ID in the list.
   - If the user ID or the group ID does not exist, do the following steps to add the ID to the list:
     a. In the field on the right side of the window, enter the user ID or group ID that you want to grant authority to.
     b. Click **Assign User** or **Assign Group** depending on what type of ID you entered in the previous step. The user ID or the group ID is added to the list on the left side of the window.
6. Ensure that the **None** check box is not selected.
7. Grant configuration database authority to the user ID or the group ID by selecting the authority name that is listed in the **Configuration Database Authorities** section. The minimum authority requirement for accessing the audit log is READ. Different authorities are required to view, modify, or delete a schedule.
   - For viewing a schedule, the minimum authority requirement is READ.
   - For modifying a schedule, the minimum authority requirement is UPDATE.
   - For deleting a schedule, the minimum authority requirement is DELETE.

Remember: The creator of a schedule always has full access to the schedule.

8. Click **Save Change**.

The user ID or the group ID has required authority to use appropriate operations on the schedule.

Related tasks:

"Viewing authority settings for scheduled actions" on page 132

Viewing authority settings of an object

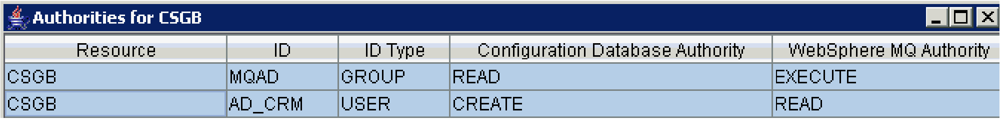
To view the access authorities that you have on an object, do the following steps:

1. In the Configuration view, click **Defined and Prototype**. The Defined and Prototype View opens.
2. Right-click the object for which you want to view its authority settings and click **Granular Security** > **View authorization**. The Authorities window is displayed, listing the access authorities that you have on this object.

Viewing authority settings for backing up the configuration database

To view the authority settings for backing up the configuration database, do the following steps:

1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, "Creating another user ID with equivalent authorities as sysadmin," on page 263.
2. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
3. To the right of the **Update mode** check box, click **Authorities**. The Authorities window that is similar as Figure 52 is displayed.



Resource	ID	ID Type	Configuration Database Authority	WebSphere MQ Authority
CSGB	MQAD	GROUP	READ	EXECUTE
CSGB	AD_CRM	USER	CREATE	READ

Figure 52. Authority settings window

In this Authorities window, the ID, to which the related authority is already granted, is listed in a table. You can check the following properties of a specific ID:

- ID Type: Indicates whether the ID is a user ID or a group ID.
- DB Authority: Indicates the authority that is granted to the ID for the configuration database.
- WMQ Authority: Indicates the authority that is granted to the ID for the WebSphere MQ environment.

4. To modify the authority settings for a specific ID, do the following steps:
   a. Click the row where the ID that you want to modify or delete is listed.
   b. Click **Modify**. The Grant Authorization window is displayed.
   c. In the Grant Authorization window, modify the authority settings as you require and click **Save Change** to close the Grant Authorization window.

d. To update the authority settings, in the Authorities window, click **Refresh** .
5. To delete the authority settings for a specific ID, do the following steps:
   a. Click the row where the ID that you want to modify or delete is listed.
   b. Click **Delete**.
   c. To confirm the deletion, click **OK**.
6. To close the Authorities window, click **Close**.

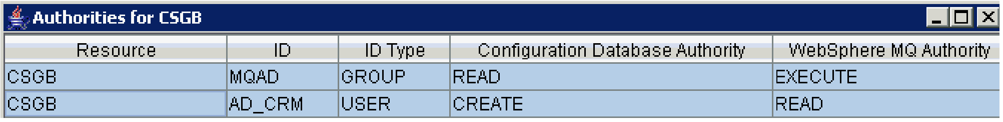
Related tasks:

"Granting authorities for backing up the configuration database to a user or group" on page 126

Viewing authority settings for global variables

Log on to the Tivoli Enterprise Portal Server as sysadmin or another user ID with equivalent authorities.

To view the authority settings for the global variables, do the following steps:
1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, "Creating another user ID with equivalent authorities as sysadmin," on page 263.
2. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
3. In the Configuration view, click **Global Variables**. The Global Variables workspace is displayed on the right side of the Configuration view.
4. Click **View Authorities**. The Authorities window that is similar as Figure 53 is displayed.



Resource	ID	ID Type	Configuration Database Authority	WebSphere MQ Authority
CSGB	MQAD	GROUP	READ	EXECUTE
CSGB	AD_CRM	USER	CREATE	READ

Figure 53. Authority settings window

In this Authorities window, the ID, to which the related authority is already granted, is listed in a table. You can check the following properties of a specific ID:
- ID Type: Indicates whether the ID is a user ID or a group ID.
- DB Authority: Indicates the authority that is granted to the ID for the configuration database.
- WMQ Authority: Indicates the authority that is granted to the ID for the WebSphere MQ environment.

5. To modify the authority settings for a specific ID, do the following steps:
   a. Click the row where the ID that you want to modify or delete is listed.
   b. Click **Modify**. The Grant Authorization window is displayed.
   c. In the Grant Authorization window, modify the authority settings as you require and click **Save Change** to close the Grant Authorization window.
   d. To update the authority settings, in the Authorities window, click **Refresh** .
6. To delete the authority settings for a specific ID, do the following steps:
   a. Click the row where the ID that you want to modify or delete is listed.

b. Click **Delete**.

c. To confirm the deletion, click **OK**.

7. To close the Authorities window, click **Close**.

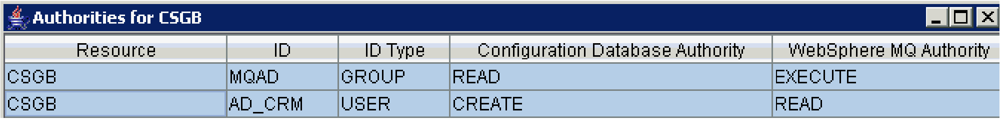
Related tasks:

"Granting authorities for adding, deleting, or modifying global variables to a user or group" on page 126

Viewing authority settings for accessing audit log

To view the authority settings for the accessing audit log, do the following steps:

1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, "Creating another user ID with equivalent authorities as sysadmin," on page 263.
2. Ensure that you are in update mode. See "Entering update mode" on page 18 for information about how to enter update mode.
3. In the Configuration view, click **Audit Log**. The Audit Log workspace is displayed on the right side of the Configuration view.
4. Click **View Authorities**. The Authorities window that is similar as Figure 54 is displayed.



Authorities for CSGB

Resource	ID	ID Type	Configuration Database Authority	WebSphere MQ Authority
CSGB	MQAD	GROUP	READ	EXECUTE
CSGB	AD_CRM	USER	CREATE	READ

Figure 54. Authority settings window

In this Authorities window, the ID, to which the related authority is already granted, is listed in a table. You can check the following properties of a specific ID:

- ID Type: Indicates whether the ID is a user ID or a group ID.
- DB Authority: Indicates the authority that is granted to the ID for the configuration database.
- WMQ Authority: Indicates the authority that is granted to the ID for the WebSphere MQ environment.

5. To modify the authority settings for a specific ID, do the following steps:
   a. Click the row where the ID that you want to modify or delete is listed.
   b. Click **Modify**. The Grant Authorization window is displayed.
   c. In the Grant Authorization window, modify the authority settings as you require and click **Save Change** to close the Grant Authorization window.
   d. To update the authority settings, in the Authorities window, click **Refresh** .
6. To delete the authority settings for a specific ID, do the following steps:
   a. Click the row where the ID that you want to modify or delete is listed.
   b. Click **Delete**.
   c. To confirm the deletion, click **OK**.
7. To close the Authorities window, click **Close**.

Related tasks:

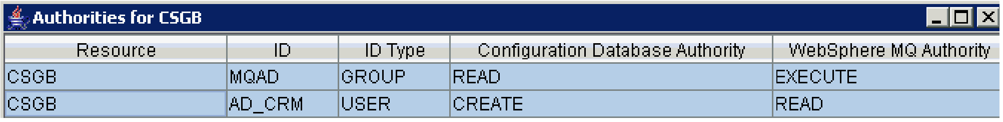
"Granting authorities for accessing audit log to a user or group" on page 127

Viewing authority settings for scheduled actions

To view the authority settings for scheduled actions, do the following steps:

1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, “Creating another user ID with equivalent authorities as sysadmin,” on page 263.
2. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
3. In the Defined View, right-click the configured system group that is associated with the scheduled action and click **Schedules** > **View**. The Scheduled Action Report window is displayed.

   For information about how to create a schedule, see “Scheduling an action” on page 198.
4. Select a scheduled action by clicking the corresponding row in the report. The Authorities window is displayed.
5. Click **View Authorization**. The Authorities window that is similar as Figure 55 is displayed.



Resource	ID	ID Type	Configuration Database Authority	WebSphere MQ Authority
CSGB	MQAD	GROUP	READ	EXECUTE
CSGB	AD_CRM	USER	CREATE	READ

Figure 55. Authority settings window

   In this Authorities window, the ID, to which the related authority is already granted, is listed in a table. You can check the following properties of a specific ID:
   - ID Type: Indicates whether the ID is a user ID or a group ID.
   - DB Authority: Indicates the authority that is granted to the ID for the configuration database.
   - WMQ Authority: Indicates the authority that is granted to the ID for the WebSphere MQ environment.
6. To modify the authority settings for a specific ID, do the following steps:
   a. Click the row where the ID that you want to modify or delete is listed.
   b. Click **Modify**. The Grant Authorization window is displayed.
   c. In the Grant Authorization window, modify the authority settings as you require and click **Save Change** to close the Grant Authorization window.
   d. To update the authority settings, in the Authorities window, click **Refresh** .
7. To delete the authority settings for a specific ID, do the following steps:
   a. Click the row where the ID that you want to modify or delete is listed.
   b. Click **Delete**.
   c. To confirm the deletion, click **OK**.
8. To close the Authorities window, click **Close**.

Related tasks:

“Granting authorities for viewing, deleting, or modifying schedules to a user or group” on page 128

Changing authority settings for an object

After you grant access authorities for an object to a user or a group, you can change the authority settings for the object. For example, add a user who can delete the object, or modify the existing authority of an ID.

To change the authority settings for an object, do the following steps:

1. Log on to the Tivoli Enterprise Portal using the sysadmin ID or another user ID with equivalent authorities. For information about how to create another user ID, see Appendix C, “Creating another user ID with equivalent authorities as sysadmin,” on page 263.
2. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
3. In the Configuration view, click **Defined and Prototype**. The Defined and Prototype View is displayed. The defined view tree and prototype view tree are positioned and sized so that you can drag objects between them.
4. Right-click the object for which you want to change authority settings and click **Granular Security** > **View authorization**. The Authorities window is displayed.
5. Select the row that you want to modify and click **Modify**. The Grant Authorization window is displayed.
6. Select the authority name in the **Configuration Database Authorities** section to grant configuration database authority to the user ID or the group ID.
7. Select the authority name in the **WebSphere MQ Authorities** section to grant WebSphere MQ authority to the user ID or the group ID.
8. To save your changes and close the window, click **Save change** .

Behavior scenarios

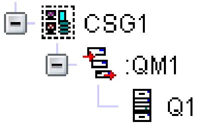
As a system administrator, you can use the behavior scenarios in this section to determine the following things:

- The process that the WebSphere MQ Configuration agent uses to check the authority settings
- The minimum security requirements of some basic operations, such as modifying an object attribute, deleting an object, and creating an object
- How the relationship between the user ID and the group ID works in authority settings

Scenario: Authorizing a user to modify an object attribute in the Defined View

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to modify the attribute of an object in the Defined View.

The existing defined view tree structure is displayed in the following figure. There is one queue manager named QM1 listed in the CSG1 configured system group. The QM1 queue manager has one Q1 resource.



There is one user named user_1 in the group_1 ID in the system.

In this scenario, the user wants to modify the attribute of the Q1 resource.

For the operation to be approved by the WebSphere MQ Configuration agent, the administrator must grant UPDATE authority (configuration database) of the related objects to the user.

For information about how to grant access authorities to a user ID or a group ID, see “Granting access authorities for an object to a user ID” on page 117 and “Granting access authorities for an object to a group ID” on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to UPDATE for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant UPDATE authority for the CSG1 configured system to the user_1 ID or the group_1 ID.
- If no authority for the CSG1 configured system group is specified for the user_1 ID or the group_1 ID, set the default access level to UPDATE for the configuration database.

When the security checking level is set to Configured system

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

The operation is approved in one of the following circumstances:

- You grant UPDATE authority for the QM1 configured system to the user_1 ID or the group_1 ID.
- If no authority for the QM1 configured system is specified for the user_1 ID or the group_1 ID, you grant UPDATE authority for the CSG1 configured system to the user_1 ID or the group_1 ID.
- If no authority for the QM1 configured system and the CSG1 configured system group is specified for the user_1 ID or the group_1 ID, set the default access level to UPDATE for the configuration database.

When the security checking level is set to Resource group

The WebSphere MQ Configuration agent starts to check the authority settings on the resource group level. There is no resource group in the tree structure, the WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

The operation is approved in one of the following circumstances:

- You grant UPDATE authority for the QM1 configured system to the user_1 ID or the group_1 ID.
- If no authority for the QM1 configured system is specified for the user_1 ID or the group_1 ID, you grant UPDATE authority for the CSG1 configured system to the user_1 ID or the group_1 ID.
- If no authority for the QM1 configured system and the CSG1 configured system group is specified for the user_1 ID or the group_1 ID, set the default access level to UPDATE for the configuration database.

When the security checking level is set to Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the resource level.

The operation is approved in one of the following circumstances:

- You grant UPDATE authority for the Q1 resource to the user_1 ID or the group_1 ID.
- If no authority for the Q1 resource is specified for the user_1 ID or the group_1 ID, you grant UPDATE authority for the QM1 configured system to the user_1 ID or the group_1 ID.
- If no authority for the Q1 resource and the QM1 configured system is specified for the user_1 ID or the group_1 ID, you grant UPDATE authority for the CSG1 configured system to the user_1 ID or the group_1 ID.
- If no authority for the following objects is specified for the user_1 ID or the group_1 ID, set the default access level to UPDATE for the configuration database.
  - Q1 resource
  - QM1 configured system
  - CSG1 configured system group

Example for authorizing a user to modify an object attribute in the Defined View

In the following example, the system administrator grants to the user_1 ID, DELETE authority for the QM1 configured system and NONE authority for the CSG1 configured system group. The administrator grants to the group_1 ID, DELETE authority for the Q1 resource and UPDATE authority for the CSG1 configured system group. The default access level is set to READ to both the configuration database and WebSphere MQ.

Table 5. Authority settings

ID	Object	Authority
user_1	QM1 configured system	DELETE
	CSG1 configured system group	NONE

Table 5. Authority settings (continued)

ID	Object	Authority
group_1	Q1 resource	DELETE
	CSG1 configured system group	UPDATE
all users	Default access level to configuration database	READ
all users	Default access level to WebSphere MQ environment	READ

- When the security checking level is set to NONE, the default access level (READ) is used. The operation is denied because the user only has READ authority for the configuration database.
- When the security checking level is set to Configured system group, the operation is approved. Because the group_1 ID is granted UPDATE authority for the CSG1 configured system group.

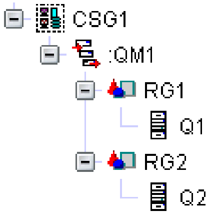
  Remember: Although the user_1 ID has NONE authority for the CSG1 configured system group, the group_ID has UPDATE authority for the CSG1 configured system group. The WebSphere MQ Configuration agent will approve the operation, if appropriate authority is granted to either the user_ID or the group_ID, regardless of the authority conflict.
- When the security checking level is set to Configured system, the operation is approved. This is because the user_1 ID is granted DELETE authority for the QM1 configured system, which is higher than the required UPDATE authority.
- When the security checking level is set to Resource group, the operation is approved. This is because the user_1 ID is granted DELETE authority for the QM1 configured system, which is higher than the required UPDATE authority.
- When the security checking level is set to Resource, the operation is approved. This is because the group_1 ID is granted DELETE authority for the Q1 resource, which is higher than the required UPDATE authority.

Scenario: Authorizing a user to create a queue in the Defined view

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to create a queue in a resource group in the Defined View.

Remember: When a user wants to create an object in the Defined View, you must grant the user CREATE authority for the object, to which the newly created object belongs.

The existing defined view tree structure is displayed in the following figure. There is one queue manager named QM1 listed in the CSG1 configured system group; the QM1 queue manager has two resource groups named RG1 and RG2; there is one queue named Q1 in the RG1 resource group and one queue named Q2 in the RG2 resource group.



The relationship between user IDs and group IDs in the system is explained in the following table. There are two user IDs named user_1 and user_2, and one group ID named group_1 in the system. The user_1 ID belongs to the group_1 ID, and the user_2 ID does not belong to any group ID.

Table 6. The relationship between the user ID and the group ID in this scenario

User ID	Group ID
user_1	group_1
user_2	N/A

In this scenario, the user wants to create a queue named Q3 in the RG2 resource group.

The operation is to create an object. The target object is a resource, and the parent object that the target object belongs to is a resource group. The WebSphere MQ Configuration agent compares security checking level with the resource group, and starts checking authority from the higher level.

For the operation to be approved by the WebSphere MQ Configuration agent, the user must have CREATE authority (configuration database) for the related objects.

For information about how to grant access authorities to a user ID or a group ID, see "Granting access authorities for an object to a user ID" on page 117 and "Granting access authorities for an object to a group ID" on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. For the user_1 ID and user_2 ID, the operation is approved when the default access level is set to CREATE for the configuration database, and the default access level to WebSphere MQ is not set to NONE.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

- For the user_1 ID, the operation is approved in one of the following circumstances:
  - You grant CREATE authority for the CSG1 configured system group to the user_1 ID or the group_1 ID.
  - If no authority for the CSG1 configured system group is specified for the user_1 ID or the group_1 ID, set the default access level to CREATE for the configuration database, and the default access level for WebSphere MQ environment to any value other than NONE.

- For the user_2 ID, the operation is approved in one of the following circumstances:
  - You grant CREATE authority for the CSG1 configured system group to the user_2 ID.
  - If no authority for the CSG1 configured system group is specified for the user_2 ID, set the default access level to CREATE for the configuration database, and the default access level to WebSphere MQ environment to any value other than NONE.

When the security checking level is set to Configured system

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

- For the user_1 ID, the operation is approved in one of the following circumstances:
  - You grant CREATE authority for the QM1 configured system to the user_1 ID or the group_1 ID.
  - If no authority for the QM1 configured system is specified for the user_1 ID or the group_1 ID, you grant CREATE authority for the CSG1 configured system group to the user_1 ID or the group_1 ID.
  - If no authority for the following objects is specified for the user_1 ID or the group_1 ID, set the default access level to CREATE for the configuration database, and the default access level for WebSphere MQ environment to any value other than NONE.
    - QM1 configured system
    - CSG1 configured system group
- For the user_2 ID, the operation is approved in one of the following circumstances:
  - You grant CREATE authority for the QM1 configured system to the user_2 ID.
  - If no authority for the QM1 configured system is specified for the user_2 ID, you grant CREATE authority for the CSG1 configured system group to the user_2 ID.
  - If no authority for the following objects is specified for the user_2 ID, set the default access level to CREATE for the configuration database, and the default access level for WebSphere MQ environment to any value other than NONE.
    - QM1 configured system
    - CSG1 configured system group

When the security checking level is set to Resource group or Resource

When the security checking level is set to Resource group, the WebSphere MQ Configuration agent starts to check the authority settings on the resource group level.

When the security checking level is set to Resource, which is lower than resource group, the WebSphere MQ Configuration agent starts to check the authority settings on the resource group level.

- For the user_1 ID, the operation is approved in one of the following circumstances:
  - You grant CREATE authority for the RG2 resource group to the user_1 ID or the group_1 ID.

  - If no authority for the RG2 resource group is specified for the user_1 ID or the group_1 ID, you grant CREATE authority for the QM1 configured system to the user_1 ID or the group_1 ID.
  - If no authority for the following objects is specified for the user_1 ID or the group_1 ID, you grant CREATE authority for the CSG1 configured system group to the user_1 ID or the group_1 ID:
    - RG2 resource group
    - QM1 configured system
  - If no authority for the following objects is specified for the user_1 ID or the group_1 ID, set the default access level to CREATE for the configuration database, and the default access level for WebSphere MQ environment to any value other than NONE:
    - RG2 resource group
    - QM1 configured system
    - CSG1 configured system group
- For the user_2 ID, the operation is approved in one of the following circumstances:
  - You grant CREATE authority for the RG2 resource group to the user_2 ID.
  - If no authority for the RG2 resource group is specified for the user_2 ID, you grant CREATE authority for the QM1 configured system to the user_2 ID.
  - If no authority for the following objects is specified for the user_2 ID, you grant CREATE authority for the CSG1 configured system group to the user_2 ID:
    - RG2 resource group
    - QM1 configured system
  - If no authority for the following objects is specified for the user_2 ID, set the default access level to CREATE for the configuration database, and the default access level for WebSphere MQ environment to any value other than NONE:
    - RG2 resource group
    - QM1 configured system
    - CSG1 configured system group

Example for authorizing a user to create a queue in the Defined View

The user wants to create a queue named Q3 in the RG2 resource group. In the following example, the system administrator grants to the user_1 ID, CREATE authority for RG2 resource group and READ authority for CSG1 configured system group. The administrator grants to the group_1 ID, UPDATE authority for the QM1 configured system; to the user_2 ID, the administrator grants CREATE authority for the QM1 configured system and READ authority for the RG2 resource group. The default access level is set to READ to both the configuration database and WebSphere MQ environment.

Table 7. Authority settings

ID	Object	Authority
user_1	RG2 resource group	CREATE
	CSG1 configured system group	READ
group_1	QM1 configured system	UPDATE

Table 7. Authority settings (continued)

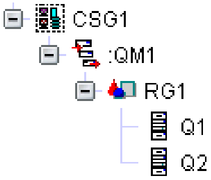
ID	Object	Authority
user_2	RG2 resource group	READ
	QM1 configured system	CREATE
all users	Default access level to configuration database	READ
all users	Default access level to WebSphere MQ environment	READ

- When the security checking level is set to NONE, the default access level (READ) is used. Both the user_1 operation and the user_2 operation are denied, because the default access level is READ for the configuration database.
- When the security checking level is set to Configured system group, both the user_1 operation and the user_2 operation are denied. This is because the user_1 ID only has READ authority of the CSG1 configured system group, and the default access level (READ) is used for the user_2 ID.
- When the security checking level is set to Configured system, the user_1 operation is denied and the user_2 operation is approved. This is because the group_1 ID only has UPDATE authority of the QM1 configured system, and the user_2 ID has CREATE authority of the QM1 configured system.
- When the security checking level is set to Resource group, the user_1 operation is approved and the user_2 operation is denied. This is because the user_1 ID has CREATE authority for the RG2 resource group, and the user_2 ID only has READ authority of the RG2 resource group.
- When the security checking level is set to Resource, the user_1 operation is approved and the user_2 operation is denied. This is because the user_1 ID has CREATE authority for the RG2 resource group, and the user_2 ID only has READ authority for the RG2 resource group.

Scenario: Authorizing a user to delete a queue manager in the Defined View

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to delete a queue manager in the Defined View.

The existing tree structure is displayed in the following figure. There is one queue manager named QM1 listed in the CSG1 configured system group; the QM1 queue manager has one resource group, RG1. The RG1 resource group has two queues named Q1 and Q2.



There is one user named user_1 in the group_1 ID in the system.

In this scenario, the user_1 ID wants to delete the QM1 queue manager from the configuration database.

For the operation to be approved by the WebSphere MQ Configuration agent, the administrator must grant UPDATE authority for the CSG1 configured system group, DELETE authority for the QM1 configured system and for all resources within the configured system to the user ID.

For information about how to grant access authorities to a user ID or a group ID, see "Granting access authorities for an object to a user ID" on page 117 and "Granting access authorities for an object to a group ID" on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent does not check the authority settings, and the default access setting is used. For the user_1 ID, the operation is approved when the default access is set to DELETE for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:
- You grant DELETE authority for the CSG1 configured system group to the user_1 ID or the group_1 ID.
- If no authority for the CSG1 configured system group is specified for the user_1 ID or the group_1 ID, the default access is set to DELETE for the configuration database.

When the security checking level is set to Configured system

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

The operation is approved in one of the following circumstances:
- You grant UPDATE authority for the CSG1 configured system group and DELETE authority for the QM1 configured system to the user_1 ID or the group_1 ID.
- If no authority for the QM1 configured system is specified for the user_1 ID or the group_1 ID, you grant DELETE authority for the CSG1 configured system group to the user_1 ID or the group_1 ID.
- If no authority for the QM1 configured system and CSG1 configured system group is specified for the user_1 ID or the group_1 ID, the default access is set to DELETE for the configuration database.

When the security checking level is set to Resource group

The WebSphere MQ Configuration agent starts to check the authority settings on the resource group level.

The operation is approved in one of the following circumstances:
- You grant UPDATE authority for the CSG1 configured system group, and DELETE authority for the RG1 and QM1 objects to the user_1 ID or the group_1 ID.

- If no authority for the RG1 resource group is specified for the user_1 ID or the group_1 ID, you grant UPDATE authority for the CSG1 configured system group and DELETE authority for the QM1 configured system to the user_1 ID or the group_1 ID.
- If no authority for the RG1 resource group and QM1 configured system is specified for the user_1 ID or the group_1 ID, you grant DELETE authority for the CSG1 configured system group to the user_1 ID or the group_1 ID.
- If no authority for the following objects is specified for the user_1 ID or the group_1 ID, the default access is set to DELETE for the configuration database.
  - RG1 resource group
  - QM1 configured system
  - CSG1 configured system group

When the security checking level is set to Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the resource level.

The operation is approved in one of the following circumstances:

- You grant UPDATE authority for the CSG1 configured system group, and DELETE authority for the Q1, Q2, RG1, and QM1 objects to the user_1 ID or the group_1 ID:
- If no authority for the Q1 or Q2 resource is specified for the user_1 ID or the group_1 ID, you grant UPDATE authority for the CSG1 configured system group, and DELETE authority for the RG1 and QM1 objects to the user_1 ID or the group_1 ID:
- If no authority for the following objects is specified for the user_1 ID or the group_1 ID, you grant UPDATE authority for the CSG1 configured system group and DELETE authority for the QM1 configured system to the user_1 ID or the group_1 ID:
  - Q1 or Q2 resource
  - RG1 resource group
- If no authority for the following objects is specified for the user_1 ID or the group_1 ID, you grant DELETE authority for the CSG1 configured system to the user_1 ID or the group_1 ID:
  - Q1 or Q2 resource
  - RG1 resource group
  - QM1 configured system
- If no authority for the following objects is specified for the user_1 ID or the group_1 ID, the default access is set to DELETE for the configuration database:
  - Q1 or Q2 resource
  - RG1 resource group
  - QM1 configured system
  - CSG1 configured system group

Example for authorizing a user to delete a queue manager in the Defined View

In the following example, the system administrator grants to the user_1 ID, READ authority for the Q1 resource and QM1 configured system, DELETE authority for the Q2 resource and RG1 resource group, and UPDATE authority for the CSG1 configured system. The administrator grants to the group_1 ID, DELETE authority for the QM1 configured system, and READ authority for the CSG1 configured system group. The default access level is set to DELETE to the configuration database.

Table 8. Authority settings

ID	Object	Authority
user_1	Q1 resource	READ
	Q2 resource	DELETE
	RG1 resource group	DELETE
	QM1 configured system	READ
	CSG1 configured system group	UPDATE
group_1	QM1 configured system	DELETE
	CSG1 configured system group	READ
all users	Default access level to configuration database	DELETE

- When the security checking level is set to NONE, the default access level (DELETE) is used. The operation is approved, because the user has DELETE authority for the configuration database.
- When the security checking level is set to Configured system group, the operation is denied. This is because the user_1 ID only has UPDATE authority for the CSG1 configured system group, and the group_1 ID only has READ authority for the CSG1 configured system group. The required minimum authority is DELETE.
- When the security checking level is set to Configured system, the operation is approved. This is because the user_1 ID has UPDATE authority for the CSG1 configured system group, and the group_1 ID is granted DELETE authority for the QM1 configured system.

  Remember: Although the user_1 ID only has READ authority for the QM1 configured system, the group_ID has DELETE authority for the QM1 configured system. The WebSphere MQ Configuration agent approves the operation, if appropriate authority is granted to either the user_ID or the group_ID, regardless of the authority conflict.
- When the security checking level is set to Resource group, the operation is approved. This is because the user_1 ID has UPDATE authority for the CSG1 configured system group, and DELETE authority for the RG1 resource group. The group_1 ID is granted DELETE authority for the QM1 configured system.
- When the security checking level is set to Resource, the operation is denied. This is because the user_1 ID only has READ authority for the Q1 resource.

Scenario: Authorizing a user to use the Update function to synchronize defined resources with actual resources in the WebSphere MQ environment

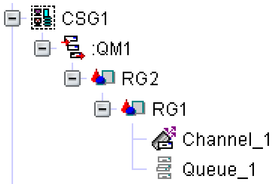
As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs who wants to use the Update function to synchronize defined resources with actual resources in the WebSphere MQ environment.

The authority requirements for the Update function for synchronization vary, depending on what level the function is used, and the differences between the configuration database and WebSphere MQ environment. For example, if the Update function is used on the configured system level, there might be the following three types of changes in the configuration database:

- The actual resources that do not exist in the configuration database are created.
- The defined resources that do not exist in the actual WebSphere MQ environment are deleted from the configuration database.
- The defined resources that have counterparts in the actual WebSphere MQ environment with different attributes are synchronized as the actual resources in the actual WebSphere MQ environment.

Therefore, for the operation to be approved by the WebSphere MQ Configuration agent, the corresponding DELETE, CREATE, or UPDATE authorities are required.

The existing hierarchical structure in the Defined View is shown in the following figure. There is one queue manager named QM1 listed in the CSG1 configured system group. The QM1 queue manager has a RG2 resource group. The RG2 resource group has a RG1 resource group. The RG1 resource group contains two resources, Channel_1 and Queue_1. The **default message priority** attribute of the Queue_1 resource is set to 4.



CSG1
:QM1
RG2
RG1
Channel_1
Queue_1

In the actual WebSphere MQ environment, there is a QM1 queue manager. The QM1 queue manager has two resources, Listener_1 and Queue_1. The **default message priority** attributes of the Queue_1 and the Listener_1 resources are set to 0.

There is one user named user_1 in the system.

In this scenario, the user_1 ID wants to use the Update function on the QM1 configured system to synchronize defined resources with actual resources. If the operation is approved, the user_1 ID can delete the Channel_1 resource, create the Listener_1 resource, and update the Queue_1 resource.

For information about how to grant access authorities to a user ID or a group ID, see “Granting access authorities for an object to a user ID” on page 117 and “Granting access authorities for an object to a group ID” on page 119.

Tip: To fully synchronize resources in the configuration database and the WebSphere MQ environment, use the Update function on the resource level or on the configured system level. If the Update function is used on the resource group level, only the differences between the resources that exists both in the actual WebSphere MQ environment and the configuration database can be synchronized. Because the WebSphere MQ Configuration agent cannot determine whether the resource with the same name exists in another resource group, newly discovered resource from the WebSphere MQ environment cannot be created. Also, the existing resource in the configuration database cannot be deleted if the resource does not exist in the WebSphere MQ environment.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to DELETE for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant DELETE authority for the CSG1 configured system to the user_1 ID.
- If no authority for the CSG1 configured system is specified for the user_1 ID, the default access level is set to DELETE for the configuration database.

When the security checking level is set to Configured system

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

The operation is approved in one of the following circumstances:

- You grant DELETE authority for the QM1 configured system to the user_1 ID.
- If no authority for the QM1 configured system is specified for the user_1 ID, you grant DELETE authority for the CSG1 configured system to the user_1 ID.
- If no authority for the QM1 configured system and the CSG1 configured system group is specified for the user_1 ID, the default access level is set to DELETE for the configuration database.

When the security checking level is set to Resource group

The WebSphere MQ Configuration agent starts to check the authority settings on the resource group level.

The operation is approved in one of the following circumstances:

- You grant DELETE authority for the RG1 resource group to the user_1 ID.
- If no authority for the RG1 resource group is specified for the user_1 ID, you grant DELETE authority for the RG2 resource group to the user_1 ID.
- If no authority for the RG1 and RG2 resource groups is specified for the user_1 ID, you grant DELETE authority for the QM1 configured system.
- If no authority for the following objects is specified for the user_1 ID, you grant DELETE authority to the CSG1 configured system group:
  - RG1 resource group
  - RG2 resource group
  - QM1 configured system
- If no authority for the following objects is specified for the user_1 ID, the default access level is set to DELETE for the configuration database:
  - RG1 resource group
  - RG2 resource group
  - QM1 configured system
  - CSG1 configured system group

When the security checking level is set to Resource

For the Channel_1 and the Queue_1 resources, the WebSphere MQ Configuration agent starts to check the authority settings on the resource level. For the Listener_1 resource, the WebSphere MQ Configuration agent starts to check the authority settings on the resource group level.

The operation is approved in one of the following circumstances:

- You grant DELETE authority for the Channel_1 resource, UPDATE authority for the Queue_1 resource, and CREATE authority for the RG1 resource group to the user_1 ID.
- If no authority for the Queue_1 resource is specified, you grant DELETE authority for the Channel_1 resource and CREATE authority for the RG1 resource group to the user_1 ID.
- If no authority for the Channel_1 resource is specified, you grant UPDATE authority for the Queue_1 resource and DELETE authority for the RG1 resource group to the user_1 ID.
- If no authority for the Queue_1 and Channel_1 resources is specified for the user_1 ID, you grant DELETE authority for the RG1 resource group to the user_1 ID.
- If no authority for the following objects is specified for the user_1 ID, you grant DELETE authority for the RG2 resource group:
  - Channel_1 resource
  - Queue_1 resource
  - RG1 resource group
- If no authority for the following objects is specified for the user_1 ID, you grant DELETE authority to the QM1 configured system:
  - Channel_1 resource
  - Queue_1 resource
  - RG1 resource group
  - RG2 resource group
- If no authority for the following objects is specified for the user_1 ID, you grant DELETE authority to the CSG1 configured system group:
  - Channel_1 resource
  - Queue_1 resource
  - RG1 resource group
  - RG2 resource group
  - QM1 configured system
- If no authority for the following objects is specified for the user_1 ID, the default access level is set to DELETE for the configuration database:
  - Channel_1 resource
  - Queue_1 resource
  - RG1 resource group
  - RG2 resource group
  - QM1 configured system
  - CSG1 configured system group

Example for authorizing a user to use the Update function to synchronize defined resources with actual resources in the WebSphere MQ environment

In the following example, the system administrator grants the following authorities to the user_1 ID. The default access level is set to READ for both the configuration database and WebSphere MQ environment.

- UPDATE authority for Queue_1 resource
- CREATE authority for RG1 resource group
- UPDATE authority for RG2 resource group
- DELETE authority for QM1 configured system
- UPDATE authority for CSG1 configured system group

Table 9. Authority settings

ID	Object	Authority
user_1	Queue_1 resource	UPDATE
	RG1 resource group	CREATE
	RG2 resource group	UPDATE
	QM1 configured system	DELETE
	CSG1 configured system group	UPDATE
all users	Default access level to configuration database	READ
all users	Default access level to WebSphere MQ environment	READ

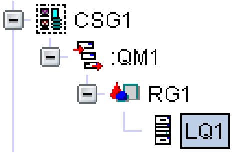
- When the security checking level is set to NONE, the default access level (READ) is used. The operation is denied because the user only has READ authority for the configuration database.
- When the security checking level is set to Configured system group, the operation is approved partially. The Queue_1 resource is modified, the Listener_1 resource cannot be created, and the Channel_1 resource is not deleted. This is because the user_1 ID only has UPDATE authority for the CSG1 configured system group.
- When the security checking level is set to Configured system, the operation is approved. This is because the user_1 ID has the DELETE authority for the QM1 configured system.
- When the security checking level is set to Resource group, the operation is approved partially. The Queue_1 resource is updated, the Listener_1 resource is created, but the Channel_1 resource cannot be deleted. This is because the granted authority for the RG1 resource group is CREATE, which is higher than the required UPDATE authority to modify the Queue_1 resource, and lower than the required DELETE authority to delete the Channel_1 resource.
- When the security checking level is set to Resource, the operation is approved partially. The Queue_1 resource is modified, because the user_1 ID has UPDATE authority for the Queue_1 resource. The Listener_1 resource is created, because the user_1 ID has the CREATE authority for the RG1 resource group. However, the Channel_1 resource cannot be deleted, because no authority for the Channel_1 resource is granted, and the granted authority for the RG1 resource group (CREATE) is lower than the required minimum DELETE authority.

Scenario: Authorizing a user to use the Update function to synchronize actual resources with defined resources in the configuration database

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to use the Update function to synchronize actual resources with defined resources in the configuration database.

This Update function changes the actual WebSphere MQ resource to match the defined version in the configuration database. If any differences exist, the actual resource is changed to match the defined version. If an actual resource exists that has no defined counterpart in the configuration database, the actual resource is deleted. If a defined resource exists that has no counterpart in the actual WebSphere MQ environment, the actual resource is created. Therefore, for the Update operation to be approved by the WebSphere MQ Configuration agent, the user must have the READ authority or higher for the configuration database and EXECUTE authority or higher for the actual WebSphere MQ environment.

The following figure shows the existing hierarchical structure in the Defined View. The QM1 queue manager is contained in the CSG1 configured system group. QM1 has a resource group named RG1. The RG1 resource group contains one local queue named LQ1.



A queue manager named QM1 exists in the actual WebSphere MQ environment, the only difference between this queue manager and its counterpart in the configuration database is that it does not contain a queue named LQ1.

There is one user named user_1 in the system. The user_1 user wants to perform the Update operation against the QM1 queue manager synchronize actual queue manager with its counterpart in the configuration database. If this operation succeeds, a local queue named LQ1 is created in the QM1 queue manager in the actual WebSphere MQ environment.

When the Security checking level is set to None

When the Security checking level is set to None, WebSphere MQ Configuration agent checks only the default access level on the Tivoli Enterprise Monitoring Server to determine if the user_1 has the required access authorities to perform this operation. The operation is approved if you set the default access level for the configuration database to READ and the default access level for WebSphere MQ environment to EXECUTE.

When the Security checking level is set to Configured System Group

Because the operation is performed against the queue manager, which is lower than the security checking level, the WebSphere MQ Configuration agent starts to check the authority settings on the configured system group.

This operation is approved if one of the following conditions is met:

- In the access authority settings for the CSG1 configured system group, you grant user_1 the READ authority for the configuration database and EXECUTE authority for the actual WebSphere MQ environment.
- You do not grant the user_1 user any access authorities for the CSG1 configured system group. Instead, you set the default access level for the configuration database to READ and the default access level for WebSphere MQ environment to EXECUTE.

When the Security checking level is set to Configured System

Because the operation is performed against the queue manager, which is the same as the security checking level, the WebSphere MQ Configuration agent starts to check the authority settings on the configured system (queue manager) level.

The operation is approved if one of the following conditions is met:

- In the access authority settings for the QM1 queue manager, you grant the user_1 user the READ authority for the configuration database and EXECUTE authority for the actual WebSphere MQ environment.
- You do not grant the user_1 user any access authorities for the QM1 queue manager. Instead, in the access authority settings for the CSG1 configured system group, you grant user_1 the READ authority for the configuration database and EXECUTE authority for the actual WebSphere MQ environment.
- You do not grant the user_1 user any access authorities for the QM1 queue manager or the CSG1 configured system group. Instead, you set the default access level for the configuration database to READ and the default access level for WebSphere MQ environment to EXECUTE.

When the Security checking level is set to Resource Group

Because the operation is performed against the queue manager, which is higher than the security checking level, the WebSphere MQ Configuration agent starts to check the authority settings on the configured system (queue manager) level.

The operation is approved if one of the following conditions is met:

- In the access authority settings for the QM1 queue manager, you grant the user_1 user the READ authority for the configuration database and EXECUTE authority for the actual WebSphere MQ environment.
- You do not grant the user_1 user any access authorities for the QM1 queue manager. Instead, in the access authority settings for the CSG1 configured system group, you grant user_1 the READ authority for the configuration database and EXECUTE authority for the actual WebSphere MQ environment.
- You do not grant the user_1 user any access authorities for the QM1 queue manager or the CSG1 configured system group. Instead, you set the default access level for the configuration database to READ and the default access level for WebSphere MQ environment to EXECUTE.

When the Security checking level is set to Resource

Because the operation is performed against the queue manager, which is higher than the security checking level, the WebSphere MQ Configuration agent starts to check the authority settings on the configured system (queue manager) level.

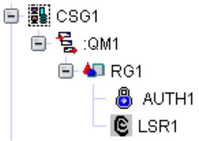
The operation is approved if one of the following conditions is met:

- In the access authority settings for the QM1 queue manager, you grant the user_1 user the READ authority for the configuration database and EXECUTE authority for the actual WebSphere MQ environment.
- You do not grant the user_1 user any access authorities for the QM1 queue manager. Instead, in the access authority settings for the CSG1 configured system group, you grant user_1 the READ authority for the configuration database and EXECUTE authority for the actual WebSphere MQ environment.
- You do not grant the user_1 user any access authorities for the QM1 queue manager or the CSG1 configured system group. Instead, you set the default access level for the configuration database to READ and the default access level for WebSphere MQ environment to EXECUTE.

Scenario: Authorizing a user to drag an object in the Defined view

As a system administrator, you can use this scenario to figure out the minimum authority requirements for a user to drag an object in the Defined View.

The Defined View tree structure is displayed in the following figure. There is a QM1 configured system listed in the CSG1 configured system group. The QM1 configured system has a RG1 resource group. The RG1 resource group has two resources, AUTH1 authentication object and LSR1 listener.



There is one user named user_1 in the system. The user wants to drag the AUTH1 resource from the RG1 resource group to the QM1 configured system.

For the operation to be approved, the user must have the authority to delete the AUTH1 resource and the authority to create resources in the QM1 configured system.

For information about how to grant access authorities to a user ID or a group ID, see “Granting access authorities for an object to a user ID” on page 117 and “Granting access authorities for an object to a group ID” on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved, when the default access level for the configuration database is set to DELETE.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check whether the user_1 ID has DELETE authority for the CSG1 configured system.

The operation is approved in one of the following circumstances:

- You grant DELETE authority for the CSG1 configured system group:
- If no authority for the CSG1 configured system group is specified for the user_1 ID, the default access level for the configuration database is set to DELETE:

When the security checking level is set to Configured system

The WebSphere MQ Configuration agent starts to check whether the user_1 ID has DELETE authority for the QM1 configured system.

The operation is approved in one of the following circumstances:

- You grant DELETE authority for the QM1 configured system to the user_1 ID.
- If no authority for the QM1 configured system is specified for the user_1 ID, you grant DELETE authority for the CSG1 configured system group:
- If no authority for the following objects is specified for the user_1 ID, the default access level for the configuration database is set to DELETE:
  - QM1 configured system
  - CSG1 configured system group

When the security checking level is set to Resource group

The WebSphere MQ Configuration agent starts to check whether the user_1 ID has DELETE authority for the RG1 resource group and CREATE authority for the QM1 configured system.

The operation is approved in one of the following circumstances:

- You grant the following authorities to the user_1 ID:
  - DELETE authority for the RG1 resource
  - CREATE authority for the QM1 configured system in the configuration database
- If no authorities for the RG1 resource group are specified for the user_1 ID, you grant DELETE authority for the QM1 configured system to the user_1 ID.
- If no authority for the following objects is specified for the user_1 ID, you grant DELETE authority for the CSG1 configured system group:
  - RG1 resource group
  - QM1 configured system
- If no authority for the following objects is specified for the user_1 ID, the default access level for the configuration database is set to DELETE:
  - RG1 resource group
  - QM1 configured system
  - CSG1 configured system group

When the security checking level is set to Resource

The WebSphere MQ Configuration agent starts to check whether the user_1 ID has DELETE authority for the AUTH1 resource and CREATE authority for the QM1 configured system.

The operation is approved in one of the following circumstances:

- You grant the following authorities to the user_1 ID:
  - DELETE authority for the AUTH1 resource
  - CREATE authority for the QM1 configured system
- If no authority for the AUTH1 resource is specified, you grant the following authorities to the user_1 ID:
  - DELETE authority for the RG1 resource group

  - CREATE authority for the QM1 configured system
- If no authorities for the AUTH1 resource and the RG1 resource group are specified for the user_1 ID, you grant DELETE authority for the QM1 configured system to the user_1 ID.
- If no authority for the following objects is specified for the user_1 ID, you grant DELETE authority for the CSG1 configured system group:
  - AUTH1 resource
  - RG1 resource group
  - QM1 configured system
- If no authority for the following objects is specified for the user_1 ID, the default access level for the configuration database is set to DELETE:
  - AUTH1 resource
  - RG1 resource group
  - QM1 configured system
  - CSG1 configured system group

Example for authorizing a user to drag an object in the Defined View

In the following example, the system administrator grants the following authorities to the user_1 ID. The default access level is set to DELETE for the configuration database:

- DELETE authority for the AUTH1 resource
- CREATE authority for the QM1 configured system
- CREATE authority for the CSG1 configured system group

Table 10. Authority settings

ID	Object	Authority
user_1	AUTH1 resource	DELETE
	QM1 configured system	CREATE
	CSG1 configured system group	CREATE
all users	Default access level to configuration database	DELETE

- When the security checking level is set to NONE, the operation is approved, because the default access level for the configuration database is set to DELETE.
- When the security checking level is set to Configured system group, the operation is denied. Because the user_1 ID only has CREATE authority for the CSG1 configured system, the AUTH1 resource cannot be deleted from the RG1 resource group first.
- When the security checking level is set to Configured system, the operation is denied. Because the user_1 ID only has CREATE authority for the QM1 configured system, the AUTH1 resource cannot be deleted from the RG1 resource group first.
- When the security checking level is set to Resource group, the operation is denied. Because no authority for the RG1 resource group is specified for the user_1 ID. And the user_1 ID only has CREATE authority for the QM1 configured system, the AUTH1 resource cannot be deleted from the RG1 resource group.

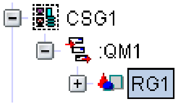
- When the security checking level is set to Resource, the operation is approved, because the user_1 ID has DELETE authority for the AUTH1 resource and CREATE authority for the QM1 configured system.

Scenario: Authorizing a user to drag a resource prototype to a resource group in the Defined View

As a system administrator, you can use this scenario to figure out the minimum authority requirements for a user who wants to drag a resource prototype to a resource group in the Defined View.

This Drag operation creates a resource that is based on the resource prototype in the resource group in the Defined View. Therefore, for the Drag operation to be approved by the WebSphere MQ Configuration agent, the user must have the CREATE authority or higher for the resource group and READ authority or higher for the resource prototype.

The following figure shows the existing hierarchical structure in the Defined View. The QM1 queue manager is contained in the CSG1 configured system group. QM1 has a resource group named RG1.



In the existing hierarchical structure in the Prototype View, a local queue prototype named PRO.LQ1 is contained in the **Resource Prototypes**.

There is one user named user_1 in the system. The user_1 user wants to create a local queue in the RG1 resource group by dragging the PRO.LQ1 prototype to the RG1 resource group. If this operation succeeds, a local queue that is based on the PRO.LQ1 prototype is created in the RG1 resource group in the Defined View.

This Drag operation consists of the following two steps:

1. The definition of the local queue prototype in the configuration database is read.
2. A local queue is created in the RG1 resource group using the definition of the local queue prototype in the configuration database.

For the Drag operation to be approved by the WebSphere MQ Configuration agent, the two steps must both be approved.

Remember: The first step is performed on the prototype object. The concept of the security checking level does not apply to the prototype view. The WebSphere MQ Configuration agent checks the authority settings from the PRO.LQ1 queue prototype directly. If no authority is specified for the current prototype object, the WebSphere MQ Configuration agent checks the authority settings for the prototype object to which the current prototype object belongs. If no authority is specified for all the related prototype objects, the default access level for the configuration database is used.

The first step is approved by the WebSphere MQ Configuration agent if one of the following conditions is met:

- In the access authority settings of the PRO.LQ1 queue prototype, you grant the user_1 user the READ authority of the configuration database.

- You do not grant the user_1 user any access authorities for the PRO.LQ1 queue prototype. Instead, you grant the READ authority for Resource Prototypes to user_1.
- You do not grant the user_1 user any access authorities for the PRO.LQ1 queue prototype or Resource Prototypes. Instead, you set the default access level for the configuration database to READ.

When the Security checking level is set to None

The second step requires that the user_1 user has CREATE authority for the RG1 resource group. Because the security checking level is set to None, WebSphere MQ Configuration agent checks only the default access level for configuration database in the Tivoli Enterprise Monitoring Server. This step is approved if you set the default access level for the configuration database to CREATE.

When the Security checking level is set to Configured System Group

The second step requires that the user_1 user has CREATE authority for the RG1 resource group. Because the Security checking level is set to **Configured System Group**, WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level. The second step is approved if one of the following conditions is met:

- In the access authority settings for the CSG1 configured system group, you grant the user_1 user the CREATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the CSG1 configured system group. Instead, you set the default access level for the configuration database to CREATE.

When the Security checking level is set to Configured System

The second step requires that the user_1 user has CREATE authority for the RG1 resource group. Because the Security checking level is set to **Configured System**, WebSphere MQ Configuration agent starts to check the authority settings on the configured system level. The second step is approved if one of the following conditions is met:

- In the access authority settings for the QM1 queue manager, you grant the user_1 user the CREATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the QM1 queue manager. Instead, in the access authority settings for the CSG1 configured system group, you grant the user_1 user the CREATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the QM1 queue manager or the CSG1 configured system group. Instead, you set the default access level for the configuration database to CREATE.

When the Security checking level is set to Resource Group

The second step requires that the user_1 user has CREATE authority for the RG1 resource group. Because the Security checking level is set to **Resource Group**, WebSphere MQ Configuration agent starts to check the authority settings on the resource group level. The second step is approved if one of the following conditions is met:

- In the access authority settings for the RG1 resource group, you grant the user_1 user the CREATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the RG1 resource group. Instead, in the access authority settings for the QM1 queue manager, you grant the user_1 user the CREATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the RG1 resource group or the QM1 queue manager. Instead, in the access authority settings for the CSG1 configured system group, you grant the user_1 user the CREATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the RG1 resource group, the QM1 queue manager, or the CSG1 configured system group. Instead, you set the default access level for configuration database to CREATE.

When the Security checking level is set to Resource

The second step requires that the user_1 user has CREATE authority for the RG1 resource group. Because the second step involves the RG1 resource group, which is higher than the security checking level, WebSphere MQ Configuration agent starts to check the authority settings on the resource group level. The second step is approved if one of the following conditions is met:

- In the access authority settings for the RG1 resource group, you grant the user_1 user the CREATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the RG1 resource group. Instead, in the access authority settings for the QM1 queue manager, you grant the user_1 user the CREATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the RG1 resource group or the QM1 queue manager. Instead, in the access authority settings for the CSG1 configured system group, you grant the user_1 user the CREATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the RG1 resource group, the QM1 queue manager, or the CSG1 configured system group. Instead, you set the default access level for configuration database to CREATE.

Scenario: Authorizing a user to discover resources on the configured system group

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to discover resources on a configured system group.

It is assumed that in the actual WebSphere MQ environment, there is a QM1 queue manager. The QM1 queue manager has many different types of resources, such as channel, process, namelist, and listener. In the configuration database, a CSG1 configured system group is just created and has no resources in it.

There is a user_1 ID in the system. And the user_1 user wants to use the Discover operation on the CSG1 configured system group.

For the operation to be approved, the system administrator must grant the user_1 ID the authority to view the actual WebSphere MQ environment and the authority to create objects in the CSG1 configured system group.

For information about how to grant access authorities to a user ID or a group ID, see "Granting access authorities for an object to a user ID" on page 117 and "Granting access authorities for an object to a group ID" on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set as follows:

- CREATE for the configuration database
- READ for the WebSphere MQ environment

When the security checking level is set to Configured system group, Configured system, Resource group, or Resource

The target object is configured system group, which is higher than the configured system, resource group, or resource. The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant the following authorities to the user_1 ID:
  - CREATE authority for the CSG1 configured system group in the configuration database
  - READ authority for the WebSphere MQ environment
- If no authority for the CSG1 configured system group is specified for the user_1 ID, the default access level is set to CREATE for the configuration database. And you grant READ authority for the WebSphere MQ environment to the user_1 ID.
- If no authority for the WebSphere MQ environment is specified for the user_1 ID, the default access level is set to READ for the WebSphere MQ environment. And you grant CREATE authority for the CSG1 configured system group in the configuration database to the user_1 ID.
- If no authority for the CSG1 configured system group and the WebSphere MQ environment is specified for the user_1 ID, the default access level is set as follows:
  - CREATE for the configuration database
  - READ for the WebSphere MQ environment

Example for authorizing a user to discover resources on the configured system group

In the following example, to the user_1 ID, the system administrator grants CREATE authority for the CSG1 configured system group. The default access level is set to READ for WebSphere MQ environment and UPDATE for the configuration database.

Table 11. Authority settings

ID	Object	Authority
user_1	CSG1 configured system group	CREATE
all users	Default access level for configuration database	UPDATE
all users	Default access level for WebSphere MQ environment	READ

- When the security checking level is set to NONE, the operation is denied. Because the default access level for the configuration database is set to UPDATE, which is lower than the required CREATE authority.
- When the security checking level is set to Resource, Resource group, Configured system, or Configured system group, the operation is approved. This is because the user_1 ID has CREATE authority for the CSG1 configured system group, and the default access level for WebSphere environment is set to READ.

Scenario: Authorizing a user to import resources to a configured system

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to import resources to a configured system.

It is assumed there is a configured system group named CSG1 in the Defined View. And the CSG1 configured system group has a QM1 configured system.

There is a user_1 ID in the group_1 group in the system. And the user_1 user wants to use the Import function to import resources to the QM1 configured system.

For the operation to be approved, the system administrator must grant CREATE authority for the related objects to the user_1 ID or the group_1 ID.

For information about how to grant access authorities to a user ID or a group ID, see "Granting access authorities for an object to a user ID" on page 117 and "Granting access authorities for an object to a group ID" on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to CREATE for the configuration database.

When the security checking level is set to configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant CREATE authority for the CSG1 configured system group to the user_1 ID or the group_1 ID.
- If no authority for the CSG1 configured system group is specified for the user_1 ID or the group_1 ID, the default access level is set to CREATE for the configuration database.

When the security checking level is set to Configured system, Resource group, or Resource

The target object is a configured system, which is higher than Resource or Resource group. The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant CREATE authority for the QM1 configured system to the user_1 ID or the group_1 ID.
- If no authority for the QM1 configured system is specified for the user_1 ID or the group_1 ID, you grant CREATE authority for the CSG1 configured system group to the user_1 ID or the group_1 ID.
- If no authorities for the CSG1 configured system group and for the QM1 configured system are specified for the user_1 ID or group_1 ID, the default access level is set to CREATE for the configuration database.

Example for authorizing a user to import resources to a configured system

In the following example, the system administrator grants the following authorities to the user_1 ID and grants CREATE authority for the CSG1 configured system group to the group_1 ID. The default access level is set to UPDATE for the configuration database.

- DELETE authority for the QM1 configured system
- UPDATE authority for the CSG1 configured system group.

Table 12. Authority settings

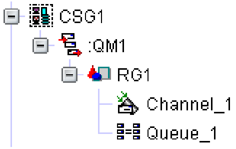
ID	Object	Authority
user_1	QM1 configured system	DELETE
	CSG1 configured system group	UPDATE
group_1	CSG1 configured system group	CREATE
all users	Default access level for configuration database	UPDATE

- When the security checking level is set to NONE, the operation is denied. This is because the default access level for the configuration database is set to UPDATE, which is lower than the required CREATE authority.
- When the security checking level is set to configured system group, the operation is approved. This is because the group_1 ID has CREATE authority for the CSG1 configured system group.
- When the security checking level is set to configured system, Resource group, or Resource, the operation is approved. This is because the user_1 ID has DELETE authority for the CSG1 configured system group, which is higher than the required CREATE authority.

Scenario: Authorizing a user to create multiple copies of an object

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to create multiple copies of an object.

The existing tree structure is displayed in the following figure. There is a configured system group named CSG1 in the Defined View. The CSG1 configured system group has a QM1 configured system. The QM1 configured system has a RG1 resource group. The RG1 resource group has two resources, Queue_1 and Channel_1.



There is a user_1 ID in the system. And the user_1 user wants to use the Replicate function to create multiple copies of RG1 resource group in the QM1 configured system.

For the operation to be approved, the user_1 ID must have READ authority for the object that is to be replicated, and CREATE authority for the object in which the replicated object is to be created.

For information about how to grant access authorities to a user ID or a group ID, see "Granting access authorities for an object to a user ID" on page 117 and "Granting access authorities for an object to a group ID" on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to CREATE for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant CREATE authority for the CSG1 configured system group to the user_1 ID.
- If no authority for the CSG1 configured system group is specified for the user_1 ID, the default access level is set to CREATE for the configuration database.

When the security checking level is set to Configured system

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

The operation is approved in one of the following circumstances:

- You grant CREATE authority for the QM1 configured system to the user_1 ID:
- If no authority for the QM1 configured system is specified for the user_1 ID, you grant CREATE authority for the CSG1 configured system to the user_1 ID.
- If no authority for the following objects is specified for the user_1 ID, the default access level to the configuration database is set to CREATE:
  - QM1 configured system
  - CSG1 configured system group

When the security checking level is set to Resource group or Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the resource group level.

The operation is approved in one of the following circumstances:

- You grant the following authorities to the user_1 ID:
  - READ authority for the RG1 resource
  - CREATE authority for the QM1 configured system in the configuration database
- If no authority for the RG1 resource group is specified for the user_1 ID, you grant CREATE authority for the QM1 configured system to the user_1 ID.
- If no authority for the following objects is specified for the user_1 ID, you grant CREATE authority for the CSG1 configured system group:
  - RG1 resource group
  - QM1 configured system
- If no authority for the following objects is specified for the user_1 ID, the default access level for the configuration database is set to CREATE:
  - RG1 resource group
  - QM1 configured system
  - CSG1 configured system group

Example for authorizing a user to create multiple copies of an object

In the following example, the system administrator grants the following authorities to the user_1 ID. The default access level is set to UPDATE for the configuration database.

- CREATE authority for the QM1 configured system
- UPDATE authority for the CSG1 configured system group

Table 13. Authority settings

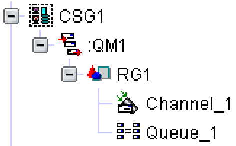
ID	Object	Authority
user_1	QM1 configured system	CREATE
	CSG1 configured system group	UPDATE
all users	Default access level for configuration database	UPDATE

- When the security checking level is set to NONE, the operation is denied. This is because the default access level for the configuration database is set to UPDATE, which is lower than the required CREATE authority.
- When the security checking level is set to Configured system group, the operation is denied. This is because the user_1 ID only has UPDATE authority for the CSG1 configured system group, which is lower than the required CREATE authority.
- When the security checking level is set to Configured system, Resource group, or Resource, the operation is approved. This is because the user_1 ID has CREATE authority for the QM1 configured system.

Scenario: Authorizing a user to view discrepancies for a configured system

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to view discrepancies between defined and actual resource definitions for an object.

The existing tree structure is displayed in the following figure. There is a configured system group named CSG1 in the Defined View. The CSG1 configured system group has a QM1 configured system. The QM1 configured system has a RG1 resource group. The RG1 resource group has two resources, Queue_1 and Channel_1.



There is a user_1 ID in the system. And the user_1 user wants to use the View discrepancies function to evaluate the difference between defined and actual resource definitions for the QM1 configured system.

The operation is to view the definition of resources that are listed in an object. The WebSphere MQ Configuration agent checks whether the user has READ authority for the resources that are listed in the target object. For the operation to be approved, the system administrator must grant the READ authority for the related resources in the configuration database and READ authority for the WebSphere MQ environment to the user_1 ID.

For information about how to grant access authorities to a user ID or a group ID, see “Granting access authorities for an object to a user ID” on page 117 and “Granting access authorities for an object to a group ID” on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to READ for both the configuration database and WebSphere MQ environment.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant the following authorities to the user_1 ID:
  - READ authority for the CSG1 configured system group
  - READ authority for WebSphere MQ environment
- If no authorities for the CSG1 configured system group and WebSphere MQ environment are specified for the user_1 ID, the default access level is set to READ for both the configuration database and WebSphere MQ environment.

When the security checking level is set to Configured system

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

The operation is approved in one of the following circumstances:

- You grant the following authorities to the user_1 ID:
  - READ authority for the QM1 configured system
  - READ authority for WebSphere MQ environment
- If no authority for the QM1 configured system is specified for the user_1 ID, you grant the following authorities to the user_1 ID:
  - READ authority for the CSG1 configured system group
  - READ authority for WebSphere MQ environment
- If no authority for the WebSphere MQ environment is specified for the user_1 ID, the default access level is set to READ for WebSphere MQ environment. And, you grant READ authority for the QM1 configured system to the user_1 ID.
- If no authorities for the QM1 configured system and WebSphere MQ environment are specified for the user_1 ID, the default access level is set to READ for the WebSphere MQ environment. And you grant READ authority for the CSG1 configured system group to the user_1 ID.
- If no authorities for the QM1 configured system and CSG1 configured system group are specified for the user_1 ID, the default access level is set to READ for the configuration database. And, you grant READ authority for the WebSphere MQ environment to the user_1 ID.
- If no authorities for the following objects are specified for the user_1 ID, the default access level is set to READ for both the configuration database and WebSphere MQ environment:
  - QM1 configured system
  - CSG1 configured system group
  - WebSphere MQ environment

When the security checking level is set to Resource group

The WebSphere MQ Configuration agent starts to check the authority settings on the resource group level.

The operation is approved in one of the following circumstances:

- You grant the following authorities to the user_1 ID:
  - READ authority for the RG1 resource group
  - READ authority for the QM1 configured system
  - READ authority for WebSphere MQ environment
- If no authority for the RG1 resource group is specified for the user_1 ID, you grant the following authorities to the user_1 ID:
  - READ authority for the QM1 configured system
  - READ authority for WebSphere MQ environment
- If no authorities for the RG1 resource group and WebSphere MQ environment are specified for the user_1 ID, the default access level is set to READ for WebSphere MQ environment. And you grant READ authority for the QM1 configured system to the user_1 ID.

- If no authorities for the RG1 resource group and QM1 configured system are specified for the user_1 ID, you grant the following authorities to the user_1 ID:
  - READ authority for the CSG1 configured system
  - READ authority for WebSphere MQ environment
- If no authorities for the following objects are specified for the user_1 ID, you grant READ authority for the CSG1 configured system to the user_1 ID. And, the default access level is set to READ for WebSphere MQ environment.
  - RG1 resource group
  - QM1 configured system
  - WebSphere MQ environment
- If no authorities for the following objects are specified for the user_1 ID, you grant READ authority for the WebSphere MQ environment to the user_1 ID. And, the default access level is set to READ for configuration database.
  - RG1 resource group
  - QM1 configured system
  - CSG1 configured system group
- If no authorities for the following objects are specified for the user_1 ID, the default access level is set to READ for both the configuration database and WebSphere MQ environment:
  - RG1 resource group
  - QM1 configured system
  - CSG1 configured system group
  - WebSphere MQ environment

When the security checking level is set to Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the resource level.

The operation is approved in one of the following circumstances:
- You grant the following authorities to the user_1 ID:
  - READ authority for the Queue_1 resource
  - READ authority for the Channel_1 resource
  - READ authority for the RG1 resource group
  - READ authority for the QM1 configured system
  - READ authority for WebSphere MQ environment
- If no authorities for the Queue_1 resource and the Channel_1 resource are specified for the user_1 ID, you grant the following authorities to the user_1 ID:
  - READ authority for the RG1 resource group
  - READ authority for the QM1 configured system
  - READ authority for WebSphere MQ environment
- If no authorities for the following objects are specified for the user_1 ID, you grant READ authority for the QM1 configured system to the user_1 ID. And you grant READ authority for WebSphere MQ environment to the user_1 ID.
  - Queue_1 resource
  - Channel_1 resource
  - RG1 resource group

- If no authorities for the following objects are specified for the user_1 ID, you grant READ authority for the QM1 configured system to the user_1 ID. And the default access level is set to READ for WebSphere MQ environment.
  - Queue_1 resource
  - Channel_1 resource
  - RG1 resource group
  - WebSphere MQ environment
- If no authorities for the following objects are specified for the user_1 ID, you grant READ authority for the CSG1 configured system to the user_1 ID. And you grant READ authority for WebSphere MQ environment to the user_1 ID.
  - Queue_1 resource
  - Channel_1 resource
  - RG1 resource group
  - QM1 configured system
- If no authorities for the following objects are specified for the user_1 ID, you grant READ authority for the CSG1 configured system to the user_1 ID. And, the default access level is set to READ for WebSphere MQ environment.
  - Queue_1 resource
  - Channel_1 resource
  - RG1 resource group
  - QM1 configured system
  - WebSphere MQ environment
- If no authorities for the following objects are specified for the user_1 ID, the default access level is set to READ for the configuration database. And, you grant READ authority for WebSphere MQ environment to the user_1 ID.
  - Queue_1 resource
  - Channel_1 resource
  - RG1 resource group
  - QM1 configured system
  - CSG1 configured system group
- If no authorities for the following objects are specified for the user_1 ID, the default access level is set to READ for the configuration database and WebSphere MQ environment.
  - Queue_1 resource
  - Channel_1 resource
  - RG1 resource group
  - QM1 configured system
  - CSG1 configured system group
  - WebSphere MQ environment

Example for authorizing a user to view discrepancies for a configured system

In the following example, the system administrator grants the following authorities to the user_1 ID. The default access level is set to READ for WebSphere MQ environment and UPDATE for the configuration database.

- NONE authority for the Queue_1 resource
- CREATE authority for the RG1 resource group

- UPDATE authority for the QM1 configured system
- READ authority for the CSG1 configured system group

Table 14. Authority settings

ID	Object	Authority
user_1	Queue_1 resource	NONE
	RG1 resource group	CREATE
	QM1 configured system	UPDATE
	CSG1 configured system group	READ
all users	Default access level for configuration database	UPDATE
all users	Default access level for WebSphere MQ environment	READ

- When the security checking level is set to NONE, the operation is approved. This is because the default access level for the configuration database is set to UPDATE, which is higher than the required READ authority. And the default access level is set to READ for WebSphere MQ environment.
- When the security checking level is set to Configured system group, the operation is approved. This is because the user has READ authority for the CSG1 configured system group, and the default access level is set to READ for WebSphere MQ environment.
- When the security checking level is set to Configured system, the operation is approved. This is because the user has UPDATE authority for the QM1 configured system, which is higher than the required READ authority. And, the default access level is set to READ for WebSphere MQ environment.
- When the security checking level is set to Resource group, the operation is approved. This is because the user has CREATE authority for the RG1 resource group, which is higher than the required READ authority. And, the default access level is set to READ for WebSphere MQ environment.
- When the security checking level is set to Resource, because the user_1 ID has NONE authority for the Queue_1 resource, you cannot view the difference between Queue_1 in the Defined View and Queue_1 in the actual WebSphere MQ environment. You can view the difference between other resources in QM1 in the Defined View and their counterparts in the actual WebSphere MQ environment.

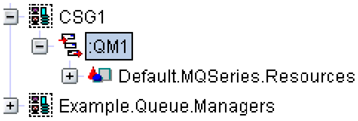
Scenario: Authorizing a user to break the association between a queue manager and its prototype

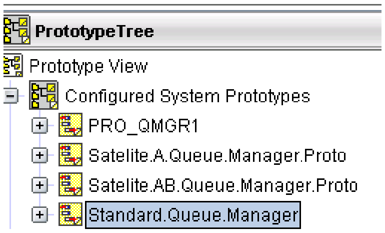
As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to break the association between a queue manager in the Defined View and the prototype that it is based on.

This Disinherit operation changes the value of the **Based on prototype** attribute of the queue manager in the Defined View. Therefore, for this Disinherit operation to be approved by the WebSphere MQ Configuration agent, the user must have the UPDATE authority or higher for the queue manager.

The following figure shows the existing hierarchical structure in the Defined View and Prototype View. The QM1 queue manager that is contained in the CSG1 configured system group is based on the queue manager prototype named

Standard.Queue.Manager. The value of the **Use Count** attribute of Standard.Queue.Manager is 5.




PrototypeTree
Prototype View
Configured System Prototypes
PRO_QMGR1
Satelite.A.Queue.Manager.Proto
Satelite.AB.Queue.Manager.Proto
Standard.Queue.Manager

There is one user named user_1 in the environment. The user_1 user wants to break the association between the QM1 queue manager and the Standard.Queue.Manager prototype.

When the Security checking level is set to None

Because the Security checking level is set to None, WebSphere MQ Configuration agent checks only the default database access level in the Tivoli Enterprise Monitoring Server. This operation is approved if you set the default access level for configuration database to UPDATE.

When the Security checking level is set to Configured System Group

This operation requires that the user_1 user has UPDATE authority or higher for the QM1 queue manager. Because the Security checking level is set to **Configured System Group**, which is higher than the resource type of the QM1 queue manager, WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level. This operation is approved if one of the following conditions is met:

- In the access authority settings for the CSG1 configured system group, you grant the user_1 user the UPDATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the CSG1 configured system group. Instead, you set the default access level for configuration database to UPDATE.

When the Security checking level is set to Configured System

This operation requires that the user_1 user has UPDATE authority or higher for the QM1 queue manager. Because the Security checking level is set to Configured System, which is the same as the resource type of the QM1 queue manager, WebSphere MQ Configuration agent starts to check the authority settings on the configured system level. This operation is approved if one of the following conditions is met:

- In the access authority settings for the QM1 queue manager, you grant the user_1 user the UPDATE authority for the configuration database.

- You do not grant the user_1 user any access authorities for the QM1 queue manager. Instead, in the access authority settings for the CSG1 configured system group, you grant the user_1 user the UPDATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the QM1 queue manager or the CSG1 configured system group. Instead, you set the default access level for configuration database to UPDATE.

When the Security checking level is set to Resource Group or Resource

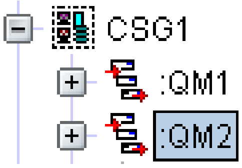
This operation requires that the user_1 user has UPDATE authority or higher for the QM1 queue manager. Because the Security checking level is lower than the resource type of the QM1 queue manager, WebSphere MQ Configuration agent starts to check the authority settings on the configured system level. This operation is approved if one of the following conditions is met:

- In the access authority settings for the QM1 queue manager, you grant the user_1 user the UPDATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the QM1 queue manager. Instead, in the access authority settings for the CSG1 configured system group, you grant the user_1 user the UPDATE authority for the configuration database.
- You do not grant the user_1 user any access authorities for the QM1 queue manager or the CSG1 configured system group. Instead, you set the default access level for configuration database to UPDATE.

Scenario: Authorizing a user to drag a queue manager to another queue manager

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to drag a queue manager to another queue manager.

In this scenario, there are two queue managers, QM1 and QM2, listed in the CSG1 configured system group. A user named user_1 wants to drag the QM2 queue manger to the QM1 queue manager.



For the operation to be approved by the WebSphere MQ Configuration agent, the user_1 ID must have CREATE authority for both the QM1 and QM2 queue managers.

For information about how to grant access authorities to a user ID or a group ID, see “Granting access authorities for an object to a user ID” on page 117 and “Granting access authorities for an object to a group ID” on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to CREATE for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant CREATE authority for the CSG1 configured system group to the user_1 ID.
- If no authority for the CSG1 configured system group is specified for the user_1 ID, the default access level is set to CREATE for the configuration database.

When the security checking level is set to Configured system, Resource group, or Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

The operation is approved in one of the following circumstances:

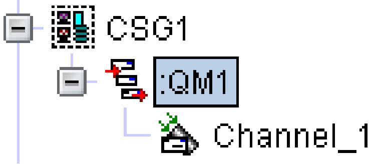
- You grant the CREATE authority for the following objects to the user_1 ID:
  - QM1 queue manager
  - QM2 queue manager
- If no authority for QM1 queue manager or QM2 queue manager is specified for the user_1 ID, you grant CREATE authority for the CSG1 configured system group to the user_1 ID.
- If no authorities for the following objects are specified for the user_1 ID, the default access level is set to CREATE for the configuration database:
  - QM1 queue manager
  - QM2 queue manager
  - CSG1 configured system group

Scenario: Authorizing a user to drag a defined object to the Prototype View

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to drag a defined object to the Prototype View.

For the operation to be approved by the WebSphere MQ Configuration agent, the user must have READ authority for the defined object and CREATE authority for the prototype object into which the defined object is dragged.

In this scenario, it is assumed that there is a queue manager, QM1, listed in the CSG1 configured system group. A user named user_1 wants to drag the QM1 queue manager from the Defined View to the Configured System Prototypes node in the Prototype View.



Remember: The concept of security checking level is not applicable to the prototype objects. The WebSphere MQ Configuration agent checks the authority settings only from the target prototype object directly. For the defined objects, the inheritance of security authority and security checking level still apply.

The operation is approved when the user has READ authority for the QM1 configured system and CREATE authority for the Configured System Prototypes node.

When the security checking level is set to NONE

The operation is approved in the following circumstances:

- You grant CREATE authority for the Configured System Prototypes node to the user_1 ID, and the default access level is set to READ for the configuration database.
- If no authority is specified for the Configured System Prototypes node, the default access level is set to CREATE for the configuration database.

When the security checking level is set to Configured system group

The operation can be approved in the one of following circumstances:

- You grant READ authority for the CSG1 configured system group and CREATE authority for the Configured System Prototypes node to the user_1 ID.
- If no authority is specified for the CSG1 configured system group, you grant CREATE authority for the Configured System Prototypes node to the user_1 ID, and the default access level is set to READ for the configuration database.
- If no authority is specified for the Configured System Prototypes node, you grant READ authority for the CSG1 configured system group and the default access level is set to CREATE for the configuration database.
- If no authorities are specified for the Configured System Prototypes node and the CSG1 configured system group, the default access level is set to CREATE for the configuration database.

When the security checking level is set to Configured system, Resource group, or Resource

The operation can be approved in the one of following circumstances:

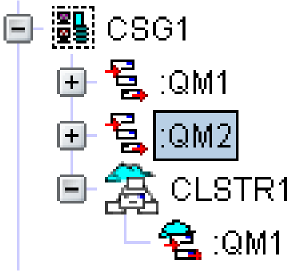
- You grant READ authority for the QM1 configured system and CREATE authority for the Configured System Prototypes node to the user_1 ID.
- If no authority is specified for the QM1 configured system, you grant READ authority for the CSG1 configured system group and CREATE authority for the Configured System Prototypes node to the user_1 ID.
- If no authority is specified for the following objects, you grant CREATE authority for the Configured System Prototypes node to the user_1 ID and the default access level is set to READ for the configuration database.

  - QM1 configured system
  - CSG1 configured system group
- If no authority is specified for the following objects, the default access level is set to CREATE for the configuration database.
  - QM1 configured system
  - CSG1 configured system group
  - Configured System Prototypes node

Scenario: Authorizing a user to drag a queue manager to a managed cluster

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to drag a queue manager to a managed cluster.

In this scenario, a CLSTR1 managed cluster is created and included in the CSG1 configured system group. The QM1 queue manager is already in the CLSTR1 managed cluster. A user named user_1 wants to drag another queue manager QM2 to the CLSTR1 cluster.



When a queue manager is dragged to a cluster, some cluster related channels are also created for both the target queue manager and queue managers that already exists in the cluster. For the operation to be approved by the WebSphere MQ Configuration agent, the user_1 ID must have CREATE authority for the following objects:

- The managed cluster (CLSTR1)
- The base queue manager that is to be dragged to the cluster (QM2)
- The base queue managers that are already dragged to the cluster (QM1)

For information about how to grant access authorities to a user ID or a group ID, see “Granting access authorities for an object to a user ID” on page 117 and “Granting access authorities for an object to a group ID” on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to CREATE for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant CREATE authority for the CSG1 configured system group to the user_1 ID.
- If no authority for the CSG1 configured system group is specified for the user_1 ID, the default access level is set to CREATE for the configuration database.

When the security checking level is set to Configured system, Resource group, or Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

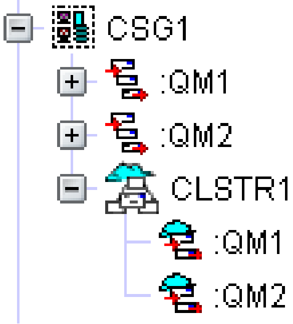
The operation is approved in one of the following circumstances:

- You grant CREATE authority for the following objects to the user_1 ID:
  - The CLSTR 1 managed cluster
  - The base QM1 queue manager
  - The base QM2 queue manager that is to be dragged to the cluster
- If no authority for the CLSTR1, QM1, or QM2 object is specified for the user_1 ID, you grant CREATE authority for the CSG1 configured system group to the user_1 ID.
- If no authorities for the following objects are specified for the user_1 ID, the default access level is set to CREATE for the configuration database:
  - The CLSTR 1 managed cluster
  - The base QM1 queue manager
  - The base QM2 queue manager that is to be dragged to the cluster
  - The CSG1 configured system group

Scenario: Authorizing a user to create a cluster queue

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to create a cluster queue in a managed cluster.

In this scenario, the existing tree structure is shown in the following figure. A user named user_1 wants to create a cluster queue in the CLSTR1 cluster.



For the operation to be approved, the user_1 ID must have CREATE authority for the CLSTR1 managed cluster and for all the base queue managers that are dragged to the CLSTR1 cluster.

For information about how to grant access authorities to a user ID or a group ID, see “Granting access authorities for an object to a user ID” on page 117 and “Granting access authorities for an object to a group ID” on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to CREATE for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant CREATE authority for the CSG1 configured system group to the user_1 ID.
- If no authority for the CSG1 configured system group is specified for the user_1 ID, the default access level is set to CREATE for the configuration database.

When the security checking level is set to Configured system, Resource group, or Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

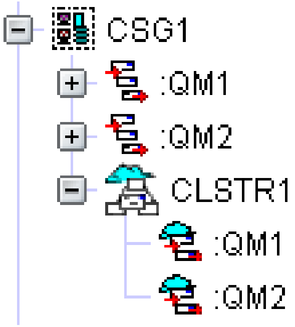
The operation is approved in one of the following circumstances:

- You grant the CREATE authority for the following objects to the user_1 ID:
  - CLSTR1 cluster
  - The base QM1 queue manager that is dragged to the cluster
  - The base QM2 queue manager that is dragged to the cluster
- If no authority for the following objects is specified for the user_1 ID, you grant CREATE authority for the CSG1 configured system group to the user_1 ID:
  - CLSTR1 managed cluster
  - The base QM1 queue manager
  - The base QM2 queue manager
- If no authorities for the following objects are specified for the user_1 ID, the default access level is set to CREATE for the configuration database:
  - CLSTR1 cluster
  - The base QM1 queue manager that is dragged to the cluster
  - The base QM2 queue manager that is dragged to the cluster
  - CSG1 configured system group

Scenario: Authorizing a user to modify a cluster queue manager

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to modify a cluster queue manager in a managed cluster.

In this scenario, a CLSTR1 managed cluster is created and included in the CSG1 configured system group. The CLSTR1 cluster has QM1 and QM2 cluster queue managers. A user named user_1 wants to modify some attributes of the QM1 queue manager.



For the operation to be approved by the WebSphere MQ Configuration agent, the user_1 ID must have UPDATE authority for the CLSTR1 managed cluster and for the base QM1 queue manager.

Remember: When a user wants to modify attributes of a cluster queue manager, the UPDATE authorities for the following objects are required:

- The managed cluster that contains the cluster queue manger
- The base queue manager that was dragged to the cluster

When a user wants to modify attributes of a cluster object (cluster queue or the manager cluster) rather than a cluster queue manager, the UPDATE authority for only the target cluster object is required.

For information about how to grant access authorities to a user ID or a group ID, see "Granting access authorities for an object to a user ID" on page 117 and "Granting access authorities for an object to a group ID" on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to UPDATE for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant UPDATE authority for the CSG1 configured system group to the user_1 ID.
- If no authority for the CSG1 configured system group is specified for the user_1 ID, the default access level is set to UPDATE for the configuration database.

When the security checking level is set to Configured system, Resource group, or Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

The operation is approved in one of the following circumstances:

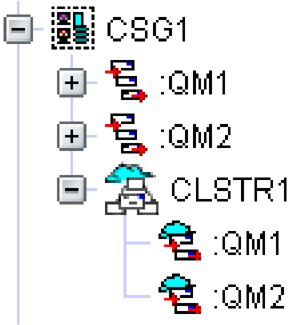
- You grant UPDATE authority for CLSTR1 managed cluster to the user_1 ID.

- If no authority for CLSTR1 managed cluster is specified for the user_1 ID, you grant UPDATE authority for the CSG1 configured system group to the user_1 ID.
- If no authorities for the following objects are specified for the user_1 ID, the default access level is set to UPDATE for the configuration database:
  - CLSTR1 managed cluster
  - CSG1 configured system group

Scenario: Authorizing a user to view a cluster queue manager

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to view a cluster queue manager in a cluster.

In this scenario, a CLSTR1 managed cluster is created and included in the CSG1 configured system group. The CLSTR1 cluster has QM1 and QM2 cluster queue managers. A user named user_1 wants to view the QM1 cluster queue manager.



For the operation to be approved by the WebSphere MQ Configuration agent, the user_1 ID must have following authorities:

- READ authority for the CLSTR1 cluster
- READ authority for the base QM1 queue manager that is dragged to the cluster

Remember: If a user wants to view a cluster queue, only READ authority for the target cluster queue is required.

For information about how to grant access authorities to a user ID or a group ID, see “Granting access authorities for an object to a user ID” on page 117 and “Granting access authorities for an object to a group ID” on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to READ for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant READ authority for the CSG1 configured system group to the user_1 ID.
- If no authority for the CSG1 configured system group is specified for the user_1 ID, the default access level is set to READ for the configuration database.

When the security checking level is set to Configured system, Resource group, or Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

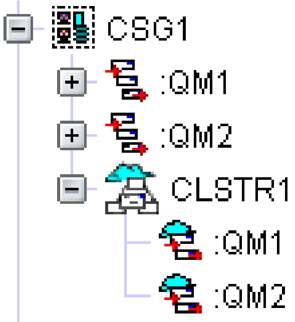
The operation is approved in one of the following circumstances:

- You grant the following authorities to the user_1 ID:
  - READ authority for the CLSTR1 cluster
  - READ authority for the base QM1 queue manager that is dragged to the cluster
- If no authority for the CLSTR1 managed cluster or the base QM1 queue manager is specified for the user_1 ID, you grant READ authority for the CSG1 configured system group to the user_1 ID.
- If no authorities for the following objects are specified for the user_1 ID, the default access level is set to READ for the configuration database:
  - CLSTR1 cluster
  - The base QM1 queue manager that is dragged to the cluster
  - CSG1 configured system group

Scenario: Authorizing a user to delete a managed cluster

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to delete a managed cluster.

In this scenario, a CLSTR1 managed cluster is created and included in the CSG1 configured system group. The CLSTR1 cluster has QM1 and QM2 cluster queue managers. A user named user_1 wants to delete the CLSTR1 cluster.



For the operation to be approved by the WebSphere MQ Configuration agent, the user_1 ID must have following authorities:

- DELETE authority for the CLSTR1 cluster
- DELETE authority for all the cluster objects that are included in the CLSTR1 cluster (QM1 and QM2 cluster queue managers)
- UPDATE authority for the CSG1 configured system group

For information about how to grant access authorities to a user ID or a group ID, see "Granting access authorities for an object to a user ID" on page 117 and "Granting access authorities for an object to a group ID" on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to DELETE for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant DELETE authority for the CSG1 configured system group to the user_1 ID.
- If no authority for the CSG1 configured system group is specified for the user_1 ID, the default access level is set to DELETE for the configuration database.

When the security checking level is set to Configured system, Resource group, or Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

The operation is approved in one of the following circumstances:

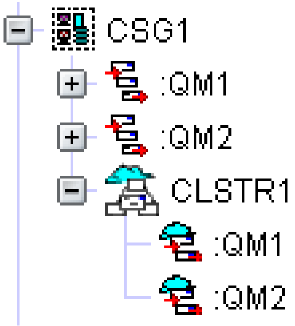
- You grant the following authorities to the user_1 ID:
  - DELETE authority for the CLSTR1 cluster
  - DELETE authority for all the cluster objects that are included in the CLSTR1 cluster (QM1 and QM2 cluster queue managers)
  - UPDATE authority for the CSG1 configured system group

  Tip: The QM1 and QM2 cluster queue managers are included in the CLSTR1 cluster. If no authority for the QM1 or QM2 cluster queue manger is specified for the user_1 ID, the operation can also be approved if you only grant DELETE authority for the CLSTR1 cluster and UPDATE authority for the CSG1 configured system group to the user_1 ID.
- If no authority for the CLSTR1 cluster is specified for the user_1 ID, you grant DELETE authority for the CSG1 configured system group to the user_1 ID.
- If no authority for the following objects are specified for the user_1 ID, the default access level is set to DELETE for the configuration database:
  - CLSTR1 cluster
  - QM1 cluster queue manager
  - QM2 cluster queue manager
  - CSG1 configured system group

Scenario: Authorizing a user to delete a cluster queue manager

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to delete a cluster queue manager from a managed cluster.

In this scenario, a CLSTR1 managed cluster is created and included in the CSG1 configured system group. The CLSTR1 cluster has QM1 and QM2 cluster queue managers. A user named user_1 wants to delete the QM1 cluster queue manager from the cluster.



For the operation to be approved by the WebSphere MQ Configuration agent, the user_1 ID must have DELETE authority for the base queue manager that is dragged to the cluster and UPDATE authority for the CLSTR1 managed cluster.

For information about how to grant access authorities to a user ID or a group ID, see “Granting access authorities for an object to a user ID” on page 117 and “Granting access authorities for an object to a group ID” on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to DELETE for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved in one of the following circumstances:

- You grant DELETE authority for the CSG1 configured system group to the user_1 ID.
- If no authority for the CSG1 configured system group is specified for the user_1 ID, the default access level is set to DELETE for the configuration database.

When the security checking level is set to Configured system, Resource group, or Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

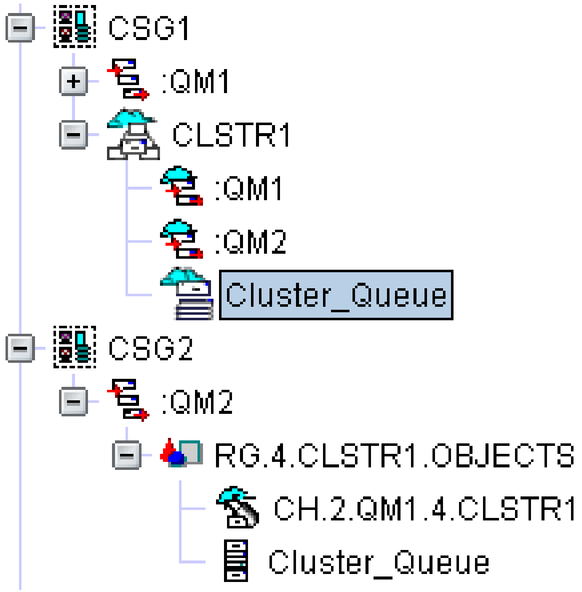
The operation is approved in one of the following circumstances:

- You grant the following authorities to to the user_1 ID:
  - DELETE authority for the QM1 queue manager
  - UPDATE authority for the CLSTR1 managed cluster
- If no authority for the CLSTR1 managed cluster is specified for the user_1 ID, you grant the following authorities to the user_1 ID.
  - DELETE authority for the QM1 queue manager
  - UPDATE authority for the CSG1 configured system group
- If no authority for the QM1 queue manager is specified for the user_1 ID, you grant the following authorities to the user_1 ID:
  - DELETE authority for the CSG1 configured system group
- If no authority for the QM1 queue manager and CLSTR1 cluster are specified for the user_1 ID, you grant DELETE authority for the CSG1 configured system group to the user_1 ID.
- If no authorities for the following objects are specified for the user_1 ID, the default access level is set to DELETE for the configuration database:
  - QM1 queue manager
  - CLSTR1 managed cluster
  - CSG1 configured system group

Scenario: Authorizing a user to delete a cluster queue

As a system administrator, you can use this scenario to determine the minimum authority requirements that a user needs to delete a cluster queue from a managed cluster.

In this scenario, a CLSTR1 managed cluster is created and included in the CSG1 configured system group. The CLSTR1 cluster has a cluster queue named Cluster_Queue. The base queue is defined in the QM2 queue manager in the CSG2 configured system group. A user named user_1 wants to delete the Cluster_Queue cluster queue from the cluster.



For the operation to be approved by the WebSphere MQ Configuration agent, the user_1 ID must have following authorities:

- DELETE authority for the Cluster_Queue cluster queue
- DELETE authority for the base Cluster_Queue queue in the QM2 queue manager
- UPDATE authority for the CLSTR1 managed cluster
- UPDATE authority for the QM2 queue manager

For information about how to grant access authorities to a user ID or a group ID, see “Granting access authorities for an object to a user ID” on page 117 and “Granting access authorities for an object to a group ID” on page 119.

When the security checking level is set to NONE

The WebSphere MQ Configuration agent checks only the default access level. The operation is approved when the default access level is set to DELETE for the configuration database.

When the security checking level is set to Configured system group

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system group level.

The operation is approved when the user_1 ID has DELETE authority for the CSG1 configured system group and the CSG2 configured system group.

When the security checking level is set to Configured system

The WebSphere MQ Configuration agent starts to check the authority settings on the configured system level.

The operation is approved when you grant the following authorities to the user_1 ID:

- DELETE authority for the CLSTR1 managed cluster
- DELETE authority for the QM2 queue manager

When the security checking level is set to Resource group

The WebSphere MQ Configuration agent starts to check the authority settings on the resource group level.

The operation is approved when you grant the following authorities to the user_1 ID:

- DELETE authority for the CLSTR1 managed cluster
- DELETE authority for the RG.4.CLSTR1.OBJECTS resource group
- UPDATE authority for the QM2 queue manager

When the security checking level is set to Resource

The WebSphere MQ Configuration agent starts to check the authority settings on the resource level.

The operation is approved when you grant the following authorities to the user_1 ID:

- UPDATE authority for the CLSTR1 managed cluster

- DELETE authority for the Cluster_Queue cluster queue
- DELETE authority for the Cluster_Queue queue in the QM2 queue manager
- UPDATE authority for the QM2 queue manager

Access authorities required for different operations

Table 15 lists the operations that the WebSphere MQ Configuration agent provides and the required minimum authorities that a user needs to perform these operations, when granular security is enabled in your environment.

In the following table, the **Configuration database authorities required** column lists the minimum access authority to objects in the configuration database that is required for the user to use the given operation. The **WebSphere MQ authorities required** column lists the minimum access authority for objects in the actual WebSphere MQ environment that is required for the user to use the given operation. For the set of possible access authorities, see "Different levels of access authorities" on page 111. After the granular security is enabled, you can use the Grant authorization window to grant configuration database authority or WebSphere MQ authority for an object to a user.

For more information about how to grant authorities for an object, see "Granting access authorities for an object to a user ID" on page 117 or "Granting access authorities for an object to a group ID" on page 119.

Table 15. Access authorities required for different operations

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Access configuration options from the workspaces of the WebSphere MQ Monitoring agent	If you install the WebSphere MQ Configuration agent and WebSphere MQ Monitoring agent, you can access the settings list of an object from the workspaces of WebSphere MQ Monitoring agent.	No security checking is performed on this operation.	No security checking is performed on this operation.
Add, delete, or modify global variables	Use the Global Variables workspace to add, delete, or modify global variables.	• UPDATE authority for global variables For information about how to grant authorities for global variables, see "Granting authorities for adding, deleting, or modifying global variables to a user or group" on page 126	None

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Back up configuration database	Use the **Backup Configuration Database** option to generate the file that stores all records in the database.	- READ authority for backing up the configuration database For information about how to grant backup authorities, see "Granting authorities for backing up the configuration database to a user or group" on page 126.	None
Compare defined items	Click **Compare items** > **Defined** to quickly compare two selected queue managers or two selected resources of the same type when the selected items are both defined objects in the configuration database.	- READ authority for the two selected objects	None
Compare defined item with actual item	Use **Compare items** > **Options** menu option to compare two selected objects in the configuration database and WebSphere MQ environment.	- READ authority for the selected objects	- READ authority for the selected objects
Create a cluster queue	Use the **Create** > **Cluster Queue** menu option to create cluster queues in a managed cluster.	- CREATE authority for the managed cluster - CREATE authority for all base queue managers that are dragged to the cluster	None
Create a managed cluster	Use the **Create** > **Managed Cluster** menu option to create a managed cluster.	- CREATE authority for the configured system group that contains the managed cluster	None
Create a schedule	Use the **Schedules** > **Create** menu option to schedule an action against an object and the descendants of the object in the Defined View.	- CREATE authority for the selected object	None

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Create an object in Defined View or Prototype view	Use the **Create** menu options to create new objects of various types in the Defined and Prototype View.	• CREATE authority for the selected object	None
Delete a cluster queue	Select a cluster queue in a managed cluster, right-click, and click **Delete**.	• UPDATE authority for the managed cluster • UPDATE authority for the base queue manager • DELETE authority for the selected cluster queue • DELETE authority for the base queue	None

Table 15. Access authorities required for different operations (continued)

Operation	**How to use the operation**	**Configuration database authorities required**	**WebSphere MQ authorities required**
Delete a cluster queue manager	Select a cluster queue manager in a managed cluster, right-click, and click **Delete**.	Different authorities are required depending on where you select the cluster queue manager: • Select the cluster queue manager that is listed in the managed cluster: – UPDATE authority for the managed cluster – DELETE authority for the base queue manager that is dragged to the managed cluster • Select the base cluster queue manager that is listed in the configured system group: – UPDATE authority for the configured system group that contains the base queue manger – UPDATE authority for the managed cluster or clusters (if the queue manager belongs to multiple managed clusters) – DELETE authority for the base queue manager that is dragged to the managed cluster – DELETE authority for all resources that are included in the base queue manager	None

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Delete a managed cluster	Select a managed cluster, right-click, and click **Delete**.	• DELETE authority for the selected cluster • DELETE authority for all cluster resources that are included in the selected cluster • DELETE authority for the base queue managers that are dragged to the cluster • UPDATE authority for the configured system group to which the selected cluster belongs	None
Delete a scheduled action	Use the **Schedules** > **View** menu option to view the Scheduled Action Report window, and delete the selected schedule.	• DELETE authority for the schedule For information about how to grant authorities for schedules, see "Granting authorities for viewing, deleting, or modifying schedules to a user or group" on page 128.	None
Delete actual	Click **Delete** > **Actual** to perform a delete action on the selected object. This action deletes an object from your actual WebSphere MQ environment.	• READ authority for the selected object • READ authority for all resources that are included in the selected object	• EXECUTE authority for the selected object • EXECUTE authority for all resources that are included in the selected object
Delete both	Click **Delete** > **Both** to perform a delete operation on the selected object. This operation deletes an object from the configuration database and from your actual WebSphere MQ environment.	• DELETE authority for the selected object • DELETE authority for all resources that are included in the selected object • UPDATE authority for the object to which the selected object belongs	• EXECUTE authority for the selected object • EXECUTE authority for all resources that are included in the selected object

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Delete defined	Click **Delete** > **Defined** to perform a delete action on the selected object. This action deletes the object from the configuration database.	• DELETE authority for the selected object • DELETE authority for all resources that are included in the selected object • UPDATE authority for the object to which the selected object belongs	None
Discover	Use the **Discover** menu option to populate a configuration database with data from existing queue managers. This option is only available at the configured system group level.	• CREATE authority for the configured system group	None
Discover new resources	Use the **Discover new resources** menu option to search the configured system (in this case, a queue manager) and add newly-discovered resources to the configuration database and the Defined View. This option is only available at the configured system level.	• CREATE authority for the configured system • UPDATE authority for all resource groups that are included in the configured system	None
Disinherit (in Defined View)	Use the **Disinherit** menu option to break the association between a prototype and the selected defined object.	• UPDATE authority for the selected defined object	None
Disinherit (in Prototype View)	Use the **Disinherit** menu option to break the association between a defined object and the selected prototype.	• UPDATE authority for the selected prototype • UPDATE authority for all defined objects that are created based on the selected prototype	None
Display status of a channel	Click **Action** > **Display status** to display the status of the selected channel.	• READ authority for the selected channel	• READ authority for the selected channel

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Drag a queue manager to a managed cluster	Use the drag-and-drop operation to create a queue manager in a managed cluster. This operation results in creating additional resources such as channels.	• CREATE authority for the selected queue manager • CREATE authority for the managed cluster • CREATE authority for all base queue managers that are already dragged to the cluster	None
Drag a queue manager to another queue manager	Use the drag-and-drop operation to create the connections between both queue managers. The operation results in creating additional resources such as channels and processes.	• CREATE authority for the selected queue manager • CREATE authority for the queue manager to which the selected queue manager is dragged	None
Drag to copy a defined object	Use the drag-and-drop operation in Defined View to make a copy of a defined object	• READ authority for the selected object • READ authority for all resources that are included in the selected object • CREATE authority for the object to which the selected object is dragged	None
Drag to create a defined object	Drag a prototype object to Defined View to create a defined object based on the prototype object.	• READ authority for the selected prototype object • READ authority for all resources that are included in the selected prototype object • CREATE authority for the defined object to which the prototype object is dragged	None

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Drag to create a prototype object	Drag a defined object to Prototype View to create a prototype object.	• READ authority for the selected defined object • READ authority for all resources that are included in the selected defined object • CREATE authority for the prototype object to which the defined object is dragged	None
Export extended	Click **Export** > **Extended** to export information about the selected object. The data is exported in XML format. This option is available for a selected object in the Defined or Prototype View.	• READ authority for the selected object • READ authority for all resources that are included in the selected object	None
Export MQSC commands	Click **Export** > **MQSC commands** to export files in MQSC commands format. This option is available for a selected object in the Defined or Prototype View.	• READ authority for the selected object • READ authority for all resources that are included in the selected object	None
Export partial	Click **Export** > **Partial** to export the application-specific information about the selected object. The data is exported in XML format. This option is available for a selected object in the Defined or Prototype View.	• READ authority for the selected object • READ authority for all resources that are included in the selected object	None
Find	Use the **Find** menu option to display the Find Objects window. The **Find** menu option is available for any selected object in the Defined View or in the Prototype View.	No security checking is performed on this operation.	No security checking is performed on this operation.

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Import	Use the **Import** menu option to import configuration information for an object. Imported files must be in XML format. The configuration information in the XML file is used to create new objects as descendants of the originally selected object in the Defined View or Prototype View.	• CREATE authority for the selected object	None
Modify a base object	Use the **Select base object** > **Modify base object** menu option to modify a base object.	• READ authority for the selected object • UPDATE authority for the base object	None
Modify a cluster queue	Select a cluster queue in a managed cluster and modify the attributes of the cluster queue.	• UPDATE authority for the cluster queue	None
Modify a cluster queue manager	Select a cluster queue manager in a managed cluster and modify the attributes of the cluster queue manager.	• UPDATE authority for the managed cluster	None
Modify a managed cluster	Select a managed cluster and modify the cluster attributes.	• UPDATE authority for the managed cluster	None
Modify a prototype object	Select a prototype object and modify its attributes. Attributes of the defined object that is created based on this prototype are updated automatically.	• UPDATE authority for the selected prototype object	None

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Modify a scheduled action	Use the **Schedules** > **View** menu option to view the Scheduled Action Report window, and modify the selected schedule.	• UPDATE authority for the schedule For information about how to grant authorities for schedules, see "Granting authorities for viewing, deleting, or modifying schedules to a user or group" on page 128.	None
Move a defined object	Use the drag-and-drop operation in Defined View to move a defined object.	• DELETE authority for the selected object • DELETE authority for all resources that are included in the selected object • UPDATE authority for the object that contains the selected object • CREATE authority for the object to which the selected object is dragged	None
Open settings for base object	Use the **Open settings for base object** menu option to open up the settings list for the base object of the placeholder.	• READ authority for the selected object • READ authority for the base object	None
Refresh	Use the **Refresh** menu option to update the defined or prototype view tree display of the selected object.	No security checking is performed on this operation.	No security checking is performed on this operation.
Regenerate cluster managed objects	Use the **Regenerate cluster managed objects** menu option to cause cluster objects that are defined on one cluster queue manager to be generated on all other queue managers within the cluster. This option is only used when things are altered within the cluster.	• CREATE authority for the managed cluster • CREATE authority for the base queue manager	None

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Replicate	Use the **Replicate** menu option to create copies of the selected object or objects in the Defined View or Prototype View. All copies are created in the same location within the tree hierarchy as the original object from which they were replicated.	• CREATE authority for the object to which the selected object belongs • READ authority for the selected object • READ authority for all resources that are included in the selected object **Remember:** When a cluster is replicated, CREATE authority for the cluster and for all the queue managers that belong to this cluster is required. The WebSphere MQ Configuration agent does not check the authority settings for other objects in the cluster, such as cluster queues.	None
Reset actual exists	In a disaster recovery situation, use the **Reset actual exists** menu option for the selected configured system in the Defined View. Use this option only when a previously discovered WebSphere MQ queue manager is lost and cannot be recovered.	• UPDATE authority for the selected configured system • UPDATE authority for all resources that are included in the selected object	None
Restore the configuration database	Use the `kcfcrstr` command to restore the configuration database from the backup file.	No security checking is performed on this operation.	No security checking is performed on this operation.
Revert to base object	Use the **Revert to base object** menu option to revert all attributes in the selected resource to the values of the base object.	• UPDATE authority for the selected object • READ authority for the base object	None

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Run a scheduled action	After a schedule is created, the scheduled action is enabled to run.	For a scheduled action to run successfully, the user ID that is used to create the schedule must have the required authorities to perform the operations that the scheduled action involves. Required authorities vary depending on the involved operations and objects. **Remember:** As the system administrator, you must grant the required authorities to the user ID that creates the schedule, regardless of the group ID or administration group that the user ID belongs to.	
Run the `MCExport` command	Use the `MCExport` command to export resource configuration from the configuration database to an XML file.	• READ authority for the selected object that is to be exported • READ authority for all resources that are included in the selected object. **Remember:** The administrator must assign authorities to the specific user ID that is used to run this command, regardless of the group ID or administrator group to which the user ID belongs.	None
Run the `MCImport` command	Use the `MCImport` command to import an MCCLI XML file to the configuration database.	• CREATE authority for the selected object **Remember:** The administrator must assign authorities to the specific user ID that is used to run this command, regardless of the group ID or administrator group to which the user ID belongs.	None

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Run the **MCImport** command (with -r option specified)	Use the **MCImport** command to import an MCCLI XML file to the configuration database and overwrite the existing resources.	• CREATE authority for the selected object • DELETE authority for the object that is to be overwritten and all resources that are included in the overwritten object • UPDATE authority for the object to which the overwritten object belongs **Remember:** The administrator must assign authorities to the specific user ID that is used to run this command, regardless of the group ID or administrator group to which the user ID belongs.	None
Run the **MCRunSchedule** command	Use the **MCRunSchedule** command to submit a command to trigger an on-demand scheduled action.	**Remember:** No security checking is performed on this operation. And only the user ID that is used to create the schedule can trigger the scheduled action with the **MCRunSchedule** command.	
Select a base object	Use the **Select base object** menu option to navigates to, and select, the base object for the placeholder.	• READ authority for the selected object **Remember:** If the user wants to read the base object, READ authority for the base object is required. If the user wants to modify the base object, UPDATE authority for the base object is required.	None
Show audit log	Click **Show Audit Log** to list all logs for previously-performed actions.	• READ authority for the audit log For information about how to grant authorities for audit logs, see "Granting authorities for accessing audit log to a user or group" on page 127.	None

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Show using	Use the **Show using** menu option on a selected prototype in the Prototype View to determine which objects use this prototype.	• Read authority for the selected prototype	None
Start a queue manager or channel	Click **Action** > **Start** to start the selected queue manager or channel.	• READ authority for the selected queue manager or channel	• EXECUTE authority for the selected queue manager or channel
Stop a queue manager or channel	Click **Action** > **Stop** to stop the selected queue manager or channel.	• READ authority for the selected queue manager or channel	• EXECUTE authority for the selected queue manager or channel
Submit MQ commands	Click **Action** > **Submit MQ command** and enter the WebSphere MQ command to submit to the selected queue manager.	• READ authority for the selected queue manager	• EXECUTE authority for the selected queue manager
Update actual from defined	Use the **Update** > **Actual from defined** menu option to update your actual configuration to match the defined configuration in general, if any differences exist.	• READ authority for the selected object • READ authority for all resources that are included in the selected object	• EXECUTE authority for the selected object • EXECUTE authority for all resources that are included in the selected object

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
Update defined from actual	Use the **Update > Defined from actual** menu option to update the defined configuration to match your actual WebSphere MQ configuration.	• UPDATE authority for the selected object • UPDATE authority for the resources that are included in the selected object • CREATE authority for the related queue manager (if new resources are to be created for the queue manager in the configuration database) • DELETE authority for the related resource (if the resource is to be deleted from the configuration database) **Remember:** This operation can be partially approved by WebSphere MQ Configuration agent. The operation on the objects with appropriate authorities can be approved, but the operation on the objects without appropriate authorities are denied.	• READ authority for the selected object • READ authority for all resources that are included in the selected object
Validate	Use the **Validate** menu option to test the definitions in your configuration database to ensure that objects are properly defined. Validation checks if correct values are entered in fields within the settings list of an object, and that no duplicate resources exist. This operation validates the selected object or objects and their descendants.	No security checking is performed on this operation.	No security checking is performed on this operation.

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
View a cluster queue	Select a cluster queue in a managed cluster and view the attributes of the cluster queue.	• READ authority for the cluster queue	None
View a cluster queue manager	Select a cluster queue manger in a managed cluster and view the attributes of the cluster queue manager.	• READ authority for the managed cluster • READ authority for the base queue managers that are dragged to the cluster	None
View a managed cluster	Select a managed cluster and view the cluster attributes.	• READ authority for the managed cluster	None
View a scheduled action	Use the **Schedules** > **View** menu option to view the Scheduled Action Report window.	• READ authority for the schedule For information about how to grant authorities for schedules, see "Granting authorities for viewing, deleting, or modifying schedules to a user or group" on page 128. **Remember:** • The ID must have READ authority for the schedule (not the object that the schedule is created against) to view the schedule. Otherwise, the schedule is not displayed in the Scheduled Action Report window. • If this operation is used by the user ID that created this scheduled action, the operation is approved by WebSphere MQ Configuration agent without security checking.	None

Table 15. Access authorities required for different operations (continued)

Operation	How to use the operation	Configuration database authorities required	WebSphere MQ authorities required
View actual	Use the **View** > **Actual** menu option to query the WebSphere MQ queue manager to obtain the actual values of the selected object in the Defined View.	None	• READ authority for the selected object
View authorities	Use the **View** > **Authorities** menu option to view the WebSphere MQ authorities in effect for objects in the selected configured system in the Defined View.	• READ authority for the selected object	None
View discrepancies	Use the **View** > **Discrepancies** menu option to evaluate the difference between the defined and actual resource definitions for an object and display any conflicts. If the selected object contains other objects, the action is also applied to the contained objects.	This operation can be partially approved by WebSphere MQ Configuration agent. The discrepancies of the objects only for which READ or higher authority is granted can be displayed in the result. The discrepancies of the objects for which no appropriate authority is granted are not shown.	
View resolved	Use the **View** > **Resolved** menu option on a selected object in the Defined View to view resolved global variables or symbolic variables.	• READ authority for the selected object	None

Chapter 8. Scheduling actions

With the action scheduling function, you can perform the following tasks:

- Compare your defined configuration to your actual WebSphere MQ configuration at specified intervals.
- Back up the configuration database at specified intervals.
- Schedule an action against one or more objects in the configuration database.
- View scheduled actions and their status information in scheduled action reports.
- Save the contents of the scheduled action report to a log file after the action has run, or optionally export the data to a specified file after the action has run. (You can use the file that is saved as input for independent software-vendor reporting utilities.)
- View scheduled action failures as Tivoli Enterprise Portal alerts.
- Optionally, run a scheduled action on demand using an activity program in a policy.

When you make changes to your defined configuration or actual WebSphere MQ configuration, you want to update or compare these configurations to keep them synchronized. However, performing these actions as configuration changes are being made, or during regular business hours, might result in a slower response time and a delay in your configuration activities. Additionally, you might be working with configurations in different time zones and want to schedule actions based on the time of day in a particular time zone. Using the action scheduling function, you can schedule an action to run weekly, daily, hourly, or every *n* hours in specified time zones. You can also schedule an action to run on demand using an activity program in a policy.

You can schedule one of the following actions for one or more objects:

- Update defined from actual
- Update actual from defined
- View discrepancies
- Delete (defined, actual, or both actual and defined)
- Validate
- Discover new resources
- Back up configuration database

You can also schedule an action to run based on the time where the Tivoli Enterprise Portal client is located or where the configured system is located.

The action scheduling function provides reports that you can use to view the nature and status of scheduled actions. WebSphere MQ Configuration agent provides the following reports:

- Scheduled Action Summary
- Scheduled Action Details
- Scheduled Action Status

Guidelines for scheduling an action

Use these guidelines when scheduling an action:

- You must be in update mode to schedule an action.
- You must have authority to update the target object.
- The object cannot be locked by someone else who is performing an action on the object in update mode.
- The object cannot be part of another scheduled action.
- The system checks scheduled actions every 5 minutes and performs all scheduled actions that have become ready to run in the past 5 minutes. Therefore, there is a delay of up to 5 minutes between the time at which an action is scheduled to run, and the time at which it actually runs.

Scheduling an action

Do the following steps to schedule an action:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. In the Defined View, right-click the object for which you want to schedule an action and click **Schedules** > **Create**.
3. Enter a name for your new scheduled action and click **OK**. The Scheduled Action settings list is displayed. In this list you can specify and schedule the action. If you are scheduling multiple actions for the same parent object and the name that you assign to this scheduled action already exists in the configuration database, the number 1 is appended to the scheduled action name. If you create another scheduled action with the same name, this number is incremented by 1.
4. Use the Name section to specify the following information:
   - The name and description of the scheduled action.
   - Whether the scheduled action should continue to run after a failure on one of the target objects when more than one target object was originally selected.
   - Whether the scheduled action is enabled. To run the scheduled action, you must select the **Enabled** check box.
   - Whether to preserve the integrity of target objects and their descendants or ancestors. This prevents another user from making any updates to target objects or their descendants or ancestors when the scheduled action is enabled.
   - The type of action to perform.
5. Use the Time section to specify the following information:
   - When the scheduled action should run
   - Whether the times specified are relative to the Tivoli Enterprise Portal client or the configured system that contains the target object or objects
   - How often the scheduled action should repeat
   - When the scheduled action should expire
   - Whether the scheduled action should be performed on a specified schedule or issued by a policy

6. Use the Detail section to view the target object or objects as part of its configured system or systems and configured system group.
7. Use the Save section to specify the following information:
   - Whether to make the scheduled action report data eligible for saving. To save the scheduled action report output later, you must first select the **Save output** check box.
   - Whether this is a one-time-only scheduled action that should be deleted after the report data is saved
   - The format of the saved report data
   - The level of detail of the saved report data
   - Whether this is a one-time-only save request
   - The file name and location of the saved report data
8. Click **Save** to save your changes.

Related tasks:

"Deleting a scheduled action" on page 200

Scheduled actions in multiple time zones

When the execution time of a scheduled action that targets multiple queue managers is specified as relative to the **Conf. System** variable, WebSphere MQ Configuration agent attempts to perform the action according to the local time of each target queue manager. Generally this means that the action is started for the eastern-most target first, then proceeds westward.

For example, suppose you have queue managers in London (GMT), New York (EST), and San Francisco (PST), and a Tivoli Enterprise Monitoring Server located in Salt Lake City (MST). You define a single scheduled action for all three queue managers. You specify that the action must run at midnight and cannot run after 2:00 a.m. and select **Conf. System** as the time zone.

At approximately 5:00 p.m. in Salt Lake City (midnight in London), the scheduled action starts running. It starts performing the requested action on the London queue manager. When the action is completed, the scheduled action waits until 10:00 p.m. Mountain time (midnight in New York), then starts performing the action on the New York queue manager. While the scheduled action is waiting between targets, its status is RUNNING. At 1:00 a.m. Salt Lake City time, the requested action is performed on the queue manager in San Francisco. Only when the requested action is performed against all the selected targets is the scheduled action considered complete.

If two or more target configured systems are located in the same time zone, the scheduled action is performed on these systems at the same time.

Modifying a scheduled action

If you have the correct authorization, you can modify a scheduled action from the Scheduled Action Summary report.

To modify an existing scheduled action:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. In the Defined View, right-click the configured system group that is associated with the scheduled action and click **Schedules** > **View**.
3. Select the action that you want to modify, and click **Edit**. The Scheduled Action settings list is displayed. Modify the scheduled action as necessary. Click **Help** at the bottom of the Scheduled Action settings list for detailed descriptions of each field.
4. Click **Save** to save your changes.
5. On the Scheduled Action Summary report, click **Refresh** to update the report.

Related tasks:

“Deleting a scheduled action”

Deleting a scheduled action

To delete a scheduled action, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. In the Defined View, right-click the configured system group that is associated with the scheduled action and click **Schedules** > **View**.
3. Select the action that you want to delete, and click **Delete**.

Tip: Use caution when deleting scheduled actions, because you cannot undo a deletion.

Related tasks:

“Scheduling an action” on page 198

“Modifying a scheduled action” on page 199

Scheduled Action Summary report

The Scheduled Action Summary report shows one row for each scheduled action that you create. It provides general information about each scheduled action, such as its status, its time zone, and the type of action that you schedule.

From the Scheduled Action Summary report, you can do the following tasks:

- View a Scheduled Action Details report showing all the targeted objects of a particular scheduled action.
- Modify an existing scheduled action. This action must be performed in update mode.
- Delete a scheduled action. This action must be performed in update mode.
- Save the output of a scheduled action report to a file after the action runs. This action must be performed in update mode.

To access the Scheduled Action Summary report:

In the Defined View, right-click the configured system group that is associated with the scheduled action and click **Schedules** > **View**.

Saving Scheduled Action Report output

You can save the output data that is associated with a scheduled action to a file, but this is not an automatic process. If you decide to save the report data to a file after the scheduled action runs, you must do a few steps from the Scheduled Action Summary Report. You can use the file that you save as input for independent software-vendor reporting utilities.

When you create or modify a scheduled action, if you intend to save the scheduled action report output data to a file, complete the **Save** section. In that section, ensure that you select the **Save output** check box to make the data eligible for saving.

When viewing the Scheduled Action Summary Report, data that is eligible for saving indicates `Yes` in the **Save** column.

To save the output of a scheduled action report to a file:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. In the Defined View, right-click the configured system group that is associated with the scheduled action and click **Schedules** > **View**.
3. Select an action that was already run and has data that you want to save to a file. Ensure that the selected action indicates `Yes`, or `Yes/Once`, or `Yes/Delete` in the Save column of the Scheduled Action Summary report.
4. Click **Save Output** to save the output. The output is saved to the file that is specified in the Save section of the Scheduled Action settings list. The default save file location is the logs directory. This directory is relative to the current working Tivoli Enterprise Portal directory (for example C:\IBM\ITM\CNP). The default file name is the name of the scheduled action with the extension `.txt`. If the save file for a particular scheduled action already exists, subsequent output is appended to the end of the file; several scheduled actions can use the same file name.

Scheduled Action Details report

The Scheduled Action Details report contains a row for each object that is targeted for a scheduled action and includes the following information:

- The name of the object that is targeted for a scheduled action
- The actual start and end time of the scheduled action
- The status of the action
- The configured system that the target object belongs to
- The ancestors of the object in the tree hierarchy

Viewing the Scheduled Action Details report

To view the Scheduled Action Details report, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. In the Defined View, right-click the configured system group that is associated with the scheduled action and click **Schedules** > **View**.
2. Select a scheduled action that was already run and that you want to know more about and click **Details**. The Scheduled Action Details report is displayed.

Scheduled Action Status report

The Scheduled Action Status report shows the status of failed actions after the actions are completed. It contains the following detailed information about the failed actions:

- The name of the configured system in which the error was detected
- The name and type of the object for which the error was detected
- The type of error that was encountered
- For a discrepancy, the type of discrepancy
- If the error was a discrepancy, the defined configuration value and the actual configuration value of the property

Viewing the Scheduled Action Status report

To view the Scheduled Action Status report, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. In the Defined View, right-click the configured system group that is associated with the scheduled action and click **Schedules** > **View**.
3. Select a scheduled action that was already run and click **Details**. The Scheduled Action Details report is displayed.
4. Select the scheduled action that you want to know more about and click **Status**. The Scheduled Action Status report is displayed.

Running a scheduled action on demand

Tivoli OMEGAMON DE users with the Policy Management solution offering enabled can build OMEGAMON policies to implement more complex workflow strategies than are possible with situations alone.

Policies and the Workflow editor are described in *Administering OMEGAMON Products: Tivoli Enterprise Portal* and the Tivoli Enterprise Portal online help.

With the Tivoli OMEGAMON DE Policy Management solution offering enabled, you can create a scheduled action to run on demand by creating a policy that uses the product-provided Run_OnDemand_Config_Action activity program. When the situations within a policy become true, the scheduled action runs.

To access the Workflow Editor, select Workflow Editor from the Tivoli Enterprise Portal tool bar.

Important: This function is displayed only if the Tivoli OMEGAMON DE Policy Management solution offering is enabled.

For more information about creating policies and for instructions for assigning authority to users, see *Administering OMEGAMON Products: Tivoli Enterprise Portal* and the Tivoli Enterprise Portal online help.

Chapter 9. Creating and defining clusters

WebSphere MQ Clustering is a powerful function that provides ease of administration for WebSphere MQ customers, a means of dynamic workload balancing.

You can define clusters as explicit objects in the Defined View. You can perform the following tasks on clusters:

- Manage clusters as other types of existing configuration objects
- Define clusters
- Delete clusters
- Drag clusters
- Modify clusters

Objects that are logically associated with the cluster, such as queue managers and cluster queues, are shown in the defined view tree as subordinate objects.

Clustering terminology

The following terms are associated with the Clustering function:

Cluster

A cluster is a network of queue managers that are logically associated in some way. The queue managers in a cluster can be physically remote.

Repository

A repository is a collection of information about the queue managers that are members of a cluster. A full repository is a complete set of information about the cluster.

Cluster queue manager

A cluster queue manager is a queue manager that is a member of a cluster. A queue manager can be a member of more than one cluster. Each cluster queue manager must have a name that is unique throughout all the clusters of which it is a member.

A cluster queue manager can host queues, which it broadcasts to the other queue managers in the cluster.

Full repository queue manager

A full repository queue manager contains all the information about the cluster. Typically, not every queue manager in a cluster contains a full repository.

You must specifically designate full repository queue managers. Other queue managers contain only a subset of the information about a cluster.

You should designate at least one, preferably two, or possibly more queue managers as full repository queue managers for each cluster.

Cluster queue

A cluster queue is a queue that is hosted by a cluster queue manager. The cluster queue manager makes a local queue definition for the queue. This has the effect of advertising the queue to the other queue managers in the cluster. The other queue managers in the cluster can put messages to a cluster queue without needing a corresponding remote queue definition.

Cluster-receiver channel
A cluster-receiver channel definition defines a channel on which a cluster queue manager can receive messages from other queue managers in the cluster.

Cluster-sender channel
A cluster-sender channel definition defines a channel on which a cluster queue manager can send messages to one of the full repository queue managers.

Configuration placeholder object
An object in the defined view tree that acts as a placeholder for another object in the configuration.

Placeholder objects are required to preserve the hierarchical structure of the configuration data.

Virtual configuration object
A defined object that is represented in WebSphere MQ Configuration agent that does not have a one-to-one correspondence to an actual object, but that can provide information about how other defined objects are to be created and configured.

Product-managed configuration object
A defined object that is dynamically created and managed by WebSphere MQ Configuration agent. Product-managed configuration objects are displayed in the defined view tree, and you can view the properties of the object; however, certain properties of the object cannot be modified directly. A product-managed configuration object is usually related to a virtual configuration object; you can indirectly control a product-managed configuration object by manipulating the related virtual configuration object.

Product-managed cluster
A product-managed cluster is a virtual configuration object that represents a WebSphere MQ cluster that you want WebSphere MQ Configuration agent to completely manage. The cluster is represented by an object in the configuration hierarchy at the configured system level.

The descendant objects of a product-managed cluster are cluster queue manager configuration objects, cluster queue configuration objects, or resource groups that contain cluster queue configuration objects. You can define prototypes for product-managed clusters.

Cluster queue manager configuration object
A cluster queue manager configuration object is a configuration placeholder object that represents the participation of a queue manager in a cluster. The object serves as a placeholder for a defined queue manager located elsewhere in the configuration tree.

A cluster queue manager configuration object is always subordinate to a product-managed cluster; you create it by dragging a defined queue manager onto the product-managed cluster.

Cluster queue configuration object
A cluster queue configuration object is a virtual configuration object that represents one or more cluster queues within a cluster, all of which have the same queue name. A cluster queue configuration object provides the

specifications for the definitions of each of the cluster queues. The settings list for a cluster queue configuration object indicates the queue managers on which the cluster queue is to be defined.

A cluster queue configuration object is always subordinate to a product-managed cluster. The object can be subordinate to a resource group within a product-managed cluster. A cluster queue configuration object can be based on a local queue prototype object; if so, any product-managed local queues created from the cluster queue object is also based on the local queue prototype object.

Product-managed configuration objects

There are two product-managed configuration objects: configuration placeholder objects and virtual configuration objects.

A configuration placeholder object is a placeholder for another object in the configuration. The placeholder object contains a reference to the other object, which is referred to as the base object. The placeholder object has properties that are accessible through the settings list for placeholder object.

There are three menu options for placeholder objects:

- **Open settings for base object**: This option opens the settings list for the base object of the placeholder.
- **Select base object**: This option navigates to, and selects, the base object of the placeholder object.
- **Regenerate cluster managed objects**: This option causes cluster objects that are defined on one cluster queue manager to be generated (defined) on all the other queue managers within the cluster.

Virtual configuration objects direct how other application-specific objects are to be defined. They do not directly correspond to an actual application-specific object.

Creating a new managed cluster: a typical scenario

All actions of the Clustering function are accessible from the Defined View. The following example describes how the function works.

Suppose that your company uses WebSphere MQ Configuration agent and your company recently migrated to a version of WebSphere MQ that supports clustering. You want to define a cluster consisting of four queue managers, QM1, QM2, QM3, and QM4. Assume that these queue managers are already defined in WebSphere MQ Configuration agent.

Tip: When you build the cluster environment, do all the required preparation steps and run the **Update** operation on the entire environment to synchronize the definition of resources in the actual WebSphere MQ environment with their counterparts in the configuration database.

Limitation: When you build a managed cluster environment, cluster channels are created automatically by the WebSphere MQ Configuration agent. The default cluster channel name is CH.2.&*QMGR*&<1:4>4.&*CLUSTER*<1:8>, where *QMGR* is the first 4 characters of the queue manager name and *CLUSTER* is the first 8 characters of the cluster name. If the first 4 characters of the queue manager names are exactly the same, the resulting channel names are the same. In this case, you have to create the cluster channels manually with unique names. To differentiate the cluster channels that are automatically created, make sure that the first 4 characters of the queue manager names are unique before you drag the queue managers to a managed cluster.

Creating a new managed cluster

Use the following procedure as an example to create a new managed cluster:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. For information about how to enter update mode, see “Entering update mode” on page 18.
2. Open the Defined View.
3. In the defined view tree, right-click the configured system group that is to contain the cluster and click **Create** > **Managed Cluster**.

   Remember: When you create a new managed cluster, make sure that the name of the cluster is unique. If another managed cluster with the same name already exists under a different configured system group, the two clusters might have different status records, none of which records the real situation of the cluster queue managers.
4. When prompted to provide a name, enter the name `new_cluster` and click **OK**.

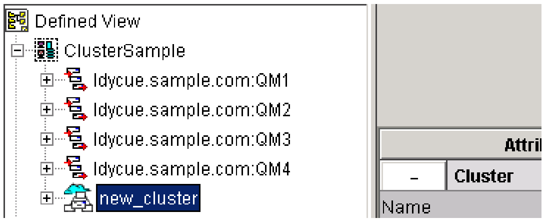
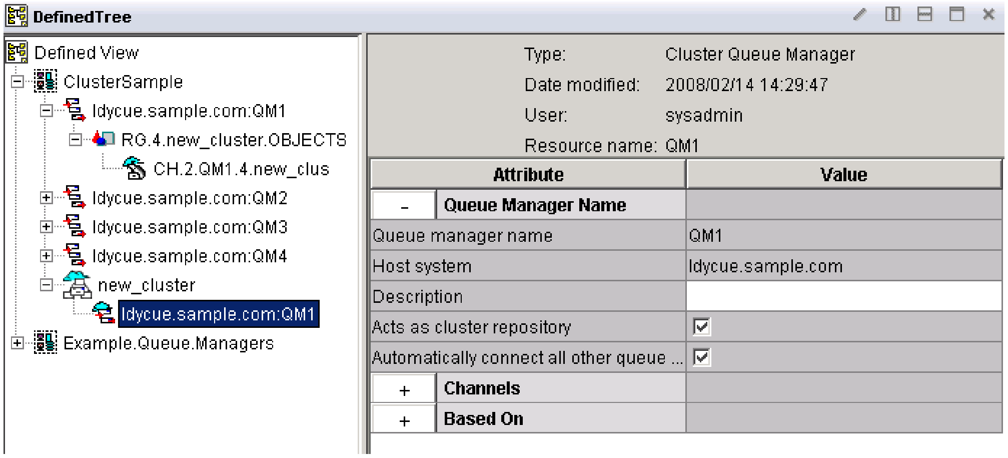


Figure 56. Creating a new managed cluster

   The new cluster is displayed in the defined view tree in the original configured system group. It has no subordinate objects.

5. Do the following procedure for both QM1 and QM2, to define them as full cluster repositories:
   a. Drag the icon of the queue manager to the managed cluster. A window is displayed prompting you to indicate whether to include the new item in the cluster.
   b. Click **YES** if the names are correct. A cluster queue manager configuration object with the same name as the queue manager is created under the new_cluster cluster. The cluster queue manager configuration object contains an internal reference to the queue manager from which it was created. The original object is the base object.
   c. Select the cluster queue manager configuration object under the new_cluster cluster. The settings list for the object is displayed on the right side of the Defined View. An example is shown in Figure 57 on page 209.



DefinedTree

Defined View
- ClusterSample
  - ldycue.sample.com:QM1
    - RG.4.new_cluster.OBJECTS
      - CH.2.QM1.4.new_clus
  - ldycue.sample.com:QM2
  - ldycue.sample.com:QM3
  - ldycue.sample.com:QM4
  - new_cluster
    - ldycue.sample.com:QM1
- Example.Queue.Managers

Type: Cluster Queue Manager
Date modified: 2008/02/14 14:29:47
User: sysadmin
Resource name: QM1

Attribute	Value
- Queue Manager Name	
Queue manager name	QM1
Host system	ldycue.sample.com
Description	
Acts as cluster repository	☑
Automatically connect all other queue ...	☑
+ Channels	
+ Based On	

Figure 57. A cluster's settings list

d. Select the **Acts as cluster repository** check box in the Queue Manager Name section of the Cluster Queue Manager settings list to indicate that the original queue manager (the base object) acts as a full repository for the cluster.

e. Select the **Automatically connect all other queue managers** check box. Other queue managers in the cluster automatically connect to the cluster repository.

f. Click **Save** to save your changes.

Remember: In each cluster you must select at least one, preferably two, or possibly more of the queue managers to hold full cluster repositories. A cluster can work quite adequately with only one full repository, but using two improves availability. Interconnect the full repository queue managers by defining cluster-sender channels between them.

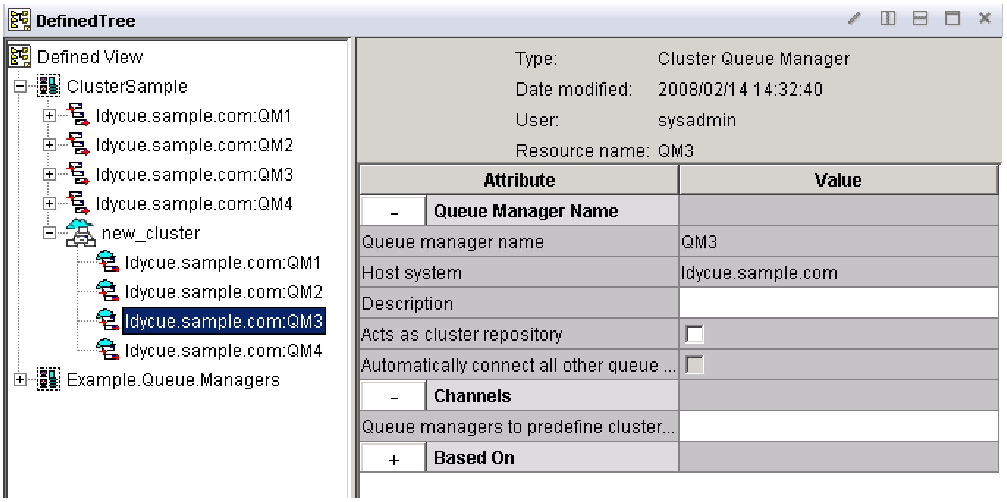
6. Do the following procedure for both QM3 and QM4 queue managers:

a. Drag the icon of the queue manager to the new_cluster cluster. This creates a cluster queue manager configuration object under new_cluster. A window is displayed prompting you to indicate whether to include the new item in the cluster.

b. Click **Yes** if the names are correct.

c. Select the cluster queue manager configuration object. The settings list for the object is displayed on the right side of the Defined View.

d. In the Queue Manager Name section of the settings list for the object, ensure that the **Acts as cluster repository** check box is cleared. This ensures that the original queue manager (the base object) does not act as a full repository for new_cluster. An example of the settings list is shown in Figure 58 on page 210.



Type: Cluster Queue Manager
Date modified: 2008/02/14 14:32:40
User: sysadmin
Resource name: QM3

Attribute	Value
- **Queue Manager Name**	
Queue manager name	QM3
Host system	ldycue.sample.com
Description	
Acts as cluster repository	□
Automatically connect all other queue ...	□
- **Channels**	
Queue managers to predefine cluster...	
+ **Based On**	

Figure 58. Queue cluster manager settings list: channels

e. Click **Save** to save your changes.

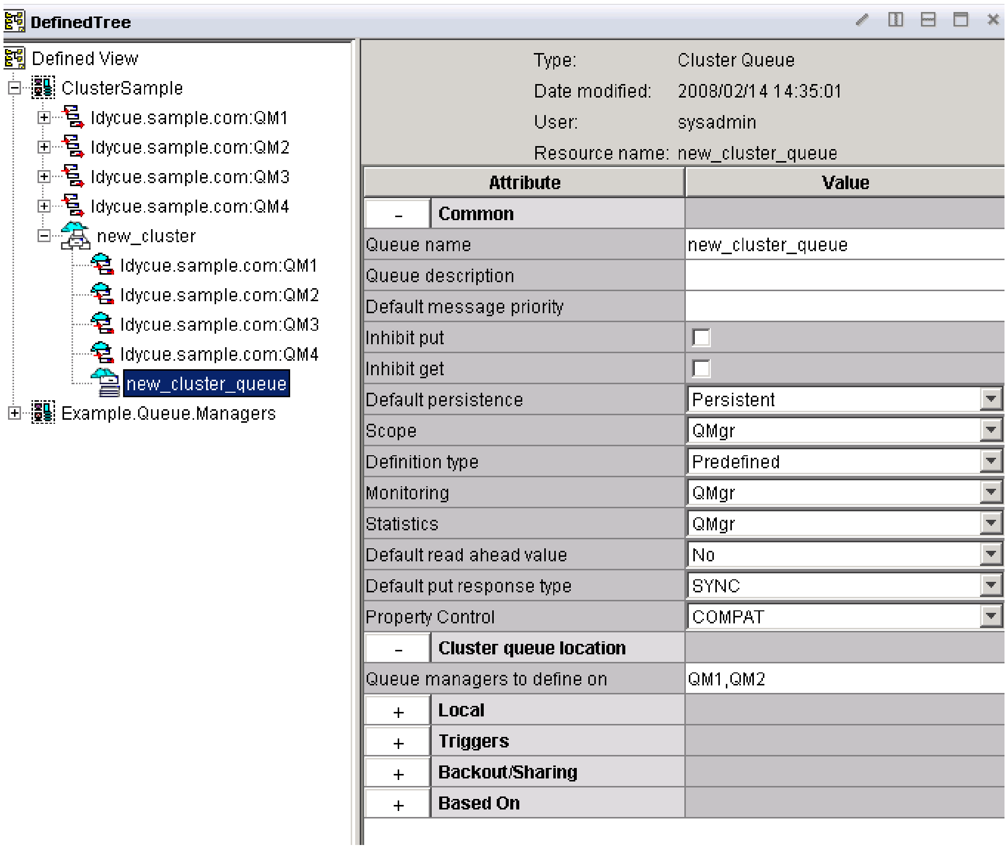
7. Do the following procedure to create a cluster queue:

   a. Right-click the new_cluster cluster and click **Create** > **Cluster Queue**. You are prompted to supply a name for the new object.

   b. Enter the name `new_cluster_queue` and click **OK**. A cluster queue configuration object is created under the new_cluster cluster.

   c. Select **new_cluster_queue**, the cluster queue configuration object. The settings list for the object is displayed on the right side of the Defined View.

   d. In the **Cluster queue location** section of the settings list, select **QM1** and **QM2** to indicate that the new cluster queue is to be defined on QM1 and QM2, which is shown in Figure 59 on page 211



Type: Cluster Queue
Date modified: 2008/02/14 14:35:01
User: sysadmin
Resource name: new_cluster_queue

Attribute	Value
- Common	
Queue name	new_cluster_queue
Queue description	
Default message priority	
Inhibit put	□
Inhibit get	□
Default persistence	Persistent
Scope	QMgr
Definition type	Predefined
Monitoring	QMgr
Statistics	QMgr
Default read ahead value	No
Default put response type	SYNC
Property Control	COMPAT
- Cluster queue location	
Queue managers to define on	QM1,QM2
+ Local	
+ Triggers	
+ Backout/Sharing	
+ Based On	

Figure 59. Queue cluster manager settings list: cluster queue location

e. Click **Save** to save your changes.

8. Run the **Validate** operation at the cluster level to verify that the cluster definitions are correct. Running the **Validate** operation ensures that the cluster definitions meet the following requirements:
   - There is at least one full repository cluster queue manager.
   - The definition of each cluster queue manager specifies that a cluster sender channel should be defined back to each full repository for the cluster.
   - The definition of each cluster queue configuration object indicates the queue is to be defined on at least one queue manager in the cluster.
   - The definition of each cluster queue configuration object does not conflict with any other cluster queue objects that have the same name and that might reside on one or more of the same queue managers.
9. Refresh QM1 and QM2 by doing the following steps:
   - In the defined view tree, right-click the QM1 (the base object) queue manager and click **Refresh**.

     WebSphere MQ Configuration agent recognizes that a cluster to which the queue manager belongs is modified, and applies the cluster definition to the defined queue manager. This causes the following processes to occur:
     – The definition of the queue manager is modified; the Clusters section of its settings list is modified to indicate that the queue manager acts as a full repository for the new_cluster cluster.
     – A new resource group is created under the queue manager. The resource group contains each new resource that is created by WebSphere MQ

Configuration agent. The name of the resource group is derived from the settings list for the new_cluster cluster.

  – New cluster receiver and cluster sender channels are defined within the new resource group. The specifications for these channels are again derived from the settings list for the new_cluster. The new channels are associated with the new_cluster cluster.
  – The local queue definitions for the new_cluster_queue queue are created in the new resource groups of the queue managers. The details of the local queue definitions are derived from the settings list for the new_cluster_queue cluster queue configuration object. The Clusters section of each local queue definition indicates that the queue is associated with the new_cluster cluster.
- In the defined view tree, right-click the QM2 (the base object) queue manager and select **Refresh**.

10. In the defined view tree, right-click **QM3** and **QM4** (the base objects) and select **Refresh** for each of them. In the new resource groups of the queue managers, a new cluster sender channel is created for each queue manager in the cluster that acts as a cluster repository. These sender channels have the same names and specifications as the cluster receivers on the queue managers that act as cluster repositories.
11. One by one, select **QM1**, **QM2**, **QM3**, and **QM4**, right-click, and click **Update** > **Actual from defined** to update your WebSphere MQ environment. This action causes the appropriate cluster definitions to be made at the actual queue managers.

    Tip: When you create a new channel inside a cluster, if another channel with the same name already exists on the same queue manager, a suffix is automatically appended to the channel name to distinguish it from the existing channel. However, if the channel is part of a pair of sender/receiver channels, the channel name is different from the other channel in the pair and validation fails. In this case, you must rename the channel so that their names are identical and there are no other channels with the same name on the same queue manager. This does not apply to validation of channels outside of clusters.

Audit log

When product-managed configuration objects are created, modified, or deleted as a result of a change to a cluster definition request, entries are added to the configuration audit log to display the change. The entries in the audit log are flagged to indicate that the changes were made as a result of a change to a virtual configuration object.

Cluster queues based on local queue prototypes

You can build a cluster queue configuration object from a local queue prototype by dragging the prototype directly to the target managed cluster, or to a resource group within the managed cluster. Any local queues that are subsequently created from this cluster queue object are also based on the local queue prototype.

Controlling product-managed configuration objects

You can control the properties and characteristics of the various product-managed configuration objects that are created and managed by the Clustering function.

Queue manager objects in clusters

For queue managers that are defined as full repositories for one or more managed clusters, WebSphere MQ Configuration agent sets the cluster name of the repository and the namelist in the Clusters section of the Queue Manager settings list.

If the queue manager is a full repository for a single cluster, the **Cluster name** field contains the name of the cluster.

If the queue manager is a full repository for more than one cluster, the **Cluster name** field is blank, and the **Namelist** field contains the name of the namelist containing the cluster names.

Resource group objects for clusters

When a queue manager participates in a managed cluster, WebSphere MQ Configuration agent creates one or more resource groups in the queue manager; the groups contain any product-managed configuration resources that are generated.

For each cluster that the queue manager is a member of, a resource group is created to contain those resources that are specifically related to the cluster. The name of the resource group is specified in the Resource Group Name field in the Cluster Resources section of the Cluster settings list. The default value for this field is RG.4.&CLUSTER<1:35>..OBJECTS; The value of &CLUSTER<1:35> indicates that the first 35 characters of the CLUSTER symbolic variable are included in the resource group name. Because WebSphere MQ Configuration agent assigns the name of the cluster to the CLUSTER symbolic variable within the resource group definition, by default the name of the resource group contains the first 35 characters of the cluster name.

For example, if the QM1 queue manager is a member of the CLUSTERA managed cluster, the resource group in QM1 that contains all resources specifically related to the CLUSTERA cluster is named RG.4.CLUSTERA.OBJECTS.

WebSphere MQ Configuration agent might also create a resource group that contains product-managed configuration resources that are not related to a specific managed cluster. Typically, this resource group contains the namelist definitions that are generated when a queue manager is part of multiple managed clusters. The name of this non-cluster specific resource group is provided in the Resource group name field in the Clusters section of the Queue Manager settings list; the default for this field is RG.FOR.CLUSTER.OBJECTS.

Cluster receiver channel objects for clusters

If a queue manager is participating in one or more managed clusters, WebSphere MQ Configuration agent creates a definition for at least one cluster receiver channel for the queue manager. The name for the cluster receiver channel is derived from one of the following names:

- The Cluster Receiver Name in the Cluster Resources section of the Managed Cluster settings list
- The Cluster receiver name in the Clusters section of the Queue Manager settings list

Tip: If both fields are specified, the name in the Managed Cluster settings list is used.

The default value for the Cluster Receiver Name field for a managed cluster is CH.2.&QMGR<1:4>.4.&CLUSTER<1:8>. Because WebSphere MQ Configuration agent assigns the value of the queue manager name to the QMGR symbolic variable, and it assigns the name of the managed cluster to the CLUSTER symbolic parameter, the resulting channel name contains the first 4 characters of the queue manager name and the first 8 characters of the cluster name.

For example, if the QM1 queue manager is a member of the CLUSTERA managed cluster, by default a cluster receiver channel named CH.2.QM1.4.CLUSTERA is created. The cluster receiver channel is located in the RG.4.CLUSTERA.OBJECTS resource group.

If the Cluster Receiver Name in the Cluster settings list is blank, the value in the Clusters section of the Queue Manager settings list is used instead. The default value for this field is CH.2.&QMGR<1:15>, implying that the first 15 characters of the queue manager name are used in the channel name.

If the queue manager is a member of more than one cluster, by default a separate cluster receiver channel is created for each cluster. However, you can define the configuration so that a single cluster receiver channel can be shared across multiple clusters. If the name that you specify for the cluster receiver channel is the same for more than one cluster (this can happen only when the cluster name is not part of the channel name), a single cluster receiver channel is generated. The definition of the cluster receiver channel refers to a cluster namelist that contains the names of each cluster that the channel is associated with.

Cluster receiver channel prototype for clusters

You can specify that the cluster receiver channel is based on a prototype. You can specify the name of the prototype either in the Cluster Resources section of the Cluster settings list or in the Clusters section of the Queue Manager settings list. If the name of the cluster receiver channel was obtained from the managed cluster settings, the name of the cluster receiver prototype is also obtained from the managed cluster setting; otherwise, the prototype name is obtained from the queue manager settings.

The following properties are automatically associated with the cluster receiver channel; therefore, you cannot modify them:

Channel name
The name of the cluster receiver channel.

Connection name
The name of the connection that is used by the channel. The connection name is derived from the values in the Auto Start section of the Queue Manager settings list.

Transport type
Derived from the Default Network Protocol property in the Cluster section of the Cluster settings list.

Cluster Name and Cluster Namelist
This is set automatically depending on the names of the managed clusters that the channel is associated with.

You can modify all other properties of the cluster receiver channel.

Cluster sender channels for clusters

Cluster sender channels are generated by WebSphere MQ Configuration agent to provide predefined connections to queue managers that are acting as full repositories. Cluster sender channels are generated for a queue manager that belongs to one of the following categories:

- Each full-repository queue manager in the cluster that has the **Automatically connect all other queue managers in the cluster** check box selected in the Queue Manager Name section of the Cluster Queue Manager settings list.
- Each queue manager that is specified in the **Queue Managers to predefined Cluster Sender Channels** field in the Channels section of the Cluster Queue Manager settings list.

The name of the cluster sender channel must match the name of the cluster receiver channel that the sender is to communicate with. Therefore, you have no direct control over the name that is assigned to the cluster sender channel. WebSphere MQ Configuration agent determines the name by locating the cluster receiver channel on the queue manager to be connected to.

The channel name, connection name, and transport type properties of the cluster sender channel are taken from the definition of the corresponding cluster receiver channel, and you cannot directly modify them. The Cluster Name and Cluster Namelist properties are set automatically, depending on the names of the managed clusters that the channel is associated with. You can set all other properties of the channel.

Local queues for clusters

WebSphere MQ Configuration agent generates a local queue for each uniquely named cluster queue that indicates residence on the queue manager. When a cluster queue is defined, you indicate which queue managers the queue is to reside on (in the Cluster Queue Location section of the Cluster Queue settings list). If you select a queue manager name in this section, a local queue is generated within that queue manager.

All properties of the local queue, including its name and the prototype that it is based on, are copied directly from the cluster queue definition.

If you create the cluster queue by dragging a local queue prototype into the managed cluster definition, the generated local queue is also based on the local queue prototype.

If a queue manager is associated with multiple clusters, and two or more cluster queue definitions that have the same name specify that the queue is to reside on the queue manager, the cluster queue definitions are merged to create the local queue. See “Generation of local queues for clusters” on page 216.

Namelists for clusters

WebSphere MQ Configuration agent generates namelists resources on an as-needed basis. Because WebSphere MQ does not allow a resource to refer directly to more than one cluster name, namelists might be required when a queue manager is participating in more than one managed cluster.

- If a resource is associated with more than one cluster, it can refer to a cluster namelist that specifies the names of all the clusters.

- If WebSphere MQ Configuration agent determines that a product-managed configuration object should be associated with more than one cluster, it builds a namelist object that specifies the clusters. The namelist is placed in the resource group that is not associated with a specific cluster. See “Resource group objects for clusters” on page 213.

WebSphere MQ Configuration agent always builds the minimum required number of namelist objects, and allows namelists to be shared among resources that are associated with the same set of clusters.

For example, if two local queues are generated that are both associated with the CLUSTERA and CLUSTERB clusters, WebSphere MQ Configuration agent builds a single namelist that specifies both cluster names, and sets the Cluster namelist property (in the Clusters section of the Queue settings list) in both queue definitions to refer to the same namelist.

The name of the namelist is determined by the Namelist name field (in the Clusters section of the Queue Manager settings list). The Namelist name field provides a prefix for each namelist name that is generated. A numeric suffix is added to each namelist name so that the names are unique.

As you make changes to the definitions of the clusters that a queue manager is participating in, namelist definitions might be automatically created, deleted, or altered by WebSphere MQ Configuration agent.

Generation of local queues for clusters

When two cluster queues with the same name exist in different clusters in the configuration, the potential exists for conflicting definitions, especially if one or more queue managers exist in both clusters.

For example, suppose that the configuration defines CLUSTERA and CLUSTERB managed clusters. The QM1 queue manager exists in both clusters. A QUEUEA cluster queue exists in both CLUSTERA and CLUSTERB managed clusters; in both definitions, you indicated that the QUEUEA cluster should reside on QM1.

As a result of these definitions, WebSphere MQ Configuration agent generates the definition for a QUEUEA single local queue on QM1 and associates the local queue with both clusters. Typically, the properties of the generated local queue are copied directly from the cluster queue, but in this case there are multiple cluster queue definitions, one residing in CLUSTERA managed cluster, and the other in CLUSTERB managed cluster. Which cluster queue is used?

The answer is that they both are. The properties associated with the QUEUEA cluster queue within CLUSTERA managed cluster are merged with the properties that are associated with the cluster queue definition within CLUSTERB managed cluster. If there are conflicting properties, WebSphere MQ Configuration agent detects this as an error, and does not generate the local queue. For example, if the QUEUEA cluster queue definition in CLUSTERA managed cluster set **Maximum Queue Depth** to 500, and the QUEUEA cluster queue definition in CLUSTERB managed cluster set **Maximum Queue Depth** to 1000, WebSphere MQ Configuration agent detects the conflict, and stops the local queue from being generated. The conflict is noted by the configuration manager as a background error. If you validate a cluster queue, the configuration manager detects potential conflicts with other cluster queue objects, and informs you of the conflict.

Modifying objects in a cluster

When you modify a managed cluster, WebSphere MQ Configuration agent checks whether you are authorized to modify the managed cluster and each queue manager participating in the cluster. Likewise, when a cluster queue within the cluster is checked for access, the Span and Scope of Control function also verifies that you have the appropriate authorization to the managed cluster itself, and to all queue managers participating in the cluster.

Important: When you modify objects in a cluster, you might modify, create, or delete objects that are not necessarily the targets of the action, but that are associated with a defined queue manager. For example, when you modify a cluster, WebSphere MQ Configuration agent might attempt to create cluster sender and receiver channels on the cluster queue managers. You must have the appropriate access to the defined queue manager when you drag the queue manager to the managed cluster. You must have ALTER access to the appropriate security profiles (as if attempting to create the channels manually) for this processing to complete successfully.

Important: Do not take the drag and drop action to move the queue manager between clusters when you work on a cluster environment that has been updated to actual. If you want to add a queue manager in a cluster to another cluster, drag the queue manager in the configured system group to the managed cluster instead of dragging it from one cluster to another cluster directly.

Removing a queue manager from a managed cluster

To remove a queue manager which acts as a partial repository from a managed cluster, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Open the Defined View.
3. In the defined view tree, expand the managed cluster that is to be modified. The cluster queue manager configuration object for the queue manager that you want to delete is displayed.
4. Right-click the cluster queue manager configuration object and select **Select base object**.
5. The configuration object for the queue manager is selected. Right-click the queue manager and click **Action** > **Submit MQ command**.
6. In the window that opens, enter the following command that suspends the queue manager:

   ```
   suspend qmgr cluster(clustername)
   ```

   where *clustername* is the name of the managed cluster.
7. Click **OK** to submit the command.
8. Clear the value of Cluster name in the settings list for each cluster channel.
9. Right-click the queue manager and click **Update** > **Actual from defined**.
10. Open the Physical view in the Channel Performance workspace. You can see the message traffic among the cluster channels of all the queue managers within the cluster.

11. After stopping the specified message traffic among the cluster channels of the queue managers within the cluster, open the Defined View and right-click each cluster channel within the queue manager that is to be modified, click **Action** > **Stop** to stop the channels.
12. Open the Physical view, double check in the Channel Performance workspace to make sure that cluster channels of the queue manager that is to be modified are all stopped.
13. In the defined view tree, if it is not already expanded, expand the managed cluster that is to be modified.
14. Right-click the cluster queue manager configuration object for the queue manager that you want to delete and click **Delete** > **Defined**. The queue manager and its defined resources for the cluster are deleted from the defined cluster.
15. Right-click the configuration object for the queue manager and select **Update** > **Actual from defined**. The real cluster resources for the queue manager are removed.
16. Right-click the queue manager that is to be modified and click **Action** > **MQSC Command**.
17. Issue the following command to remove any auto-defined cluster channels:

    ```
    REFRESH CLUSTER(clustername) REPOS(YES)
    ```

    where *clustername* is the name of the managed cluster.

To remove a queue manager that acts as a full repository from a managed cluster, at least one other working queue manager which acts as a full repository in the managed cluster has to be ensured. The procedures for removing a queue manager that acts as a full repository from a managed cluster are similar to the procedures for removing a queue manager inWebSphere MQ. You can refer to the WebSphere MQ help for the further information.

Chapter 10. Audit logging

You can use the audit logging function to view historical records of the changes that you make to your defined and actual configurations using WebSphere MQ Configuration agent. Auditors, WebSphere MQ system administrators, or anyone else interested in checking configuration changes can view this information in a report format.

The following changes are reported:

- Creation of new objects or action schedules
- Deletion of objects or action schedules
- Changes to settings
- Updates to defined or actual objects
- Actual object discoveries
- Prototype disinheritance
- Security violations
- Changes to product-managed configuration objects made as a result of a change to a managed cluster
- Creation of security authorities for non-secure objects
- Updates of security authorities for secure objects
- Deletion of security authorities for secure objects

For performance and storage considerations, archive the audit log on a regular basis.

Disabling audit logging

The WebSphere MQ Configuration agent audit logging function is enabled by default. However, you can deactivate this function.

To disable audit logging on distributed systems, set the KDS_KCF_AUDIT environment variable to NO. And restart the Tivoli Enterprise Monitoring Server to make the change take effect.

- On Windows systems, the KDS_KCF_AUDIT variable is defined in the `*install_dir*\cms\KBBENV` file, where *install_dir* is the installation directory of IBM Tivoli Monitoring.
- On UNIX and Linux systems, it is defined in the *install_dir*/config/kbbenv.ini file.

To disable audit logging on z/OS systems, set the PARMGEN parameter, **KMC_CFG_AUDIT_FLAG**, to NO.

If your Tivoli Enterprise Monitoring Server is on a z/OS system, and you have the Tivoli Enterprise Monitoring Server enhanced security feature enabled, you can control access to the audit log by defining a ADMIN.AUDIT RACF® profile. Users must have READ access to this profile to view audit log reports.

Archiving the audit log

For performance and storage considerations, you should archive the audit log on a regular basis.

Historical disk space requirements for the audit log

Because of the variations in client distributed systems, system size, number of managed systems, and for other reasons, it is difficult to provide actual additional disk space requirements that are necessary for audit log data collection.

The Audit Log table is used for logging changes that are made to your configuration. You can use this table if you are using archiving and conversion functions that are described in the *IBM Tivoli Monitoring Administrator's Guide*, which is available in the IBM Tivoli Monitoring information center. This log data is written only on the Tivoli Enterprise Monitoring Server node and cannot be configured by the historical configuration program.

The Audit Log table has no default HDC table and contains data that is stored in the KCFAUDIT history file. The audit log table stores one 600 byte record for each configuration change. Approximately 59 kilobytes of storage space are required to store historical data collected over a 24 hour period (based on making 100 configuration updates per 24 hour period).

Audit Log reports

These reports contain information about each change to your defined and actual configurations, including the name of the user who made the changes. Depending on the type of configuration change, you can access additional details reports.

Accessing audit log reports

Use the Audit Log workspace to access the Audit Log report.

To view an Audit Log report, do one of the following actions:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

- Specify a custom time period for which you want to view records (using the Start time and End time controls) and click **Show Audit Log**.
- Click one of the predefined time periods for which you want to view records:
  - **Last week log**
  - **Yesterday log**
  - **Last hour log**
  - **Last 15 minutes log**

Accessing additional details reports

An additional details report is available for entries in the Audit Log report that represent update and drag and drop actions. The contents of the report vary according to the type of action.

For update actions, a detailed report contains one row for every property that was altered. Every row contains the name of the property and the value that the property had both before and after it was modified.

For drag actions, a detailed report contains the name of the original configured system, the name of the original parent, and the name of the new parent.

To get additional information for a particular entry in the Audit Log report:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Highlight an entry that contains one of the following actions: DragDrop, Copy, Settings Change, Update Defined.
2. Click **Open as Details**. The Details report opens.

Chapter 11. Backing up and restoring the configuration database

It is good practice to regularly back up the configuration database.

You perform a backup using a Tivoli Enterprise Portal client. The backup process does not interfere with the functioning of WebSphere MQ Configuration agent, and you do not need to stop the Tivoli Enterprise Monitoring Server to run the backup process.

The backup begins only when there are no outstanding deferred database updates pending; the backup also waits until all database commits have completed. While the backup is running, it is possible to fetch records from the database as required by other transactions; however, any deferred database updates that are created while the backup is running remain queued until the backup completes; other update transactions continue to run.

The format of the backup file is system independent; therefore, you can use the backup process to migrate the configuration data from one system to another. If you use FTP, you must specify ASCII format. Also, if you transfer a backup file to a z/OS system, the logical record length (LRECL) of the receiving data should be defined as follows:

```
RECFM=FB,LRECL=440,BLKSIZE=<some multiple of 440>
```

Important: To restore the configuration database, a previous backup of the configuration database must have been performed.

Backing up the configuration database

To back up the configuration database to a file, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Click **Configuration** to open the Configuration View.
3. In the Configuration View, click **Backup Configuration Database**. You are prompted to supply a file name.
4. When prompted to provide a name, enter the name of the backup file on the hub Tivoli Enterprise Monitoring Server.

   The contents of the configuration database will be stored in the backup file. The format of the file name depends on the operating system on which the hub Tivoli Enterprise Monitoring Server runs:

   - If the hub Tivoli Enterprise Monitoring Server is running on a UNIX or Linux system, this name identifies a file in the `*install_dir*/tables/*TEMS_Name*` directory, where *install_dir* is the installation directory of IBM Tivoli Monitoring and *TEMS_Name* is the name of the hub Tivoli Enterprise Monitoring Server. If the file does not exist, it is created; if it does exist, its current contents are overwritten.

- If the hub Tivoli Enterprise Monitoring Server is running on a Windows system, this name identifies a file in the current Tivoli Enterprise Monitoring Server working directory (for example, `C:\IBM\ITM\CMS`). If the file does not exist, it is created; if it does exist, its current contents are overwritten.
- If the hub Tivoli Enterprise Monitoring Server is running on a z/OS system, this name references a predefined sequential data set. Do *not* enclose the name in quotation marks. The data set must be allocated manually. The following DCB information is required for this data set:

```
RECFM=FB,LRECL=440,BLKSIZE=<some multiple of 440>
```

5. Click **OK**.
6. Wait for the message that indicates that the configuration database was successfully backed up and click **OK**.

Related tasks:

"Restoring a product-provided internal configuration database" on page 225

"Restoring a DB2 UDB configuration database" on page 226

Restoring the configuration database

To restore the configuration database, you must have already created the backup file, as described in "Backing up the configuration database" on page 223.

The restoration process is performed at the hub Tivoli Enterprise Monitoring Server.

If you want to restore the contents of the configuration database from the backup file, use the restore utility that is appropriate for the type of configuration database that is used by your hub Tivoli Enterprise Monitoring Server.

Restore utility for product-provided internal configuration database

Depending on the operating system on which the hub Tivoli Enterprise Monitoring Server is running, use one of the following utilities to restore the product-provided internal configuration database:

- If the hub Tivoli Enterprise Monitoring Server is running on a UNIX or Linux system, use the kcfcrstr utility located in the current Tivoli Enterprise Monitoring Server working directory (the default is `/opt/IBM/ITM/`*`arch_code`*`/ms/bin/`, where *arch_code* is the architecture code of the operating system.

  See Appendix B, "Architecture codes," on page 261 for a list of architecture codes). See "Restoring a product-provided internal configuration database" on page 225 for information about how to use this utility to restore a product-provided internal configuration database.
- If the hub Tivoli Enterprise Monitoring Server is running on a Windows system, use the KCFCRSTR utility located in the current Tivoli Enterprise Monitoring Server working directory (the default is `C:\IBM\ITM\CMS`).

  See "Restoring a product-provided internal configuration database" on page 225 for information about how to use this utility to restore a product-provided internal configuration database.
- If the hub Tivoli Enterprise Monitoring Server is running on a z/OS system, use the KCFARSM utility. For sample JCL to run the KCFARSM utility, see the member named KCFRCDBJ that is located in the &RHILEV..TKANSAM library.

See "Restoring a product-provided internal configuration database" for information about how to use this utility to restore a product-provided internal configuration database.

Restore utility for DB2 UDB configuration database

Depending on the operating system on which the hub Tivoli Enterprise Monitoring Server is running, use one of the following utilities to restore the configuration database if it is a DB2 Universal Database™:

- If the hub Tivoli Enterprise Monitoring Server is running on a UNIX or Linux system, use the kcfcrst2 utility located in the current Tivoli Enterprise Monitoring Server working directory (the default is `/opt/IBM/ITM/`*arch_code*`/ms/bin/`, where *arch_code* is the architecture code of the operating system.)

  See Appendix B, "Architecture codes," on page 261 for a list of architecture codes.
- If the hub Tivoli Enterprise Monitoring Server is running on a Windows system, use the KCFCRST2 utility located in the current Tivoli Enterprise Monitoring Server working directory (the default is `C:\IBM\ITM\CMS`).
- If the hub Tivoli Enterprise Monitoring Server is running on a z/OS system, use the KCFCRST2 utility. For sample JCL to run the KCFCRST2 utility, see the sample member named KCFRSDB2 that is located in the &RHILEV..TKANSAM library.

Restoring a product-provided internal configuration database

To restore the product-provided internal configuration database from a backup file that you previously created, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Stop the hub Tivoli Enterprise Monitoring Server if it is running.
2. If the hub Tivoli Enterprise Monitoring Server is running on a Windows, Linux or UNIX system, do the following steps:
   a. Go to the directory where the restore utility is located. If the hub Tivoli Enterprise Monitoring Server is running on a UNIX or Linux system, by default the kcfcrstr utility is located in the `/opt/IBM/ITM/`*arch_code*`/ms/bin` directory, where *arch_code* is the architecture code of the operating system. See Appendix B, "Architecture codes," on page 261 for a list of architecture codes. If the hub Tivoli Enterprise Monitoring Server is running on a Windows system, by default the KCFCRSTR utility is located in the `C:\IBM\ITM\CMS` directory.
   b. Run the following command:

      ```
      kcfcrstr -i input_file -o database_name
      ```

      where
      - *input_file* is the full path of the configuration database backup file.
      - *database_name* is the full path of the configuration database file.

      For example, run the following command on UNIX or Linux systems:

      ```
      kcfcrstr -i /opt/IBM/ITM/tables/tems1/RKCFbackup.txt
         -o /opt/IBM/ITM/tables/tems1/RKCFAPLD
      ```

      Tip: At the command prompt, you can enter `kcfcrstr` with no operands to display usage information for this utility.

3. If the hub Tivoli Enterprise Monitoring Server is running on a z/OS system, see the member named KCFRCDBJ that is located in the &RHILEV..TKANSAM library, modify the sample JCL found in this member to suit your environment, then submit it to run the KCFARSM utility.

Tips:

- Make sure that the hub Tivoli Enterprise Monitoring Server stops completely before restoring the database.
- Copy the original backup file to a safe location in case the restoration process fails. If the restoration process ends unexpectedly, you should use the copy in the safe location to perform the process again.
- Add the following line to the configuration file of the hub Tivoli Enterprise Monitoring Server to enable the caching mechanism of the operating system, which improves the performance at the cost of some reliability:

  ```
  KGLCB_FSYNC_ENABLED='0'
  ```

  The KGLCB_FSYNC_ENABLED variable is introduced in IBM Tivoli Monitoring 6.2 for the Tivoli Enterprise Monitoring Server on UNIX and Linux systems. This variable can be used to specify whether the fsync() system call should be issued after writes to the file system. This configuration variable can be set in the standard configuration file for the monitoring server. For maximum reliability, the default value is 1, which means fsync() is called.

The current contents of the configuration database are completely replaced by the contents of the backup file.

Related tasks:

"Backing up the configuration database" on page 223

"Changing the configuration database type from DB2 UDB to the internal type" on page 228

Restoring a DB2 UDB configuration database

If the hub Tivoli Enterprise Monitoring Server is running on a UNIX or Linux system, you must have permission to use the configuration database. If you need to stop then restart the Tivoli Enterprise Monitoring Server on a UNIX or Linux system, you must have appropriate permissions to work with the configuration database. The Tivoli Enterprise Monitoring Server stops if the user starting the Tivoli Enterprise Monitoring Server does not have permissions to the configuration database KCFT schema and the KCFT.KCFATTRIBUTES, and KCFT.KCFOBJECT tables. A restored database has to be granted permissions for users or groups. The DB2 GRANT commands must be used to give users permission to work with the database. For a user named `usr2`, these commands are as follows:

```
GRANT CREATEIN, ALTERIN ON SCHEMA KCFT TO USER usr2
GRANT ALL ON KCFT.KCFATTRIBUTES TO USER usr2
GRANT ALL ON KCFT.KCFOBJECT TO USER usr2
```

These DB2 GRANT commands are different from the commands that are used to install and set up the DB2 UDB configuration database on UNIX or Linux systems.

To restore the DB2 UDB type of configuration database from a backup file that you previously created, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Stop the hub Tivoli Enterprise Monitoring Server if it is running.
2. Set up your environment for issuing DB2 commands. See DB2 documentation for information about how to set up your environment for issuing DB2 commands.
3. If the hub Tivoli Enterprise Monitoring Server is running on a UNIX or Linux system, go to the current Tivoli Enterprise Monitoring Server working directory and run the following command:

   ```
   kcfcrst2 -i input_file -d database_name -u userid -p password
   ```

   where:

   - *input_file* is the full name and path of the configuration database backup file.
   - *database_name* is the name of the DB2 configuration database into which the data in the file specified by the *input_file* value is to be restored.
   - *userid* is the user ID that was used to start the Tivoli Enterprise Monitoring Server. It must have write access to the DB2 database.
   - *password* is the password of the user ID that is used to administer DB2.

   Tip: At the command line, you can enter `kcfcrst2` with no operands to display usage information for this utility.
4. If the Tivoli Enterprise Monitoring Server is running on a Windows system, issue the following command at a command prompt when you are in the current Tivoli Enterprise Monitoring Server working directory (for example, `C:\IBM\ITM\CMS`):

   ```
   kcfcrst2 -i input_file -d database_name -u userid -p password
   ```

   where:

   - *input_file* is the full name and path of the configuration database backup file.
   - *database_name* is the name of the DB2 configuration database into which the data in the file specified by the *input_file* value is to be restored.
   - *userid* is the user ID that was used to start the Tivoli Enterprise Monitoring Server. It must have write access to the DB2 database.
   - *password* is the password that is used to administer DB2.

   Tip: At the command prompt, you can enter `KCFCRST2` with no operands to display usage information for this utility.

   For example, if your configuration database backup file is named `C:\IBM\ITM\CMS\RKCFbackup`, your DB2 configuration database is named rkcfaplt, your user ID is db2admin, and your password is db2, issue the following command.

   ```
   kcfcrst2 -i c:\IBM\ITM\CMS\RKCFbackup -d rkcfaplt -u db2admin -p db2
   ```
5. If the Tivoli Enterprise Monitoring Server is running on a z/OS system, see the sample member named KCFRSDB2 that is located in the *&RHILEV*..TKANSAM library, modify the sample JCL found in this member to suit your environment, then submit it to run the KCFCRST2 utility.

Related tasks:

"Backing up the configuration database" on page 223

"Changing the configuration database type from Internal type to DB2 UDB type" on page 228

Changing the type of configuration database

You can use the configuration database backup file that is generated by the backup process to change from one supported type of configuration database to another. The product-provided internal type and the DB2 Universal Database (UDB) type are supported.

Changing the configuration database type from DB2 UDB to the internal type

To change the configuration database type from the DB2 UDB type to the product-provided internal type, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Back up your existing configuration database, as described in "Backing up the configuration database" on page 223.
2. Stop the hub Tivoli Enterprise Monitoring Server if it is running.
3. Use one of the following methods to reconfigure your hub monitoring server to use the internal type of configuration database:
   - If the hub monitoring server is running on a UNIX or Linux system, run the configuration process that was used to define WebSphere MQ Configuration agent to the hub monitoring server (see information about setting up the configuration database in *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide* for details). In the Tivoli Enterprise Monitoring Server configuration window, you specify the type of database that you want to use. Specify **Internal**.
   - If the hub monitoring server is running on a Windows system, open a command prompt in the current monitoring server working directory (for example, `C:\IBM\ITM\CMS`) and run the `KCFDataSource.exe` program. A window with a Database Type option opens. In the Database Type area of the window, select **Internal** and click **OK**. The registry entries are adjusted so that the product-provided Internal type of configuration database is used.

     Tip: At the command prompt, you can enter `KCFDataSource /?` to display usage information for this utility.
   - If the hub monitoring server is running on a z/OS system, use the PARMGEN parameter, **`KMC_CFG_DATABASE_TYPE`**, to choose the type of configuration database (See *IBM Tivoli OMEGAMON XE for Messaging for z/OS: Planning and Configuration Guide*).
4. Restore the contents of the configuration database from the backup file into the new configuration database. Follow the instructions in "Restoring a product-provided internal configuration database" on page 225.
5. Start the hub Tivoli Enterprise Monitoring Server.

Related tasks:

"Restoring a product-provided internal configuration database" on page 225

Changing the configuration database type from Internal type to DB2 UDB type

To change the configuration database type from the product-provided Internal type to the DB2 UDB type, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Back up your existing configuration database, as described in "Backing up the configuration database" on page 223.
2. Stop the hub Tivoli Enterprise Monitoring Server if it is running.
3. Set up DB2 UDB for use as the configuration database as described in the following documents:
   - *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide*
   - *IBM Tivoli OMEGAMON XE for Messaging for z/OS: Planning and Configuration Guide*
4. Use one of the following methods to reconfigure your hub Tivoli Enterprise Monitoring Server so that the DB2 UDB type of configuration database is used.
   - If the hub monitoring server is running on a UNIX or Linux system, run the configuration process that was used to define WebSphere MQ Configuration agent to the hub monitoring server (see the information about configuring database setup in *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide* for details). In the Tivoli Enterprise Monitoring Server configuration window, the database section contains database choices. Specify DB2 and enter the DB2 home directory and the DB2 instance name.
   - If the hub monitoring server is running on a Windows system, open a command prompt in the current Tivoli Enterprise Monitoring Server working directory (for example, `C:\IBM\ITM\CMS`) and run the `KCFDataSource.exe` program. A window that has a Database Type option opens. In the Database Type area of the window, select the option that contains the words **DB2 UDB**, complete the required DB2 information and click **OK**. The registry entries are adjusted so that the DB2 UDB type of configuration database is used.

     Tip: At the command prompt, you can enter `KCFDataSource /?` to display usage information for this utility.
   - If the hub monitoring server is running on a z/OS system, use the PARMGEN parameter, **`KMC_CFG_DATABASE_TYPE`**, to choose the type of configuration database.
5. Restore the contents of the configuration database from the backup file into the new configuration database. Follow the instructions in "Restoring a DB2 UDB configuration database" on page 226.
6. Start the hub Tivoli Enterprise Monitoring Server.

Related tasks:

"Restoring a DB2 UDB configuration database" on page 226

Chapter 12. Creating multiple instances of the WebSphere MQ Configuration agent

If the queue managers that you want to configure are running in a Microsoft Cluster Services (MSCS) or High Availability Cluster Multi Processing (HACMP™) cluster environment, you might need to create a secondary agent instance.

By default a single WebSphere MQ Configuration agent instance is created during installation, which is called the primary WebSphere MQ Configuration agent. Under normal circumstances, you can use the primary agent to perform all your configuration tasks. However, if the queue managers that you want to configure are running in a Microsoft Cluster Services (MSCS) or High Availability Cluster Multi Processing (HACMP) cluster environment, you might need to create a secondary agent instance.

Creating an instance of the WebSphere MQ Configuration agent on a Windows system

Do the following steps to create a secondary instance of WebSphere MQ Configuration agent on a Windows system:

1. Select **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services** to open the Manage Tivoli Enterprise Monitoring Services window.
2. From the Manage Tivoli Enterprise Monitoring Services window, right-click **WebSphere MQ Configuration Agent** and select **Create Instance**.
3. Enter a name for the instance when prompted and click **OK**. The new agent instance is created and listed in the Manage Tivoli Enterprise Monitoring Services window.
4. Right-click the newly created agent instance in the Manage Tivoli Enterprise Monitoring Services window and select **Configure Using Defaults**.
5. A message is displayed asking if you want to update the configuration file of the agent instance prior to configuration of WebSphere MQ Configuration agent. Click **Yes**.
6. A message is displayed stating that configuration will wait for you to close the Notepad edit session before continuing. Click **OK**.
7. Set the **KMC_CLUSTERNAME** and **KMC_QUEUEMGRS** parameters. **KMC_CLUSTERNAME** is the host name of the cluster node on which the agent runs. **KMC_QUEUEMGRS** is the name of one or more queue managers on the cluster node that you want the agent instance to configure. Separate different queue manager names with a comma (,).
8. A message is displayed stating that the configuration file edit session is complete. Click **Yes** to configure the agent.

Creating an instance of the WebSphere MQ Configuration agent on a UNIX or Linux system

Do the following steps to create an instance of the WebSphere MQ Configuration agent on UNIX and Linux systems:

1. Log on to the UNIX or Linux system as root.

2. Navigate to the *install_dir*/bin directory, where *install_dir* is the IBM Tivoli Monitoring installation directory.
3. Run the following command to create a secondary instance of the WebSphere MQ Configuration agent:

   ```
   ./itmcmd agent -o instance_name start mc
   ```

   where *instance_name* is the name of the new agent instance.
4. Go to the *install_dir*/config directory, where *install_dir* is the IBM Tivoli Monitoring installation directory.
5. Open the configuration file of the newly created agent instance in a text editor. The file name is in the following format:

   ```
   hostname_mc_instance_name.cfg
   ```

   where *hostname* is the host name of the Linux or UNIX system and *instance_name* is the name of the new agent instance.
6. Set the **KMC_CLUSTERNAME** and **KMC_QUEUEMGRS** parameters and close Notepad. **KMC_CLUSTERNAME** is the host name of the cluster node on which the agent runs. **KMC_QUEUEMGRS** is the name of one or more queue managers on the cluster node that you want the agent instance to configure. Separate different queue manager names with a comma (,).
7. Edit any other parameters as necessary then save and close the file.

Chapter 13. Configuring WebSphere MQ Configuration agent to work in a cluster environment on Windows systems

You can configure WebSphere MQ Configuration agent to run in a cluster environment on Windows systems.

MSCS clusters are different from WebSphere MQ clusters, as follows:

WebSphere MQ clusters
WebSphere MQ clusters are groups of two or more queue managers running on one or more computers, providing automatic interconnection, and allowing queues to be shared for load balancing and redundancy.

MSCS clusters
Microsoft Cluster Server (MSCS) clusters are groups of two or more computers, connected together and configured so that, if one fails, MSCS performs a failover, transferring the state data of applications from the failing computer to another computer in the cluster and re-initiating their operations there.

You can use MSCS to connect servers into a cluster, giving higher availability of data and applications, and making it easier to manage the system. MSCS can automatically detect and recover from server or application failures.

Every computer that is configured by WebSphere MQ Configuration agent has an instance of the WebSphere MQ Configuration agent installed. If monitored resources are running in a cluster environment, you must configure the WebSphere MQ Configuration agent to run in the cluster environment. The WebSphere MQ Configuration agent supports both active/active and active/passive clustering. For configuration instructions, see "Configuring the WebSphere MQ Configuration agent."

The configuration database runs on the same system as the Tivoli Enterprise Monitoring Server, either using the internal database or a DB2 database. If you want to configure the configuration database to run in a cluster environment, you must also configure the monitoring server to run in that environment. The monitoring server and the configuration database support active/passive clustering only. For configuration instructions, see "Configuring the configuration database to work in an active/passive cluster environment" on page 241.

Configuring the WebSphere MQ Configuration agent

The WebSphere MQ Configuration agent supports both active/active and active/passive clustering. If you are configuring the agent in an active/active cluster environment, see "Configuring the WebSphere MQ Configuration agent in an active/active cluster environment" on page 234 for instructions. If you are configuring the agent in an active/passive cluster environment, see "Configuring the WebSphere MQ Configuration agent in an active/passive cluster environment" on page 238 for instructions.

Configuring the WebSphere MQ Configuration agent in an active/active cluster environment

Before you begin configuring the WebSphere MQ Configuration agent to run in a cluster environment, ensure that the two systems that host the WebSphere MQ Configuration agent are correctly configured. Ensure that both systems fulfill the following requirements:

- Microsoft Windows 2003 Server is installed. This includes Microsoft Cluster Server (MSCS), which is used to manage your cluster environment.
- You have configured both systems as cluster nodes using MSCS.
- The IBM Tivoli Monitoring framework is installed. This must be installed separately on both cluster nodes. For instructions for installing IBM Tivoli Monitoring in a cluster environment, see your IBM Tivoli Monitoring documentation.
- The WebSphere MQ Configuration agent is installed. This must be installed on both cluster nodes. See *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide* for installation instructions.

You must also have two separate logical drives that can be shared between the two cluster nodes that are available for storing log and historical data collected from the agents. These drives are drives R and S in the following procedure.

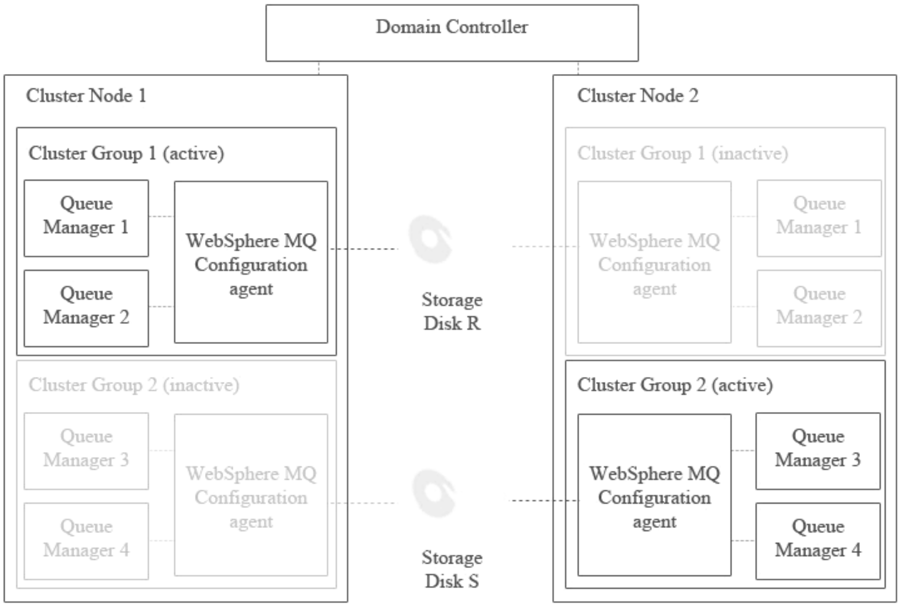


Figure 60. An example active/active cluster environment architecture with one cluster group active on each cluster node

An example of an active/active cluster environment is displayed in Figure 60. The environment consists of two cluster nodes on separate physical systems. Each cluster node hosts two cluster groups. The cluster groups that are hosted by each system are the same, so there are two identical copies of cluster group 1 and two identical copies of cluster group 2. Each cluster group contains a number of WebSphere MQ queue managers (two in Figure 60, but there is no limit to the number of queue managers that can be included in a cluster group) and a single instance of the WebSphere MQ Configuration agent to configure the queue managers.

Only one copy of each cluster group can be active simultaneously. For example, if cluster group 1 is active on cluster node 1 (as in Figure 60 on page 234), the copy of cluster group 1 hosted by cluster node 2 is inactive. In most environments with two cluster nodes and two cluster groups where both cluster nodes are running correctly, one cluster group runs on each cluster node, balancing the load between the two systems. If one of the nodes fails, then the second cluster group on the node that is still active starts automatically to continue the work of the cluster group that was active on the node that failed.

Information shared between different copies of the same agent, such as error log information, is stored on a separate disk that can be accessed by all copies of the agent running on different cluster nodes. If the node that hosts the active agent fails and a copy of the agent on another node starts, shared information such as log files can still be read and written to the disk as if the same copy of the agent was still running. The agent is installed separately on each cluster node. Shared disks store only log files and historical information that must be accessed by different copies of the same agent. Data related to your WebSphere MQ environment is stored in the configuration database on the Tivoli Enterprise Monitoring Server.

To configure the WebSphere MQ Configuration agent to run in an active/active cluster environment, do the following procedure:

Tip: The following procedure assumes that you have two cluster groups, as this is the most common configuration. If you have more than two cluster groups, create additional instances of the WebSphere MQ Configuration agent to configure the queue managers in each additional cluster group.

1. Create new instances of the WebSphere MQ Configuration agent by doing the following steps on both cluster nodes:
   a. Open the Manage Tivoli Monitoring Services window.
   b. In the Manage Tivoli Monitoring Services window, right-click the WebSphere MQ Configuration agent and click **Create Instance**. A new instance of the WebSphere MQ Configuration agent to monitor the queue managers in cluster group 1 is created.
   c. When prompted, enter a name for the instance and click **OK**. Assume that you entered the name kmc1.
   d. Edit the configuration file of the kmc1 agent as follows:

      ```
      KMC_CLUSTERNAME=cluster1
      KMC_QUEUEMGRS=[QM1,QM2]
      ```

      Tip: Edit the `KMC_CLUSTERNAME` parameter to specify the name of the cluster, which will be displayed in the Configuration view and physical view. It should be identical for different instances that are in the same cluster in their configuration files. The `KMC_QUEUEMGRS` parameter should include the names of the queue managers that you want to configure and the names are separated by commas.
   e. Right-click the WebSphere MQ Configuration agent and click **Create Instance** again to create a second new instance of the WebSphere MQ Configuration agent to monitor the queue managers in cluster group 2.
   f. When prompted, enter a name for the instance and click **OK**. Assume that you entered the name kmc2.
   g. Edit the configuration file of the kmc2 agent as follows:

      ```
      KMC_CLUSTERNAME=cluster2
      KMC_QUEUEMGRS=[QM3,QM4]
      ```

h. Stop the primary WebSphere MQ Configuration agent instance.

   Important: Do not use the primary WebSphere MQ Configuration agent to configure queue managers in a cluster environment.

2. Set local variables by completing the following steps on each cluster node:

   a. Right-click the kmc1 agent and click **Advanced** > **Edit Variables**.

   b. In the Override Local Variable Settings window, add the variables shown in Table 16, which specify where data saved by the kmc1 agent is stored. The value of each variable is the location on drive R where you want the data to be stored. You must specify a different location for each variable.

Table 16. Overriding local variables

Variable	Details
CTIRA_LOG_PATH	The location where log data is stored.
CTIRA_HIST_DIR	The location where historical data is stored.
KMC_MQ_LOG_NAME	The WebSphere MQ Configuration agent audit log file. If this file does not exist, it is created automatically.

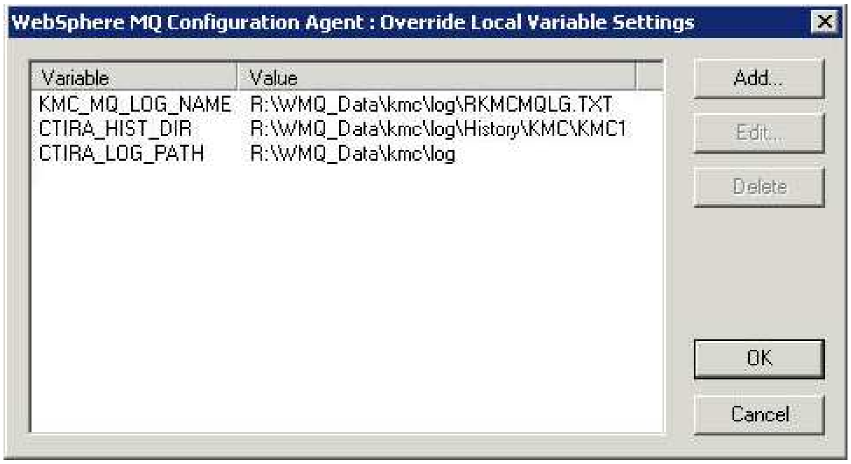
For example, you might set the variables as follows:

- CTIRA_LOG_PATH = R:\WMQ_Data\kmc\log
- CTIRA_HIST_DIR = R:\WMQ_Data\kmc\log\History\KMC\KMC1
- KMC_MQ_LOG_NAME = R:\WMQ_Data\kmc\log\RKMCMQLG.TXT

This is illustrated in Figure 61.

Remember:

- Variable paths cannot contain spaces. For example, CTIRA_LOG_PATH = R:\Websphere MQ\kmc\log is not valid.
- Each agent must have its own logical drive on which to store data. More than one agent cannot share a single drive.



WebSphere MQ Configuration Agent : Override Local Variable Settings
Add...
Edit...
Delete
OK
Cancel

Variable	Value
KMC_MQ_LOG_NAME	R:\WMQ_Data\kmc\log\RKMCMQLG.TXT
CTIRA_HIST_DIR	R:\WMQ_Data\kmc\log\History\KMC\KMC1
CTIRA_LOG_PATH	R:\WMQ_Data\kmc\log

Figure 61. Setting local variables

   c. Click **OK** to close the window.

   d. Right-click the kmc2 agent and click **Advanced** > **Edit Variables**.

e. In the Override Local Variable Settings window, add the same variables as specified in step 2b on page 236 to specify the location on drive S where you want data saved by the kmc2 agent to be stored.

   For example, you might set the variables as follows:

   - CTIRA_LOG_PATH = S:\WMQ_Data\kmc\log
   - CTIRA_HIST_DIR = S:\WMQ_Data\kmc\log\History\KMC\KMC2
   - KMC_MQ_LOG_NAME=S:\WMQ_Data\kmc\log\RKMCMQLG.TXT

f. Click **OK** to close the window.

g. Reconfigure the kmc1 and kmc2 agents. The new configuration settings now takes effect.

h. Change the start mode of the kmc1 and kmc2 agents to manual startup.

3. If you want a trace log to be written by the agents, do the following steps on both cluster nodes:

   a. Open the Manage Tivoli Monitoring Services window.

   b. Right-click the WebSphere MQ Configuration agent and click **Advanced** > **Edit Trace Parms**. The Trace Parameters window is displayed.

   c. Select `ERROR (UNIT:KMC0 INPUT OUTPUT STATE)` in the **Enter RAS1 Filters** field.

   d. Select the level of data that you want to be included in the trace log in the **KDC_DEBUG Setting** field.

   e. Click **OK** to close the window.

   f. Navigate to the *itm_home*\tmaitm6\ directory, where *itm_home* is your IBM Tivoli Monitoring installation directory.

   g. Do the following steps for each instance of the WebSphere MQ Configuration agent:

      1) Open the kmcenv_*instance* file in a standard text editor, where *instance* is the name of the WebSphere MQ Configuration agent instance.

         For example, if your agent is called kmc1, you open the `kmcenv_kmc1` file.

      2) Locate the following line. If it does not exist, add it to the end of the file.

         ```
         KBB_RAS1_LOG=C:\IBM\ITM\logs\hostname_MC_$(sysutcstart)-.log
         INVENTORY=C:\IBM\ITM\logs\hostname_MC.inv
         MAXFILES=32 LIMIT=5 COUNT=5 PRESERVE=1
         ```

         Where *hostname* is the name of the system that hosts the cluster node in which the agent instance runs.

      3) Change `C:\IBM\ITM\logs` to *X*`:\WMQ_Data\kmc\log`, where *X* is the letter that is assigned to the drive where log data from this agent is stored.

         When configuring WebSphere MQ Configuration agent instance kmc1, *X* is R, and when configuring agent instance kmc2, *X* is S.

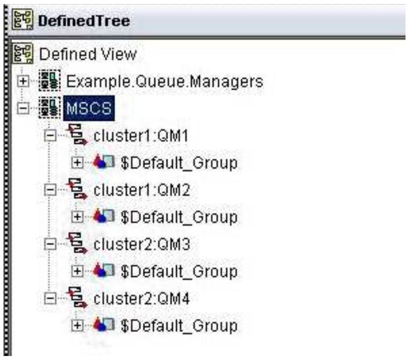
      4) Save and close the file.

4. Use Cluster Administrator (a part of MSCS) to add the kmc1 cluster resource to cluster group 1 and the kmc2 cluster resource to cluster group 2.

5. Use Cluster Administrator to set the group owner of cluster group 1 to cluster node 1 and the group owner of cluster group 2 to cluster node 2.

6. Use Cluster Administrator to start all queue managers and the WebSphere MQ Configuration agent in each cluster group. Your cluster environment is now configured. If you expand the WebSphere MQ Configuration agent in the navigation tree, your configuration should look similar to that shown in

Figure 62.



DefinedTree
Defined View
Example.Queue.Managers
MSCS
cluster1:QM1
$Default_Group
cluster1:QM2
$Default_Group
cluster2:QM3
$Default_Group
cluster2:QM4
$Default_Group

Figure 62. A correctly configured cluster environment

Related tasks:

"Creating an instance of the WebSphere MQ Configuration agent on a Windows system" on page 231

"Testing the configuration" on page 245

Configuring the WebSphere MQ Configuration agent in an active/passive cluster environment

Before you begin configuring the WebSphere MQ Configuration agent to run in an active/passive cluster environment, ensure that the two systems that host the WebSphere MQ Configuration agent are correctly configured. Ensure that both systems fulfill the following requirements:

- Microsoft Windows 2003 Server is installed. This includes Microsoft Cluster Server (MSCS), which is used to manage your cluster environment.
- You have configured both systems as cluster nodes using MSCS.
- The IBM Tivoli Monitoring framework is installed. This must be installed separately on both cluster nodes. For instructions for installing IBM Tivoli Monitoring in a cluster environment, see your IBM Tivoli Monitoring documentation.
- The WebSphere MQ Configuration agent is installed. This must be installed on both cluster nodes. For installation instructions, see *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide* .

You must also have a shared logical disk for storing log and historical data that is collected from the agents that can be shared between the two cluster nodes. This drive is drive R in the following procedure.

An example of an active/passive cluster environment is displayed in Figure 63 on page 239. The environment consists of two cluster nodes on separate physical systems. Both cluster nodes host a single cluster group. The cluster groups hosted by the two systems are identical. Each cluster group contains a number of WebSphere MQ queue managers (two in Figure 63 on page 239, but there is no limit to the number of queue managers that can be included in a cluster group) and a single instance of the WebSphere MQ Configuration agent to configure the queue managers.

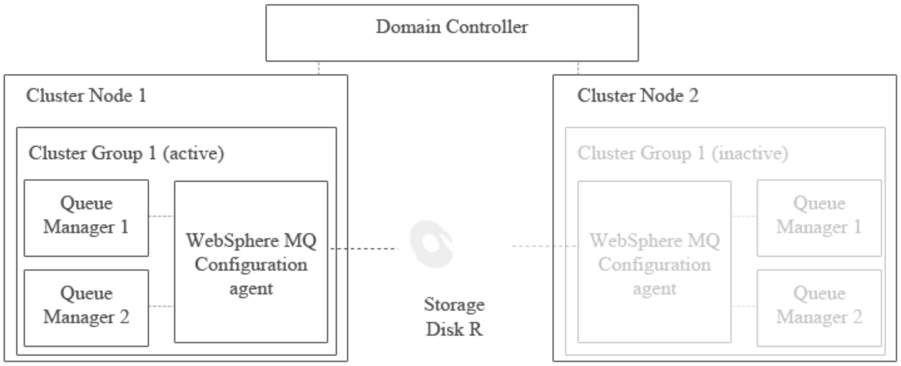


Figure 63. An example active/passive cluster environment architecture with one cluster group active.

Only one copy of the cluster group can be active simultaneously. For example, if cluster group 1 is active on cluster node 1 (as in Figure 63), the copy of cluster group 1 hosted by cluster node 2 is inactive. If the cluster node that hosts the active cluster group fails, the cluster group on the node that has not failed starts automatically to continue the work of the cluster group on the node that failed.

Information that is shared between different copies of the same agent, such as error log information, is stored on a separate disk that can be accessed by all copies of the agent running on different cluster nodes. If the node that hosts the active agent fails and a copy of the agent on another node starts, shared information such as log files can still be read and written to the disk as if the same copy of the agent was still running. The agent is installed separately on each cluster node. Shared disks store only log files and historical information that must be accessed by different copies of the same agent. Data related to your WebSphere MQ environment is stored in the configuration database on the Tivoli Enterprise Monitoring Server.

To configure the WebSphere MQ Configuration agent to run in an active/passive cluster environment, do the following steps:

Tip: The following procedure assumes that you have two cluster groups, as this is the most common configuration. If you have more than two cluster groups, create additional instances of the WebSphere MQ Configuration agent to configure the queue managers in each additional cluster group.

1. Create new instances of the WebSphere MQ Configuration agent by doing the following steps on both cluster nodes:
   a. Open the Manage Tivoli Monitoring Services window.
   b. In the Manage Tivoli Monitoring Services window, right-click the WebSphere MQ Configuration agent and click **Create Instance**. A new instance of the WebSphere MQ Configuration agent is created.
   c. When prompted, enter a name for the instance and click **OK**. Assume that you entered the name kmc1.
   d. Reconfigure the new instance of the WebSphere MQ Configuration agent.
   e. Stop the primary WebSphere MQ Configuration agent instance.

      Important: Do not use the primary WebSphere MQ Configuration agent to configure queue managers in a cluster environment.

2. Set local variables by completing the following steps on each cluster node:
   a. Right-click the kmc1 agent and click **Advanced** > **Edit Variables**.
   b. In the Override Local Variable Settings window, add the variables shown in Table 17, which specify where data saved by the kmc1 agent is stored. The value of each variable is the location on drive R where you want the data to be stored. You must specify a different location for each variable.

Table 17. Overriding local variables

Variable	Details
CTIRA_LOG_PATH	The location where log data is stored.
CTIRA_HIST_DIR	The location where historical data is stored.
KMC_MQ_LOG_NAME	The WebSphere MQ Configuration agent audit log file. If this file does not exist, it is created automatically.

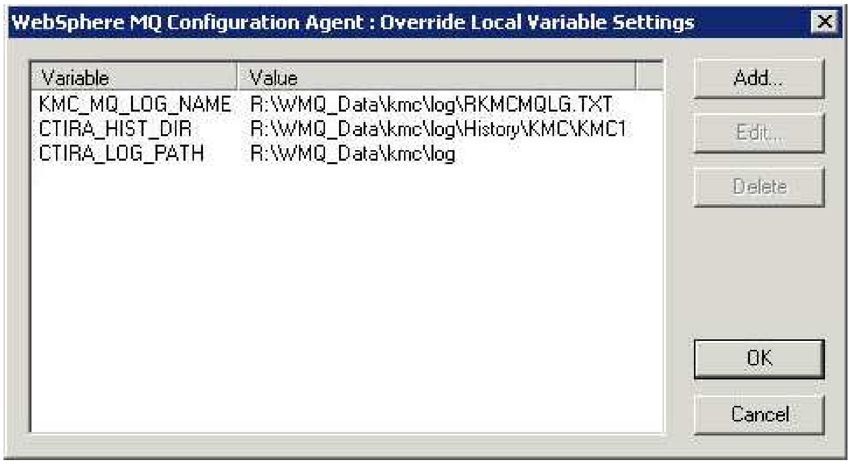
For example, you might set the variables as follows:

- CTIRA_LOG_PATH = R:\WMQ_Data\kmc\log
- CTIRA_HIST_DIR = R:\WMQ_Data\kmc\log\History\KMC\KMC1
- KMC_MQ_LOG_NAME=R:\WMQ_Data\kmc\log\RKMCMQLG.TXT

This is illustrated in Figure 64.

Remember:

- Variable paths cannot contain spaces. For example, CTIRA_LOG_PATH = R:\Websphere MQ\kmc\log is not valid.
- Each agent must have its own logical drive on which to store data. More than one agent cannot share a single drive.


WebSphere MQ Configuration Agent : Override Local Variable Settings

Variable	Value
KMC_MQ_LOG_NAME	R:\WMQ_Data\kmc\log\RKMCMQLG.TXT
CTIRA_HIST_DIR	R:\WMQ_Data\kmc\log\History\KMC\KMC1
CTIRA_LOG_PATH	R:\WMQ_Data\kmc\log

Figure 64. Setting local variables

   c. Click **OK** to close the window.
   d. Reconfigure the kmc1 agent. The new configuration settings now takes effect.
   e. Change the start mode of the kmc1 agent to manual startup.
3. If you want a trace log to be written by the agents, perform the following procedure on both cluster nodes:
   a. Open the Manage Tivoli Monitoring Services window.

b. Right-click the WebSphere MQ Configuration agent and click **Advanced** > **Edit Trace Parms**. The Trace Parameters window is displayed.

c. Select `ERROR (UNIT:KMC0 INPUT OUTPUT STATE)` in the **Enter RAS1 Filters** field.

d. Select the level of data that you want to be included in the trace log in the **KDC_DEBUG Setting** field.

e. Click **OK** to close the window.

f. Navigate to the *itm_home*\tmaitm6\ directory, where *itm_home* is your IBM Tivoli Monitoring installation directory.

g. Open the KMCENV_*instance* file in a standard text editor, where *instance* is the name of the WebSphere MQ Configuration agent instance. For example, if your agent is called kmc1, you open the KMCENV_kmc1 file.

h. Locate the following line (If it does not exist, add it to the end of the file):

```
KBB_RAS1_LOG=C:\IBM\ITM\logs\hostname_MC_$(sysutcstart)-.log
INVENTORY=C:\IBM\ITM\logs\hostname_MC.inv
MAXFILES=32 LIMIT=5 COUNT=5 PRESERVE=1
```

Where *hostname* is the name of the system that hosts the cluster node in which the agent instance runs.

i. Change C:\IBM\ITM\logs to *X*:\WMQ_Data\kmc\log, where *X* is the letter that is assigned to the drive where log data from this agent is stored. So, when configuring WebSphere MQ Configuration agent instance kmc1, *X* is R.

j. Save and close the file.

4. Use Cluster Administrator (a part of MSCS) to add the kmc1 cluster resource to cluster group 1.
5. Use Cluster Administrator to set the group owner of cluster group 1 to cluster node 1.
6. Use Cluster Administrator to start all queue managers and the WebSphere MQ Configuration agent in each cluster group.

Related tasks:

"Creating an instance of the WebSphere MQ Configuration agent on a UNIX or Linux system" on page 231

"Testing the configuration" on page 245

"Configuring the configuration database to work in an active/passive cluster environment"

Configuring the configuration database to work in an active/passive cluster environment

Because the WebSphere MQ configuration database and associated application support files are stored at the Tivoli Enterprise Monitoring Server, configuring them to run in a cluster environment requires configuring the monitoring server to run in a cluster environment. The information in this section provides instructions for configuring both the Tivoli Enterprise Monitoring Server and the WebSphere MQ configuration database to run in an active/passive cluster environment. The monitoring server and the configuration database do not support active/active clustering.

Before you begin configuring theTivoli Enterprise Monitoring Server, ensure that you have the following resources available:

- You have two systems to use as cluster nodes, with Microsoft Windows 2003 Server installed. Microsoft Windows 2003 Server includes Microsoft Cluster

Server (MSCS), which is used to manage your cluster environment. Refer to these systems as cluster node 1 and cluster node 2.
- You have configured both systems as cluster nodes using MSCS.
- The IBM Tivoli Monitoring framework and Tivoli Enterprise Monitoring Server are installed. For instructions about installing IBM Tivoli Monitoring in a cluster environment, see your IBM Tivoli Monitoring documentation.
- A shared disk is accessible by both cluster nodes. Refer to this disk as shared disk S.
- A cluster group containing disk S has been created on both cluster nodes.

An example showing the Tivoli Enterprise Monitoring Server with WebSphere MQ Configuration agent and the configuration database installed running in a cluster environment is shown in Figure 65. The diagram represents a system that uses the internal database as the WebSphere MQ configuration database, if a DB2 database is used instead, the database exists outside of the monitoring server.

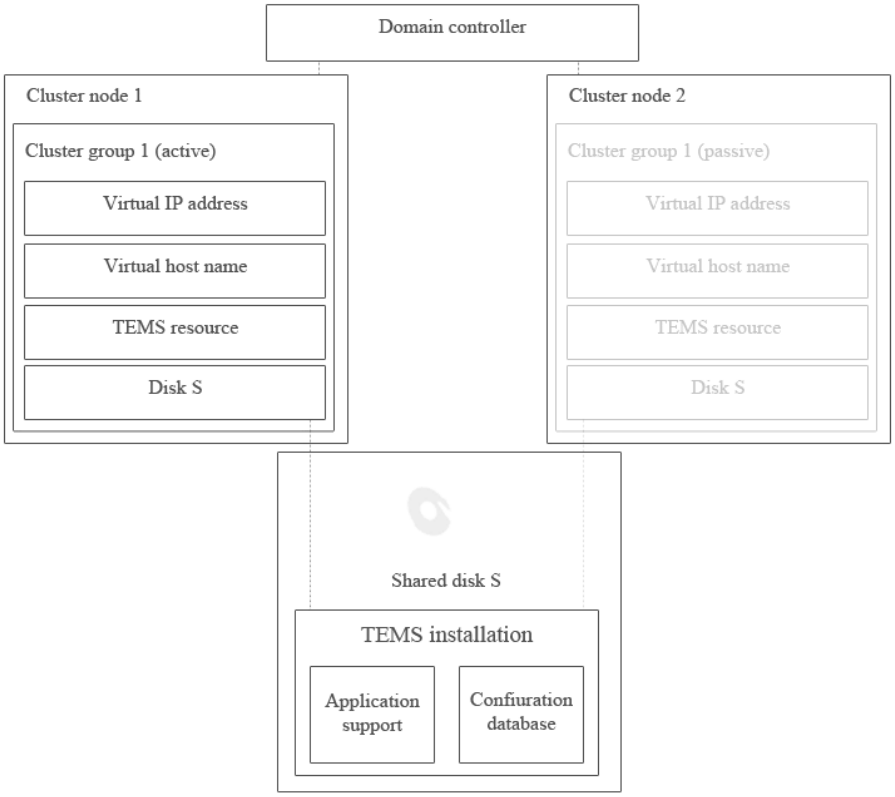


Figure 65. An example active/passive cluster environment architecture with one cluster group active on each cluster node

In Figure 65, the Tivoli Enterprise Monitoring Server is not installed on the cluster nodes. Instead, it is installed on a shared disk that can be accessed by a generic service that represents the monitoring server in the cluster groups and has access to shared disk S. This generic service and the shared disk S exist on both cluster nodes. Each cluster group also contains virtual IP address and host name resources that are used by agents to connect to the monitoring server. Because the virtual IP address and host names are identical on both cluster nodes, agents can connect to the monitoring server regardless of which physical cluster node it is running on.

Important: Because only one monitoring server installation is used in this configuration, a separate backup system, such as RAID, should be used to ensure the availability of the data that is stored on shared disk S.

Related tasks:

"Configuring the WebSphere MQ Configuration agent in an active/passive cluster environment" on page 238

Configuring cluster node 1

Do the following procedure to configure cluster node 1:

1. Start the Cluster Administrator and connect to the cluster.
2. Create a virtual IP address for the Tivoli Enterprise Monitoring Server, which is shared between both cluster nodes:
   a. Right-click the name of the cluster group and click **New** > **Resource**.
   b. Select IP Address in the **Resource type** field and enter IP in the **Name** field.
3. Create a virtual network name for the monitoring server, which is shared between both cluster nodes:
   a. Right-click the name of the cluster group and click **New** > **Resource**.
   b. Select Network Name in the **Resource type** field and enter a virtual host name that is used by agents for connecting to the Tivoli Enterprise Monitoring Server in the **Name** field.
4. From cluster node 1, install monitoring server on shared disk S.

   Important: During installation, any IBM Tivoli Monitoring components that are already installed on cluster node 1 are removed.

   a. Copy the installation files from the installation media on cluster node 1 to shared disk S. Do not install the monitoring server directly from the installation media on cluster node 1 because this might cause problems in the event of a network failure during the installation process.
   b. Run the `setup.exe` file to start the installation process.
   c. When prompted to install the IBM GSkit and IBM Java Runtime Environment, install them on shared disk S.
   d. When prompted to specify the directory in which to install IBM Tivoli Monitoring, specify a directory on shared disk S. For example, `S:\IBM\ITM`.
   e. When prompted to enter a name for the Tivoli Enterprise Monitoring Server, enter an appropriate name, but do not use the name of a cluster node. Using the name of a cluster node is confusing because the monitoring server runs on both cluster nodes.
   f. When prompted to enter the host name of the system on which the monitoring server runs, enter the name that is specified in step 3b.

   For more detailed information about installing the Tivoli Enterprise Monitoring Server, see your IBM Tivoli Monitoring documentation.
5. Install application support for the WebSphere MQ Configuration agent and any other agents that you want to use.

   Requirement: If you want to use a DB2 database instead of the internal database as the WebSphere MQ Configuration Database, you must install it in your cluster environment. For installation instructions, see your DB2 documentation. The DB2 instance should be added to the same cluster group as the monitoring server.

6. Configure the monitoring server to start manually. This is necessary because starting and stopping the monitoring server is handled by the cluster, not IBM Tivoli Monitoring. Do the following procedure:
   a. Open the Manage Tivoli Enterprise Monitoring Services window.
   b. Right-click the Tivoli Enterprise Monitoring Server and click **Change Startup** from the menu.
   c. Select `Manual` in **Startup Type** and click **OK**.
7. Set the network interface that is used by the monitoring server:
   a. Shut down cluster node 2.
   b. In Manage Tivoli Enterprise Monitoring Services window, right-click the Tivoli Enterprise Monitoring Server and click **Advanced** > **Set Network Interface**.
   c. Enter the host name that is specified in step 3b as the **Network Interface** name.
   d. Recycle the Tivoli Enterprise Monitoring Server.
8. Start cluster node 2.
9. Create the monitoring server resource in the cluster group:
   a. Open the Cluster Administrator.
   b. Right-click the cluster group and click **New** > **Resource**.
   c. Select `Generic Service` in the **Resource type** field, enter a name for the monitoring server resource in the **Name** field and click **Next**.
   d. Add both cluster node 1 and cluster node 2 to the list of possible owners and click **Next**.
   e. In **Services Properties** add the following variables:

```
HKEY_LOCAL_two-system cluster\SOFTWARE\Candle
HKEY_LOCAL_two-system cluster\SOFTWARE\IBM
HKEY_LOCAL_two-system cluster\SYSTEM\CurrentControlSet\Services\TEMS1
HKEY_LOCAL_two-system cluster\SYSTEM\CurrentControlSet\Control
   \Session Manager\Environment
```

   f. Click **OK** to finish configuring the resource.

Related tasks:

"Configuring cluster node 2"

Configuring cluster node 2

To configure cluster node 2, do the following steps:

1. Do the following steps on cluster node 1:
   a. Open the Cluster Administrator.
   b. Right-click the Tivoli Enterprise Monitoring Server resource group, and click **Move Group**.

   The operation fails and the cluster group remains on cluster node 1. However, this copies the required registry entries to cluster node 2.
2. Restart cluster node 2.
3. Do the following steps on cluster node 1:
   a. Open the Cluster Administrator.
   b. Right-click the Tivoli Enterprise Monitoring Server resource group, and click **Move Group**.

   This time the operation completes successfully and the cluster group is moved to cluster node 2.

4. To make the monitoring server displayed in the Manage Tivoli Enterprise Monitoring Services window when it is running on cluster node 2, run the following command on cluster node 2:

   ```
   S:\ITM_install\InstallITM\kinconfig.exe
   ```

   Where *ITM_install* is the directory on drive S in which IBM Tivoli Monitoring is installed.

Related tasks:

"Configuring cluster node 1" on page 243

Testing the configuration

To test your configuration to ensure that it is working correctly, do the following procedure. If you get any errors, check that you completed all configuration steps correctly to determine the cause of the problem.

1. Install the WebSphere MQ Configuration agent and configure it to connect to the Tivoli Enterprise Monitoring Server.
2. Log on to Tivoli Enterprise Portal, select the Configuration View and enter update mode.
3. Perform a discovery operation to discover the resources that can be configured using the WebSphere MQ Configuration agent.
4. Use the Cluster Administrator to perform a failover operation, moving the monitoring server to the other cluster node.
5. Do the following tests, and check that the result is as expected to ensure that WebSphere MQ Configuration agent work correctly:
   - Check whether resource attributes in settings lists are displayed correctly.
   - Discover a previously undiscovered resource.
   - Create a new resource in the defined view and deploy it to your environment by right-clicking it and then clicking **Update** > **Actual from defined**.
   - Validate a resource that is in the defined view.

Chapter 14. Configuring WebSphere MQ Configuration agent to work in a cluster environment on AIX systems

If you want the WebSphere MQ Configuration agent to work in a cluster environment on AIX systems using high-availability cluster multiprocessing (HACMP), you must follow the instructions in this section to configure it. The WebSphere MQ Configuration agent supports both active/active and active/passive clustering. For information about how to configure hardware such as redundant power supplies, redundant disk controllers, disk mirroring or multiple network or adapter configurations, see your HACMP documentation. For information about configuring WebSphere MQ and IBM Tivoli Monitoring to run in a cluster environment, see the documentation of each product.

Configuring the WebSphere MQ Configuration agent in an active/active clustering

Before you begin configuring the WebSphere MQ Configuration agent to run in an HACMP active/active cluster environment, ensure that the two systems that form the cluster nodes in the environment are correctly configured. Both systems must meet the following requirements:

- HACMP is installed and your HACMP cluster environment is correctly configured.
- Both cluster nodes have access to a shared disk, on which information that is shared between copies of the WebSphere MQ Configuration agent that are running on different cluster nodes is stored.
- WebSphere MQ is installed and configured to run in an HACMP cluster environment. See your WebSphere MQ documentation for information about how to install WebSphere MQ in a cluster environment.
- The queue managers that you want to configure have been created on both cluster nodes within the HACMP cluster environment. Ensure that failover occurs correctly. See your WebSphere MQ documentation for more information.

An example of an active/active cluster environment is displayed in Figure 66 on page 248. The environment consists of two cluster nodes that are running on separate physical systems. Each cluster node hosts two cluster groups. The cluster groups that are hosted by each system are the same. Between them there are two identical copies of cluster group 1 and two identical copies of cluster group 2. Each cluster group contains one or more WebSphere MQ queue managers and an instance of the WebSphere MQ Configuration agent to monitor each queue manager.

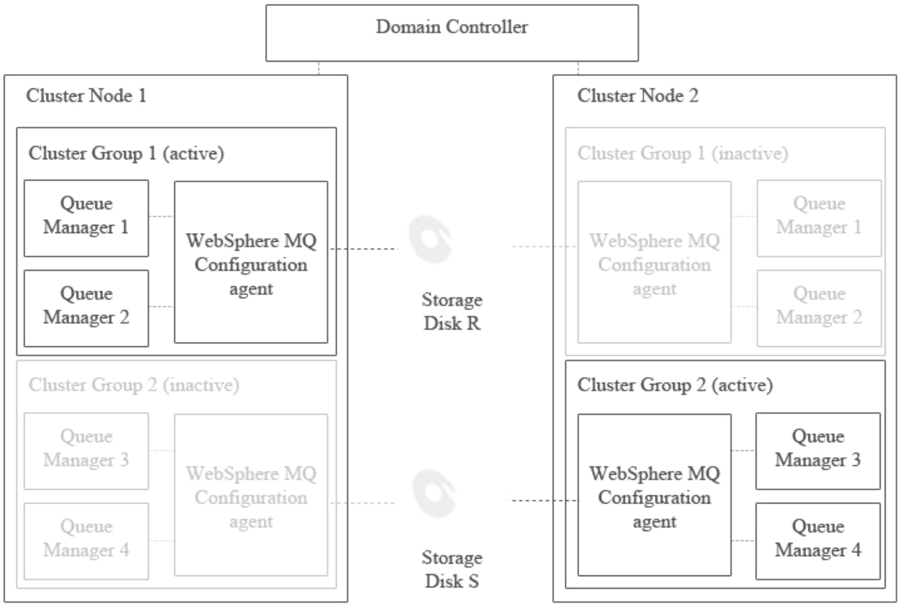


Figure 66. An example of active-active cluster environment architecture

Only one copy of each cluster group can be active simultaneously. For example, if cluster group 1 is active on cluster node 1 (as in Figure 66), the copy of cluster group 1 that is hosted by cluster node 2 is inactive. In most environments with two cluster nodes and two cluster groups where both cluster nodes are running correctly, one cluster group runs on each cluster node, balancing the load between the two systems. If one of the nodes fails, the second cluster group on the node that is still active starts automatically to continue the work of the cluster group that was active on the node that failed.

Information that is shared between different copies of the same agent is stored on a separate disk that can be accessed by all copies of the agent that are running on different cluster nodes. In active/active clustering, at least two instances of the agent run on each cluster node, each requiring a separate disk to store shared information. If the node that hosts the active agent fails and a copy of the agent on the other node is started, shared information can still be read and written to the disk as if the same copy of the agent was still running. The agent is installed separately on each cluster node. Shared disks store only log files and historical information that must be accessed by different copies of the same agent. Data that is related to your WebSphere MQ environment is stored in the configuration database on the Tivoli Enterprise Monitoring Server.

To install and configure the WebSphere MQ Configuration agent, repeat the procedure in “Configuring the WebSphere MQ Configuration agent” on page 250 for each instance of the WebSphere MQ Configuration agent in your environment.

Requirement: You must repeat this procedure for different copies of the same agent instance that are running on different cluster nodes.

Related tasks:

“Configuring the WebSphere MQ Configuration agent” on page 250

Configuring the WebSphere MQ Configuration agent in an active/passive clustering

Before you begin configuring the WebSphere MQ Configuration agent to run in an HACMP active/passive cluster environment, ensure that the two systems that form the cluster nodes in the environment are correctly configured. Both systems must meet the following requirements:

- HACMP is installed and your HACMP cluster environment is correctly configured.
- Both cluster nodes have access to a shared disk, on which information that is shared between copies of theWebSphere MQ Configuration agent that are running on different cluster nodes is stored.
- WebSphere MQ is installed and configured to run in an HACMP cluster environment. See your WebSphere MQ documentation for information about how to install WebSphere MQ in a cluster environment.
- The queue managers that you want to configure have been created on both cluster nodes within the HACMP cluster environment. Ensure that failover occurs correctly. See your WebSphere MQ documentation for more information.

An example of an active/passive cluster environment is displayed in Figure 67. The environment consists of two cluster nodes that are running on separate physical systems. The cluster groups that are hosted by each system are the same. Between them there are two identical copies of cluster group 1. Each cluster group contains one or more queue managers and an instance of the WebSphere MQ Configuration agent to monitor each queue manager.

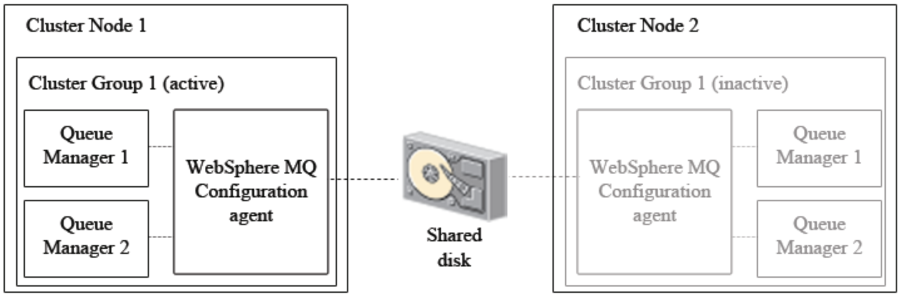


Figure 67. An example active-passive cluster environment architecture

Only cluster groups on one cluster node are active at one time. For example, if cluster group 1 is active on cluster node 1 (as in Figure 67), the copy of cluster group 1 on cluster node 2 is inactive. In an active/passive cluster environment with two cluster nodes, only cluster groups on the active cluster node run. If the active node fails, the cluster groups on the other node starts automatically to continue the work of the cluster groups that were active on the node that failed.

Information that is shared between different copies of the same agent is stored on a separate disk that can be accessed by all copies of the agent that are running on different cluster nodes. If the node that hosts the active agent fails and a copy of the agent on the other node starts, shared information can still be read and written to the disk as if the same copy of the agent was still running. The agent is installed separately on each cluster node.

To install and configure the WebSphere MQ Configuration agent, repeat the procedure in "Configuring the WebSphere MQ Configuration agent" for each instance of the WebSphere MQ Configuration agent in your environment.

Requirement: You must repeat this procedure for different copies of the same agent instance that are running on different cluster nodes.

Related tasks:

"Configuring the WebSphere MQ Configuration agent"

"Configuring the configuration database in an active/passive cluster environment" on page 251

Configuring the WebSphere MQ Configuration agent

Follow the instructions in this section to configure the WebSphere MQ Configuration agent to run in an HACMP cluster environment.

The configuration database is stored at the Tivoli Enterprise Monitoring Server and supports only active/passive clustering (the monitoring server also supports only active/passive clustering). For configuration instructions see "Configuring the configuration database in an active/passive cluster environment" on page 251.

To configure the WebSphere MQ Configuration agent for use in an HACMP cluster environment, do the following procedure:

1. Install the WebSphere MQ Configuration agent on the cluster node on which you want the agent to run. See *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide* for installation instructions.
2. Create new instances of the WebSphere MQ Configuration agent for each queue manager that you want to configure by doing the following steps:
   a. Navigate to the `ITM_HOME/config` directory, where *ITM_HOME* is the directory where IBM Tivoli Monitoring is installed. The default directory is `/opt/IBM/ITM`.
   b. Create a new configuration file for each instance of the WebSphere MQ Configuration agent by copying the content of the default `mc.cfg` configuration file to `hostname_mc_instancename.cfg`, where *hostname* is the hostname of the cluster node and *instancename* is the name of the WebSphere MQ Configuration agent instance.
   c. Edit each of the created new configuration files as follows:

      ```
      KMC_CLUSTERNAME=clus_name
      KMC_QUEUEMGRS=[qm1_name,qm2_name, ...]
      ```

      where *clus_name* is the name of the cluster that you want to be displayed in the Tivoli Enterprise Portal Configuration view and physical view, *qm1_name* and *qm2_name* are the names of the queue managers that you want to configure and the queue manager names are separated by commas.
3. Create a file that contains the startup script that is used to start the agent:
   a. Create a new text file and enter the following lines:
      - To start the queue manager:

        ```
        MC91_install/bin/hamqm_start QM_name
        ```
      - To start the WebSphere MQ Configuration agent:

        ```
        ITM_HOME/bin/itmcmd agent -o instance_name start mc
        ```

      where *ITM_HOME* is the directory in which IBM Tivoli Monitoring is installed on the shared disk, *MC91_install* is the directory in which

WebSphere MQ supportpac MC91 is installed, *QM_name* is the name of the queue manager and *instance_name* is the name of the WebSphere MQ Configuration agent instance. WebSphere MQ supportpac MC91 should have been installed when installing WebSphere MQ in the HACMP cluster environment. See your WebSphere MQ documentation for further information.

b. Save the file as `kmc_start.sh`.

Remember: When writing a startup script, ensure that the queue manager is started before the WebSphere MQ Configuration agent.

4. Create a file that contains the shutdown script that is used to stop the agent:

a. Create a new text file and enter the following lines:

- To stop the WebSphere MQ Configuration agent:

```
ITM_HOME/bin/itmcmd agent -o instance_name stop mc
```

- To stop the queue manager:

```
MC91_install/bin/hamqm_stop QM_name 5
```

where *ITM_HOME* is the directory in which IBM Tivoli Monitoring is installed on the shared disk, *MC91_install* is the directory in which WebSphere MQ supportpac MC91 is installed, *QM_name* is the name of the queue manager and *instance_name* is the name of the WebSphere MQ Configuration agent instance. WebSphere MQ supportpac MC91 should have been installed when installing WebSphere MQ in the HACMP cluster environment. See your WebSphere MQ documentation for further information.

b. Save the file as `kmc_stop.sh`.

Remember: When writing a shutdown script, ensure that the WebSphere MQ Configuration agent is stopped before the queue manager.

5. Do the following steps to set the scripts that are used to start and stop the agent in HACMP environment:

a. Open the cluster group in the HACMP cluster software.

b. Under Application Server set the start script as `kmc_start.sh`.

c. Under Application Server set the stop script as `kmc_stop.sh`.

The WebSphere MQ Configuration agent is now configured to operate in an HACMP cluster environment.

Related tasks:

"Configuring the WebSphere MQ Configuration agent in an active/active clustering" on page 247

"Configuring the WebSphere MQ Configuration agent in an active/passive clustering" on page 249

Configuring the configuration database in an active/passive cluster environment

The configuration database is stored at the Tivoli Enterprise Monitoring Server. Both the configuration database and the monitoring server supports active/passive clustering only. To configure the configuration database for use in an HACMP active/passive cluster environment, do the following procedure:

1. Install the Tivoli Enterprise Monitoring Server in an HACMP active/passive cluster environment on a shared disk. See your IBM Tivoli Monitoring documentation for installation instructions. After installation is complete, ensure that failover occurs correctly.
2. Install application support for the WebSphere MQ Configuration agent at the monitoring server. This includes the configuration database. See *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide* for instructions.
3. Add application support to the monitoring server by running the following command:

   ```
   shared_disk/ITM/bin/itmcmd support -t TEMS_name cf
   ```

   where *shared_disk* is the name of the shared disk and *TEMS_name* is the name of the monitoring server.
4. Recycle the Tivoli Enterprise Monitoring Server.

The configuration database is now configured to operate in an HACMP active/passive cluster environment.

Related tasks:

"Configuring the WebSphere MQ Configuration agent in an active/passive clustering" on page 249

Chapter 15. Configuring a remote queue manager

Use this section to learn the basic concepts of remote configuration and follow the instructions to set up your environment to configure a queue manager that is running on an operating system that is not currently supported by the WebSphere MQ Configuration agent.

Remote configuration is a method of using a WebSphere MQ Configuration agent to configure a queue manager that is located on a remote system with no configuration agent. Local configuration uses a WebSphere MQ Configuration agent to configure a queue manager that is located on the same system as the configuration agent.

Tip: The WebSphere MQ Configuration agent cannot discover or create remote queue managers. Because of this, install a configuration agent on every node in your environment that is running on a supported operating system instead of using the remote configuration feature if possible.

If you want to configure queue managers within your WebSphere MQ environment that are running on operating systems that are not currently supported by WebSphere MQ Configuration agent, such as Tandem, you can use remote configuration. Table 18 compares configuring a queue manager locally to configuring a queue manager remotely.

If you want to submit an MQSC command from the WebSphere MQ Configuration agent to the remote queue manager, make sure that a WebSphere MQ Monitoring agent is installed on the same computer as the WebSphere MQ Configuration agent and it is configured to monitor the remote queue manager.

Table 18. Comparison between configuring a queue manager locally and remotely

Functionality	Configuring a queue manager locally	Configuring a queue manager remotely
Discover an existing queue manager	√	
Discover the resources of an existing queue manager	√	√
Create a queue manager in your WebSphere MQ environment	√	
Create resources for an existing queue manager	√	√
Configure an existing queue manager	√	√
Configure resources of an existing queue manager	√	√
Start and stop a queue manager and its resources	√	
Create and define clusters	√	√
Update defined configuration from actual	√	√

Table 18. Comparison between configuring a queue manager locally and remotely (continued)

Functionality	**Configuring a queue manager locally**	**Configuring a queue manager remotely**
Update actual configuration from defined	√	√
View discrepancy between defined resources and actual resources	√	√
Set access authority for WebSphere MQ Objects	√	
Configure multiple queue managers running on different Tandem two-system clusters		√

Remote configuration is a method of configuring a queue manager that is deployed on a system with no configuration agent. When using remote configuration, a WebSphere MQ Configuration agent that is located on one system performs configuration tasks on another system. The WebSphere MQ Configuration agent uses communication channels between a local queue manager and the queue manager on the system that does not have a WebSphere MQ Configuration agent to perform configuration.

The WebSphere MQ Configuration agent is connected to a queue manager on the local system, and uses this queue manager to send configuration messages to the remote queue manager using standard WebSphere MQ transmission channels. The information that is contained in the messages is used to instruct the remote message queue to perform the configuration actions. Confirmation is then sent to the local WebSphere MQ Configuration agent, also using WebSphere MQ messages. The following diagram illustrates this architecture.

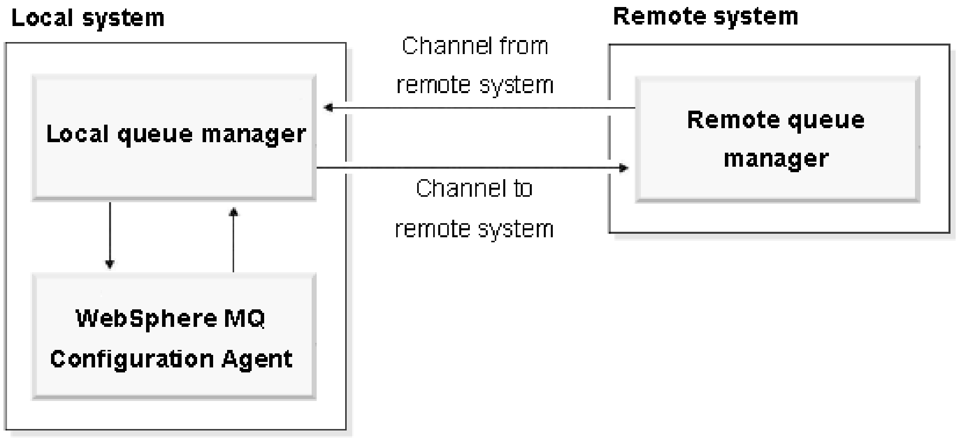


Figure 68. Remote configuration communications architecture

Prerequisite

Before setting up your environment for remote configuration, you must have a WebSphere MQ Configuration agent and a queue manager running on Windows 2000, Windows 2003, Linux, or AIX systems.

Setting up queue managers for remote configuration

Do the following procedures to set up queue managers for remote configuration:

1. "Creating user accounts for remote configuration"
2. "Checking your existing configuration"
3. "Defining transmission queues for WebSphere MQ Configuration agent" on page 256

Related tasks:

"Creating remote queue manager objects" on page 257

Creating user accounts for remote configuration

On operating systems that are not Windows systems, remote configuration is performed using the mqm user account on both the local and remote systems by default. However you can also use another user account to perform remote configuration. On Window systems, the mqm user account does not exist. So you must create another equivalent user account for remote configuration on Window systems.

To use a different account, you must set up the relevant user permissions on both the local and remote systems by doing the following steps:

1. On both the local and remote systems, create a user account with the authority to administer WebSphere MQ. These accounts must both have the same name.
2. On the local system (on which the WebSphere MQ Configuration agent is installed), use a text editor to open the parameters file that is stored in the IBM Tivoli Monitoring installation directory. For example, on Windows systems this directory is `C:\IBM\ITM\tmaitm6` by default. The file name varies depending on which operating system you are using, as follows:
   - On Windows and z/OS systems, the file name is `kmcenv`.
   - On all systems other than Windows and z/OS systems, the file name is `mc.ini`.
3. Add the following line at the end of the parameters file:

   ```
   KMC_REMOTE_CONFIG_USER_NAME=user_name
   ```

   where *user_name* is the user name that you used when creating the user accounts in step 1.
4. Save and exit the text editor.
5. Restart the WebSphere MQ Configuration agent.

Related tasks:

"Checking your existing configuration"

Checking your existing configuration

If your existing WebSphere MQ environment already has channels and transmission queues that can be used for communication between the WebSphere MQ Configuration agent and the remote queue manager, you do not need to define new transmission queues or channels. Otherwise, you should create queues and channels that are necessary to facilitate this communication. See the WebSphere MQ documentation for more information about creating these objects.

If there are intermediate WebSphere MQ queue managers that receive and then retransmit messages between the local and remote queue managers, you must define queue manager aliases on each intermediate queue manager to identify the destination queue managers.

Related tasks:

"Creating user accounts for remote configuration" on page 255

"Defining transmission queues for WebSphere MQ Configuration agent"

Defining transmission queues for WebSphere MQ Configuration agent

If your WebSphere MQ environment already contains two-way communication links between the remote queue manager and the local queue manager, the WebSphere MQ Configuration agent can use your existing configuration. However, you must ensure that the transmission queue on the remote queue manager has the same name as the local queue manager and that the transmission queue on the local queue manager has the same name as the remote queue manager. If these names are not correct, you can assign queue manager aliases to them (using the WebSphere MQ **DEFINE QREMOTE** command) with the names of the destination queue managers.

Related tasks:

"Checking your existing configuration" on page 255

Example of configuring WebSphere MQ for communication between local and remote queue managers

There are many ways to configure WebSphere MQ so that the local queue manager that is used to communicate with the configuration agent can pass commands to the remote queue manager and receive replies. The following example shows you how you might configure your WebSphere MQ network to use the remote configuration feature.

The simplest way is to create new transmission queues and channels specifically for remote configuration. This example shows how you can configure the WebSphere MQ Configuration agent running on AIX node AIX1 (with QMAIX1 queue manager) so that it can configure the WebSphere MQ environment that is running on Tandem node TandemA (with queue manager QMTandem1). This example uses sender and receiver channels.

The following commands are the definitions for QMTandem1 queue manager:

```
DEFINE QLOCAL(QMAIX1) USAGE(XMITQ)

DEFINE CHANNEL(QMTandem1.TO.QMAIX1) +
CHLTYPE(SDR) TRPTYPE(TCP) +
CONNAME('AIX1(1414)') +
XMITQ(QMAIX1)

DEFINE CHANNEL(QMAIX1.TO.QMTandem1) +
CHLTYPE(RCVR) +
TRPTYPE(TCP)
```

The following commands are the definitions for QMAIX1:

```
DEFINE QLOCAL(QMTandem1) USAGE(XMITQ)

DEFINE CHANNEL(QMAIX1.TO.QMTandem1) +
CHLTYPE(SDR) +
TRPTYPE(TCP) +
CONNAME('TandemA(1414)') +
XMITQ(QMTandem1)

DEFINE CHANNEL(QMTandem1.TO.QMAIX1) +
CHLTYPE(RCVR) +
TRPTYPE(TCP)
```

Creating remote queue manager objects

When you add a remote queue manager object to your Defined View, you must specify its indirect connection to the WebSphere MQ Configuration agent that is used to configure it.

The following procedure assumes that you have completed the tasks described in “Setting up queue managers for remote configuration” on page 255.

Related tasks:

“Setting up queue managers for remote configuration” on page 255

Defining the remote queue manager in the Defined View

Remote configuration requires that the remote queue manager already exists. See “Setting up queue managers for remote configuration” on page 255. It is not possible to actually create the new queue manager on the remote system using the WebSphere MQ Configuration agent.

To define the remote queue manager in the Defined View, do the following steps:

Important: If the granular security function is enabled in your environment, make sure that your system administrator has granted you the required authorities to perform this operation.

1. Ensure that you are in update mode. See “Entering update mode” on page 18 for information about how to enter update mode.
2. Open the Defined View.
3. In the defined view tree, right-click the configured system group to which you want to add the remote queue manager and click **Create** > **Queue Manager**. You are prompted to supply a name for the new queue manager.
4. Enter the name of the existing remote queue manager.
5. Click **OK**. The new queue manager is added to the defined view tree.
6. In the defined view tree, select the new remote queue manager. The settings list for the object is displayed on the right side of the Defined View.
7. Expand the Connection section.
8. In the Connection section, do the following steps:
   a. Select the **Indirect connection** check box.
   b. In the **Through queue manager** field, enter the name of the local queue manager that the WebSphere MQ Configuration agent is directly connected to, or select its name from the list. Specify the queue manager name exactly as it is displayed in the Defined View.
9. If your site uses a queue manager alias to connect the remote queue manager to the local queue manager that the WebSphere MQ Configuration agent is connected to, specify that alias in the **Queue manager alias** field.

10. If the remote queue manager is running on a z/OS system, select the check box that indicates an OS/390® system.
11. In the Manager section of the settings list, enter a host system name in the **Host system name** field or select a name from the list. The host system name is the name of the system that hosts the local queue manager.
12. Complete the remaining sections of the settings list as necessary.
13. Click **Save** to save your changes.
14. In the defined view tree, right-click the new remote queue manager object and click **Discover new resources** to add newly discovered resources that are in the new remote queue manager to the configuration database and the defined view tree.
15. In the defined view tree, right-click the new remote queue manager object and click **Update** > **Defined from actual** to update the definition of the new remote queue manager.

Restriction: If the remote queue manager is running on a Linux or UNIX operating system, its **Queue Manager Platform Type** attribute in the settings list is set to UNIX.

Appendix A. Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully. With the major accessibility features in this product, users can do the following things:

- Use assistive technologies, such as screen-reader software and digital speech synthesizer, to hear what is displayed on the screen. Consult the product documentation of the assistive technology for details on using those technologies with this product.
- Operate specific or equivalent features using only the keyboard.
- Magnify what is displayed on the screen.

In addition, the product documentation was modified to include the following features to aid accessibility:

- All documentation is available in both HTML and convertible PDF formats to give the maximum opportunity for users to apply screen-reader software.
- All images in the documentation are provided with alternative text so that users with vision impairments can understand the contents of the images.

Magnifying what is displayed on the screen

You can enlarge information on the product windows using facilities provided by the operating systems on which the product is run. For example, in a Microsoft Windows system environment, you can lower the resolution of the screen to enlarge the font sizes of the text on the screen. Refer to the documentation provided by your operating system for more information.

Navigating the interface using the keyboard

Standard shortcut and accelerator keys are used by the product and are documented by the operating system. Refer to the documentation provided by your operating system for more information.

Appendix B. Architecture codes

IBM Tivoli software uses abbreviations to represent the various operating system architectures. The table below shows the most current listing of these abbreviations.

This information can also be found in the following file on UNIX systems: *install_dir*/registry/archdsc.tbl.

Table 19. Operating system architecture abbreviations

Abbreviation	Operating System Architecture
aix513	AIX v5.1 (32 bit)
aix516	AIX v5.1 (64 bit)
aix523	AIX v5.2 (32 bit)
aix526	AIX v5.2 (64 bit)
aix533	AIX v5.3 (32 bit)
aix536	AIX v5.3 (64 bit)
citrix	Citrix Metaframe
hp10	HP-UX v10.01/10.10
hp102	HP-UX v10.20
hp11	HP-UX v11
hp116	HP-UX v11 (64 bit)
li622	Linux Intel v2.2
li6223	Linux Intel v2.2 (32 bit)
li624	Linux Intel v2.4
li6242	Linux Intel v2.4 GCC 2.9.5 (32 bit)
li6243	Linux Intel v2.4 (32 bit)
li6245	Linux Intel v2.4 GCC 2.9.5 (64 bit)
li6246	Linux Intel v2.4 (64 bit)
li6262	Linux Intel v2.6 GCC 2.9.5 (32 bit)
li6263	Linux Intel v2.6 (32 bit)
li6265	Linux Intel v2.6 GCC 2.9.5 (64 bit)
li6266	Linux Intel v2.6 (64 bit)
ls322	Linux zSeries, 2.2 kernel
ls3223	Linux zSeries, v2.2 (32 bit)
ls3226	Linux zSeries, v2.2 (64 bit)
ls324	Linux zSeries, v2.4
ls3243	Linux zSeries, v2.4 (32 bit)
ls3246	Linux zSeries, v2.4 (64 bit)
ls3262	Linux S390 v2.6 GCC 2.9.5 (32 bit)
ls3263	Linux S390 v2.6 (32 bit)
ls3265	Linux S390 v2.6 GCC 2.9.5 (64 bit)

Table 19. Operating system architecture abbreviations (continued)

Abbreviation	Operating System Architecture
ls3266	Linux S390 v2.6 (64 bit)
osf1	Digital UNIX (prior to V5.0)
os390	OS/390 or z/OS
os400	OS/400®
sol24	Solaris v2.4
sol25	Solaris v2.5
sol26	Solaris v2.6
sol273	Solaris v7 (32 bit)
sol276	Solaris v7 (64 bit)
sol283	Solaris v8 (32 bit)
sol286	Solaris v8 (64 bit)
sol293	Solaris v9 (32 bit)
sol296	Solaris v9 (64 bit)
sol503	Solaris v10 (32 bit)
sol506	Solaris v10 (64 bit)
sol603	Solaris v10 Opteron (32 bit)
sol606	Solaris v10 Opteron (64 bit)
tsf50	Tru64 v5.0
unix	UNIX
winnt	Windows 2000 and Windows 2003 Server

Appendix C. Creating another user ID with equivalent authorities as sysadmin

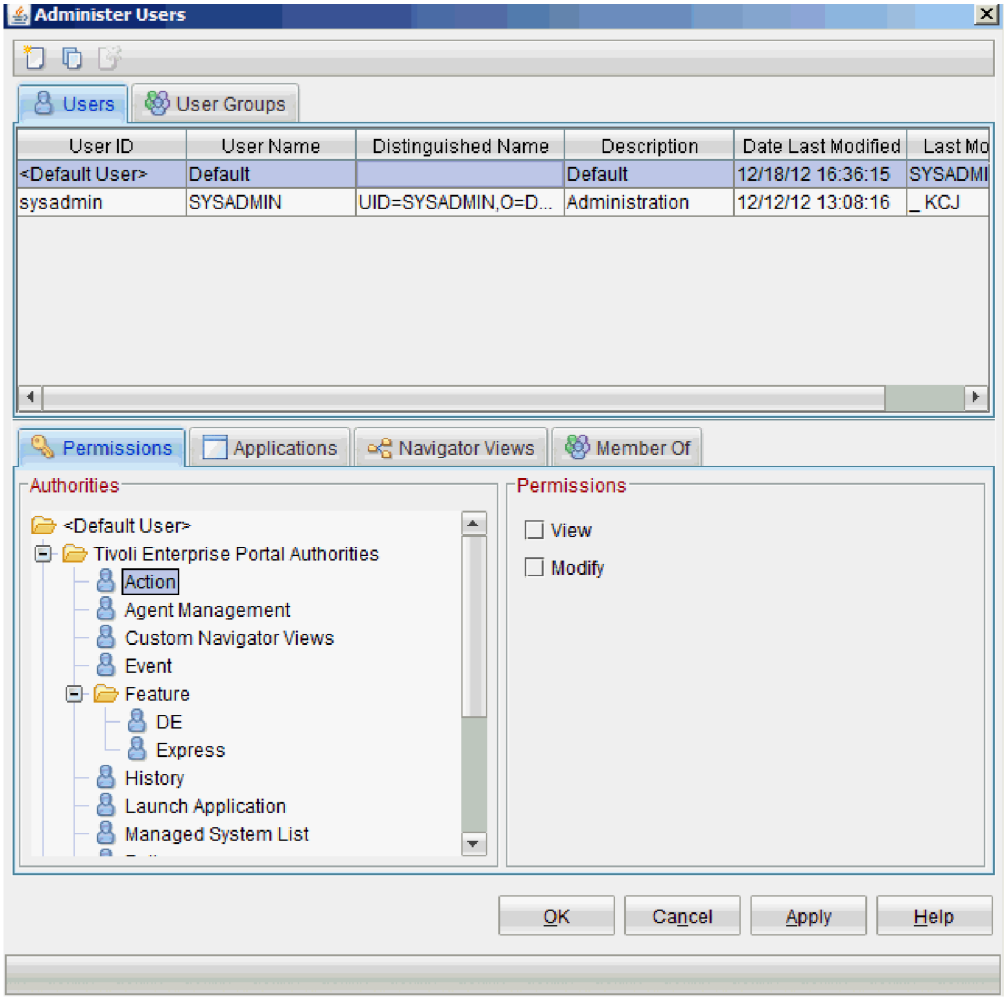
If you do not want to use the sysadmin ID to log on to Tivoli Enterprise Portal, you can use the User Administration function to create another user ID with equivalent authorities as sysadmin.

By default, the sysadmin ID is used as the security administrator. However, you can abandon the sysadmin ID and use another user ID for administration.

Remember: The initial sysadmin user ID with full administrator authority is provided during the installation of IBM Tivoli Monitoring. You can use the procedure in this section as an example to create a user ID with equivalent authorities as the sysadmin ID. For detailed information about authorizing the sysadmin user ID, see *IBM Tivoli Monitoring Installation and Setup Guide*. For more information about user administration, see *IBM Tivoli Monitoring Administrator's Guide*.

To create another user ID with equivalent authorities as sysadmin, do the following steps:

1. Log on to the Tivoli Enterprise Portal as sysadmin.
2. Click **Edit** > **Administer Users**. The Administer Users window is displayed as shown in Figure 69 on page 264.



User ID	User Name	Distinguished Name	Description	Date Last Modified	Last Mo
<Default User>	Default		Default	12/18/12 16:36:15	SYSADMI
sysadmin	SYSADMIN	UID=SYSADMIN,O=D...	Administration	12/12/12 13:08:16	_ KCJ

- <Default User>
  - Tivoli Enterprise Portal Authorities
    - Action
    - Agent Management
    - Custom Navigator Views
    - Event
    - Feature
      - DE
      - Express
    - History
    - Launch Application
    - Managed System List

□ View

□ Modify

Figure 69. The Administer Users window

3. Click **Create New User**.
4. In the Create New User window, enter the following user information:
   - **User ID**: The logon name. This name can be up to 10 characters and can contain no spaces. The name is limited to eight characters if user authentication is at the hub monitoring server and uses resource access control facility (RACF) security for z/OS systems.
   - **User Name**: The name of the user or job classification or both. This name can include spaces and be up to 32 characters. The user name is displayed in Users list.
   - **Distinguished Name**: The unique identifier in the Lightweight Directory Access Protocol repository for the name given in the **User ID** field. Click **Find** to locate and insert the distinguished name.
   - **User Description**: Optional description for the user. The text can include spaces and punctuation.
5. Click **OK** to close the Create New User window. The new user ID is listed alphabetically in the **Users** list.
6. Click the **Permissions** tab and select the following permission options for the user ID.

Table 20. Required permissions for a security administrator ID

Function		Permission
Tivoli Enterprise Portal Authorities	Action	• View • Modify
	Agent Management	• Manage • Start/Stop
	Custom Navigator Views	• Modify
	Event	• Attach • Close • View • Acknowledge
	History	• Configure
	Launch Application	• Launch • View • Modify
	Managed System List	• View • Modify
	Policy	• View • Modify • Start/Stop
	Query	• View • Modify
	Situation	• View • Modify • Start/Stop
	Terminal Script	• View • Modify
	User Administration	• Logon Permitted • Modify • Author Mode Eligible • View • Administration Mode Eligible
	Workspace Administration	• Workspace Author Mode
WebSphere MQ Configuration Authorities	Configure	• View • Modify

7. Click the **Applications** tab.
8. Select **<All Applications>**, and click the left arrow to move it to the **Allowed Applications** list.
9. Click the **Navigator Views** tab.
10. From the **Available Views** list, select **Configuration**, **Logical**, and **Physical**, and then click the left arrow to add them to the **Assigned Views** list.

11. To save your changes and keep the Administer Users window open, click **Apply**. Or to save the changes and close the window, click **OK**.

Now the new user ID has equivalent authorities as the sysadmin ID. For more information about administering users, see User administration in *IBM Tivoli Monitoring Administrator's Guide*.

Tip: When you log on to the Tivoli Enterprise Portal, the Logon window has a field for entering a password. If you want the new user ID to include a password, you must define the same user ID, including a password, to your network domain user accounts or to the operating system where the hub monitoring server is installed.

Appendix D. Granting WebSphere MQ OAM authorities to a user ID

If you are using WebSphere MQ version 7.0.1 or later, you can use a user ID that is not a member of the **mqm** group to start, stop, or run the WebSphere MQ Configuration agent.

If the user ID that is used to start, stop, or run the agent does not belong to the **mqm** group, do the following steps to grant object authority manager (OAM) authorities to the user ID:

1. Log on to the computer with a user ID that is a member of the **mqm** group.
2. Run the following command to grant OAM authorities for the queue managers to the user ID that is used to start, stop or run the agent:

   ```
   setmqaut -m QMgrName -t qmgr -p userID +inq +connect +dsp +setid
   ```

   where *QMgrName* is the name of the queue manager for which you want to grant authorities, *userID* is the user ID for which the OAM authorities are granted.
3. Run the following command to grant OAM authorities for the following queues to the user ID that is used to start, stop or run the agent:

   ```
   setmqaut -m QMgrName -t q -n SYSTEM.ADMIN.COMMAND.QUEUE -p userID +inq +get
      +dsp +put +setid
   setmqaut -m QMgrName -t q -n KMC.IRA.* -p userID +inq +get +dsp +put
   setmqaut -m QMgrName -t q -n SYSTEM.DEFAULT.MODEL.QUEUE -p userID +dsp +get
   setmqaut -m QMgrName -t q -n SYSTEM.AUTH.DATA.QUEUE -p userID +dsp
   ```

   Now the user ID can be used to start and stop the agent. And the user can see the WebSphere MQ Configuration agent from Tivoli Enterprise Portal.

If the user wants to use the operations that are provided by the WebSphere MQ Configuration agent, you must also grant specific OAM authorities for the related WebSphere MQ objects to the user ID. For example, if the user wants to use the Discovery function, the user ID must have "dsp" authority for all objects of the queue manager. If the user wants to use the Update function to synchronize defined resources with actual resources in the WebSphere MQ environment, the user ID must have "dsp" authorities for the related WebSphere MQ objects. If the user wants to use the Update function to synchronize actual resources with defined resources in the configuration database, the user ID must have "dsp" and "chg" authorities for the related WebSphere MQ objects. For more information about the WebSphere MQ OAM authority requirements, see *WebSphere MQ System Administration Guide*.

Appendix E. Using the command line interface function

If you have no access to Tivoli Enterprise Portal Server or Tivoli Enterprise Portal, you can use the command line interface to import XML files to the configuration database, export resource configurations to XML files, and trigger on-demand scheduled actions.

The command line interface function (referred to as the MCCLI function hereafter) is a standalone program that is designed to assist users who has no access to Tivoli Enterprise Portal Server or Tivoli Enterprise Portal to do the following things:

- Import XML files to the configuration database
- Export resource configurations to XML files
- Trigger on-demand scheduled actions

The MCCLI function consists of the following commands that are available on Windows, Linux, and UNIX systems:

- **MCExport**, which is used to export configurations of resources from the configuration database to an XML file.
- **MCImport**, which is used to import an XML file to the configuration database.
- **MCRunSchedule**, which is used to trigger on-demand scheduled actions.

Important: You can use the function to update the resource definitions in the configuration database by first exporting them to an XML file and then importing the XML file after modification. Because this process uses the resource name to identify the resource that will be updated in the configuration database, you must ensure the name of the resource you want to operate (both the resolved and unresolved name if the resource uses a symbolic variable in its name) is unique in the configuration database when using this function.

The MCCLI program is provided in the `MCCLI` directory of the product installation CD. Copy the content of the directory to the system where you want to use the MCCLI commands. Different files are provided for the MCCLI commands. The `.sh` files apply to UNIX and Linux systems, and the `.bat` files apply to Windows systems. To run the commands, navigate to the directory where you save the `.sh` files or `.bat` files, and run the corresponding file.

Remember: Java version 1.4.2 or later is required for the MCCLI function.

MCExport

Use the MCExport command to export resource configuration from the configuration database to an XML file.

Syntax

The MCExport command is used to export configuration information of resources from the configuration database to an XML file. The `MCExport.sh` file applies to UNIX and Linux systems, and the `MCExport.bat` file applies to Windows systems.

Remember: If the granular security function is enabled in your environment, when you run the **MCExport** command, the WebSphere MQ Configuration agent only checks your user ID to see if your are authorized to perform the operation on the target object; it does not check the group IDs that your user ID belongs to. The administrator must assign authorities to the specific user ID that is used to run this command, regardless of the group ID or administrator group to which the user ID belongs.

```
MCExport -ExportOption -t TemsHost -p Port -u UserName -w Password -f FileName -d
    Location -o ObjectList
```

After you run the command, an MCCLI XML file is created. For an example of an MCCLI XML file and the major tags, see "Example of an MCCLI XML file" on page 275. For a detailed list of tags of WebSphere MQ resource attributes in an MCCLI XML file, see "Tags of WebSphere MQ resource attributes in an MCCLI XML file" on page 276.

Important: If you want to export multiple objects, ensure that they belong directly to the same node in the defined view or prototype view. For example, if you want to export multiple resources, ensure that they belong directly to the same resource group.

Parameters

ExportOption
The export option. It has the following valid options:

- PARTIAL: Specify PARTIAL to export information about only WebSphere MQ resources and their attributes to an XML file.
- EXTENDED: Specify EXTENDED to export information about WebSphere MQ resources, their attributes, and WebSphere MQ Configuration resources such as resource groups.
- MQSC: Specify MQSC to export MQSC commands that are used to create the WebSphere MQ resources.
- ALL: Specify ALL to export the entire configuration database, including global variables, defined resources, and prototype resources.

TemsHost
Specify the host name or IP address of the host on which the Tivoli Enterprise Monitoring Server is installed.

Port
Specify the port number of SOAP.

UserName
Specify the user ID that is used to log on to the Tivoli Enterprise Monitoring Server.

Password
Specify the password of the user ID. Specify a random string if security validation is disabled at the Tivoli Enterprise Monitoring Server.

Location
Specify the location of the resources that you want to export in the hierarchical tree. Do not specify the names of the resources that you want to export in this parameter. It takes the following format:

```
/Configured_System_Goup_Name/Configured_System_Name/Resource_Group_Name/
```

Depending on the location of the resources, you might specify multiple resource group names in the parameter.

Remember:

- On UNIX systems, if the dollar sign ($) is used in a location string, it must be prefixed by a backslash (\). For example, `/TESTENV_CSG/localhost.cn.ibm.c:TESTENV_QMA/\$Default_Group`.
- On Windows systems, if the a defined object name contains the forward slash (/), replace each forward slash with double forward slashes (//) in the location string. For example, if you want to export resources in the Q1//1/1 resource group, specify `/TESTENV_CSG/localhost.cn.ibm.c:TESTENV_QMA/Q1////1//1`.
- On UNIX or Linux systems, if the a defined object name contains the forward slash (/), replace each forward slash with double forward slashes (//) in the location string and add a backslash (\) in front of the first forward slash. For example, if you want to export resources in the Q1//1/1 resource group, specify `/TESTENV_CSG/localhost.cn.ibm.c:TESTENV_QMA/Q1\////1\//1`.
- Enclose the location string in quotation marks (" ") if it contains spaces.

FileName

Name of the XML file in which the exported data is stored.

ObjectList

Specify the names of the resources whose configuration information you want to export. Use a comma (,) to separate multiple resources and do not include space or backslash (\) in this parameter.

Important: The objects that you want to export must have unique names even if they are of different resource types.

Example 1: Exporting Q1 and CH1 in the Defined View

To export Q1 and CH1 in the Defined View in Figure 70, use the following command:

```
MCExport –Extended –t 9.123.145.129 –p 1920 –u sysadmin –w 11a00 –d /TESTENV_CSG/
   LENOVO-295688DD.cn.ibm.c:TESTENV/$Default_Group/TEST –f TESTENV1.xml –o
   Q1,CHL1
```

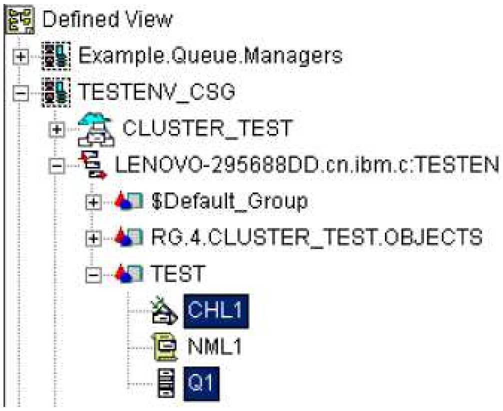


Figure 70. Q1 and CH1 in the Defined View

Example 2: Exporting the Queues resource group prototype in the Prototype View

To export the Queues resource group prototype in the Prototype View in Figure 71 on page 272, use the following command:

```
MCExport –Extended –t 9.123.145.129 –p 1920 –u sysadmin –w 11a00 –d "/Configured
    System Prototypes/TESTENV_QM_Proto" –f TESTENV2.xml –o Queues
```

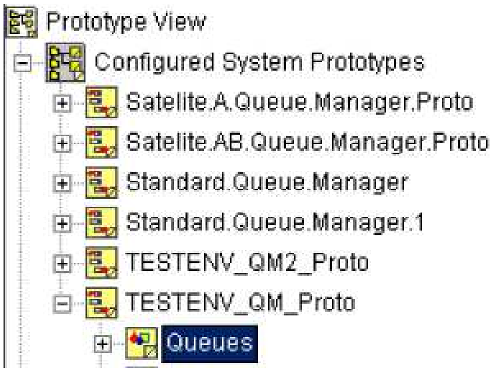


Figure 71. The Queues resource group prototype in the Prototype View

MCImport

Use the **MCImport** command to import an MCCLI XML file to the configuration database.

Syntax

You can use the **MCImport** command to import an XML file to the configuration database. It is a good practice to back up the configuration database before you use the **MCImport** command. The MCImport.sh file applies to UNIX and Linux systems, and the MCImport.bat file applies to Windows systems.

Remember: If the granular security function is enabled in your environment, when you run the **MCImport** command, the WebSphere MQ Configuration agent only checks your user ID to see if your are authorized to perform the operation on the target object; it does not check the group IDs that your user ID belongs to. The administrator must assign authorities to the specific user ID that is used to run this command, regardless of the group ID or administrator group to which the user ID belongs.

```
MCImport -t TemsHost -p Port -u UserName -w Password -f FileName -d Location -r
```

Important: To avoid syntax errors, use an exported MCCLI XML file as a template to create an XML file that you import to the configuration database.

Parameters

TemsHost
: Specify the host name or IP address of the host on which the Tivoli Enterprise Monitoring Server is installed.

Port
: Specify the port number of SOAP.

UserName
: Specify the user ID that is used to log on to the Tivoli Enterprise Monitoring Server.

Password

Specify the password of the user ID. Specify a random string if security validation is disabled on the Tivoli Enterprise Monitoring Server.

Location

Specify the location of the resource to which you want to import the resources in the XML file in the hierarchical tree. It takes the following format:

```
/Configured_System_Goup_Name/Configured_System_Name/Resource
   _Group_Name/Resource_Group_Name
```

Depending on the location of the resource, you might specify multiple resource group names in this parameter.

Remember:

- On UNIX systems, if the dollar sign ($) is used in a location string, it must be prefixed by a backslash (\), for example, /TESTENV_CSG/ localhost.cn.ibm.c:TESTENV_QMA/\$Default_Group.
- Enclose the path in quotation marks (" ") if it contains spaces.

FileName

Specify the name of the XML file that is to be imported.

-r Replace option. If one or more resources that are defined in the XML file already exist in the resource group, configured system, or configured system group that you import the XML file to, with the `-r` option specified, the resources are overwritten by those defined in the MCCLI XML file.

Remember:

- Be careful with specifying the `-r` option when the granular security function is enabled in your environment. If you specify the `-r` option, secure objects become non-secure objects after import. In that case, you must grant authorities for these objects again to protect them from unauthorized access.
- When the granular security function is enabled, the following authorities are required for this `-r` option:
  - DELETE authority for the object that is to be replaced
  - DELETE authority for all resources that are included in the object to be replaced
  - CREATE authority for the parent object to which the new object belongs

Example: Importing an XML file

To import an XML file that contains configuration information of Q1 and CHL1 to the &Default_Group resource group in the TESTENV_QMB queue manager in Figure 72 on page 274, use the following command:

```
MCImport –t 9.123.145.9 –p 1920 –u sysadmin –w 11a00 –d /TESTENV_CSG/LENOVO-295688DD
   .cn.ibm.c:TESTENV/$Default_Group TESTENV1.xml
```

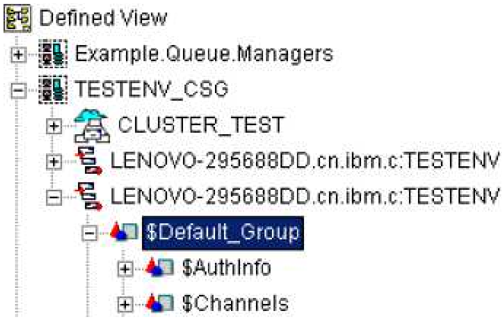


Figure 72. Default group in the Defined View

MCRunSchedule

Use the **MCRunSchedule** command to submit a command to trigger an on-demand scheduled action.

Purpose

You can use the **MCRunSchedule** command to submit a command to trigger an on-demand scheduled action. The `MCRunSchedule.sh` file applies to UNIX systems, and the `MCRunSchedule.bat` file applies to Windows systems.

Remember: If the granular security function is enabled in your environment, when you run the **MCRunSchedule** command, the WebSphere MQ Configuration agent only checks your user ID to see if your are authorized to perform the operation on the target object; it does not check the group IDs that your user ID belongs to. The administrator must assign authorities to the specific user ID that is used to run this command, regardless of the group ID or administrator group to which the user ID belongs.

```
MCRunSchedule -t TemsHost -p Port -u UserName -w Password -s ScheduleName
```

Parameters

TemsHost
Specify the host name or IP address of the host on which the Tivoli Enterprise Monitoring Server is installed.

Port
Specify the port number of SOAP.

UserName
Specify the user ID that is used to log on to the Tivoli Enterprise Monitoring Server.

Important: To run the **MCRunSchedule** command successfully, the *UserName* value must be the user ID that is used to create the schedule specified by the *ScheduleName* parameter.

Port
Specify the password of the user ID. Use a random string if security validation is disabled on the Tivoli Enterprise Monitoring Server.

ScheduleName
Specify the name of the on-demand scheduled action that you want to trigger.

Remember: After the **MCRunSchedule** command is issued, the message returned only indicates if the command is successfully triggered. It does not show if the scheduled actions run successfully.

Sample

To trigger the on-demand scheduled action named BackupDatabase, use the following command:

```
MCRunSchedule –t 9.123.145.129 –p 1920 –u sysadmin –w 11a00 –s BackupDatabase
```

Example of an MCCLI XML file

The following example MCCLI XML file uses the major elements that are used to represent different resources in the configuration database:

```
<?xml version="1.0" standalone="no" ?>
<CNFG Ver="07.00.01" Appl="MQ" Type="EXTENDED" Level="2" Date="03/09/2009" Time="
   16:07:06">
 <MGSYSGROUP>
  <HANDLE>0100000000000101</HANDLE>
  <PARENT>0000000000000000</PARENT>
  <CSGNAME>Example.Queue.Managers</CSGNAME>
   <MGSYS>
    <HANDLE>0800000000000201</HANDLE>
    <PARENT>0100000000000101</PARENT>
    <QMNAME>QM10</QMNAME>
    <RSCGROUP>
     <HANDLE>1400000000000301</HANDLE>
     <PARENT>0800000000000201</PARENT>
     <RGNAME>$Default_Group</RGNAME>
     <RSCGROUP>
      <HANDLE>1500000000000301</HANDLE>
      <PARENT>1400000000000301</PARENT>
      <RGNAME>$Processes</RGNAME>
       <RESOURCE>
        <HANDLE>5704000000000401</HANDLE>
        <PARENT>1500000000000301</PARENT>
        <PROCESS>SYSTEM.DEFAULT.PROCESS</PROCESS>
        <APPLTYPE>WINDOWSNT</APPLTYPE>
       </RESOURCE>
     </RSCGROUP>
    </RSCGROUP>
   <MGSYS>
 <MGSYSGROUP>
</CNFG>
```

Major tags in an MCCLI XML file

A traditional MCCLI XML file uses the following elements:

- CNFG is the root tag in an MCCLI XML file.
- MGSYSGROUP represents a configured system group.
- MGSYS represents a configured system.
- RSCGROUP represents a resource group.
- RESOURCE represents a resource.
- VRTOBJECT and PLACEHLDR are used for cluster resources.

Tags of WebSphere MQ resource attributes in an MCCLI XML file

The following tables list the tags of WebSphere MQ resource attributes in an MCCLI XML file and their descriptions.

Queue manager attributes and their tags in an MCCLI XML file

Table 21 lists the tags of queue manager attributes in an MCCLI XML file and their descriptions.

Table 21. Tags of queue manager attributes in an MCCLI XML file and their descriptions

Tag in an MCCLI XML file	Attribute description in WebSphere MQ
ACCTCINT	The time interval, in seconds, at which intermediate accounting records are written
ACCTONO	Specifies whether applications can override the settings of the ACCTQ and ACCTMQI queue manager parameters
ACCTMQI	Specifies whether accounting information for MQI data is collected
ACTIVREC	Whether activity reports are generated if requested in the message
ACCTQ	Specifies whether accounting data is collected for all queues
ACTCHL	The maximum number of channels that can be active at any time
ADOPTCHK	Specifies which elements are checked to determine whether an MCA should be adopted when a new inbound channel is detected with the same name as an MCA that is already active
ADOPTMCA	Whether an orphaned instance of an MCA should be restarted
AUTHOREV	Whether authorization (Not Authorized) events are generated
BRIDGEEV	Whether IMS™ Bridge events are generated
CCSID	The coded character set identifier for the queue manager
CHAD	Whether receiver and server-connection channels can be defined automatically
CHADEV	Whether channel auto-definition events are generated
CHLEV	Whether channel events are generated
CHIADAPS	The number of channel initiator adapter subtasks to use for processing WebSphere MQ calls
CHIDISPS	The number of dispatchers to use in the channel initiator
CHADEXIT	Auto-definition exit name
CLWLDATA	Cluster workload exit data

Table 21. Tags of queue manager attributes in an MCCLI XML file and their descriptions (continued)

Tag in an MCCLI XML file	Attribute description in WebSphere MQ
CLWLLEN	The maximum number of bytes of message data that is passed to the cluster workload exit
CLWLEXIT	Cluster workload exit name
CLWLMRUC	The maximum number of most recently used outbound cluster channels
CLWLUSEQ	For queues whose CLWLUSEQ parameter has a value of QMGR, specifies the behavior of an MQPUT operation when the target queue has a local instance and at least one remote cluster instance (except where the MQPUT originates from a cluster channel)
CMDEV	Specifies whether command events are generated
CMDLEVEL	Command level. This indicates the function level of the queue manager
CONFIGEV	Whether configuration events are generated
DEADQ	The local name of a dead-letter queue
DEFXMITQ	Local name of the default transmission queue
DESCR	Optional plain-text comment.
DNSGROUP	The name of the group that the TCP listener handling inbound transmissions for the queue-sharing group should join when using Workload Manager for Dynamic Domain Name Services support
INHIBTEV	Whether inhibit events are generated
IPADDRV	Specifies which IP protocol is used for channel connections
LOCALEV	Whether local error events are generated
LOGGEREV	Whether recovery log events are generated
LU62ARM	The suffix of the APPCPM member of SYS1.PARMLIB
LU62CHL	The maximum number of channels that can be current, or clients that can be connected, that use the LU 6.2 transmission protocol.
LUGROUP	The generic LU name that is used by the LU 6.2 listener
LUNAME	The name of the LU to use for outbound LU 6.2 transmissions
MAXHANDS	The maximum number of open handles that any one connection can have at any one time.

Table 21. Tags of queue manager attributes in an MCCLI XML file and their descriptions (continued)

Tag in an MCCLI XML file	Attribute description in WebSphere MQ
MAXMSGL	The maximum message length that can be handled by the queue manager. Individual queues or channels might have a smaller maximum than this
MAXPRTY	The maximum priority
MAXUMSGS	Maximum number of uncommitted messages within one syncpoint
MONCHL	Controls the collection of online monitoring data for channels
MONQ	Whether online monitoring data is collected for queues, and, if so, the rate of data collection
MONACLS	Whether online monitoring data is collected for auto-defined cluster-sender channels, and, if so, the rate of data collection
QMNAME	The queue manager name
PERFMEV	Whether performance-related events are generated
PLATFORM	The architecture of the platform on which the queue manager is running
REMOTEEV	Whether remote error events are generated
REPOS	The name of a cluster for which this queue manager provides a repository manager service
REPOSNL	The name of a namelist of clusters for which this queue manager provides a repository manager service
ROUTEREC	Whether trace-route information is recorded if requested in the message
SCHINIT	Whether the channel initiator should start automatically when the queue manager starts
SCMDSERV	Whether the command server should start automatically when the queue manager starts
SSLCRLNL	The name of a namelist of authentication information objects that are used for Certificate Revocation List (CRL) checking by the queue manager
SSLCRYP	Sets the name of the parameter string required to configure the cryptographic hardware present on the system
SSLEV	Whether SSL events are generated
SSLFIPS	Whether only FIPS-certified algorithms are used if cryptography is executed in WebSphere MQ itself

Table 21. Tags of queue manager attributes in an MCCLI XML file and their descriptions (continued)

Tag in an MCCLI XML file	Attribute description in WebSphere MQ
SSLKEYR	The name of the Secure Sockets Layer key repository
SSLRKEYC	Indicates the number of unencrypted bytes sent and received within an SSL conversation before the secret key is renegotiated
STATACLS	Whether statistics data is collected for auto-defined cluster-sender channels
STATINT	The time interval, in seconds, at which statistics monitoring data is written to the monitoring queue
STATCHL	Whether statistics data is collected for channels
STATQ	Whether statistics data is collected for queues
STRSTPEV	Whether start and stop events are generated
SYNCPOINT	Whether syncpoint support is available
TCPNAME	The name of either the only, or default, TCP/IP system that is used, depending on the value of TCPSTACK
TRAXSTR	Specifies whether the channel initiator trace should start automatically
TRAXTBL	The size, in megabytes, of the channel initiator's trace data space
TRIGINT	The trigger interval

Queue attributes and their tags in an MCCLI XML file

Table 22 lists the tags of queue attributes in an MCCLI XML file and their descriptions.

Table 22. Tags of queue attributes and their descriptions

Tag in MCCLI XML file	Attribute name in WebSphere MQ
ALTDATE	The date on which the definition or information was last altered, in the form yyyy-mm-dd
ALTTIME	The time at which the definition or information was last altered, in the form hh.mm.ss
BOTHRESH	The backout threshold
BOQNAME	The excessive backout queue name
CLUSTER	The name of the cluster that the queue belongs to
CLUSNMLNM	The name of the namelist that specifies a list of clusters that the queue belongs to

Table 22. Tags of queue attributes and their descriptions (continued)

Tag in MCCLI XML file	Attribute name in WebSphere MQ
CLWLPRTY	Specifies the priority of the queue for the purpose of cluster workload distribution
CLWLRANK	Specifies the rank of the queue for the purpose of cluster workload distribution
DEFBIND	Default message binding
DEFSOPT	Default share option on a queue that is opened for input
DEFPRTY	Default priority of messages that are put on this queue
DEFPSIST	Default persistence of messages that are put on this queue
DEFTYPE	Queue definition type
DESCR	Optional plain text comment
DISTL	Specifies whether distribution lists are supported by the partner queue manager
GET	Specifies whether the queue is enabled for gets
HARDENBO	Specifies whether the back out count is hardened to ensure that the count of the number of times that a message has been backed out is accurate
INITQ	The local name of a local queue (known as the *initiation* queue) on this queue manager that trigger messages relating to this queue are written to
MAXMSGL	Maximum message length
MAXDEPTH	Maximum depth of queue
MSGDLVSQ	Message delivery sequence
NPMCLASS	Level of reliability that is assigned to nonpersistent messages that are put to the queue
PUT	Specifies whether the queue is enabled for puts
QUEUE	The local name of the queue definition that is displayed
QDPHIEV	Specifies whether queue depth high events are generated
QDEPTHHI	Threshold of queue death high event generation
QDELOEV	Specifies whether queue depth low events are generated
QDEPTHLO	Threshold of queue death low event generation
QDPMAXEV	Specifies whether queue full events are generated
QSVCINT	Service interval event generation threshold

Table 22. Tags of queue attributes and their descriptions (continued)

Tag in MCCLI XML file	Attribute name in WebSphere MQ
QSVCIEV	Specifies whether service interval events are generated
RETINTVL	Retention interval
RQMNAME	Remote queue manager name
RNAME	Name of the local queue, as known by the remote queue manager
SCOPE	Scope of queue definition
SHARE	Specifies whether the queue can be shared
TARGQ	The name of the queue being aliased
TRIGDATA	The data that is inserted in the trigger message
TRIGDPTH	The number of messages that have to be on the queue before a trigger message is written, if TRIGTYPE is DEPTH.
TRIGMPRI	The message priority number that triggers this queue
TRIGGER	Specifies whether triggers are active
TRIGTYPE	Specifies whether and under what conditions a trigger message is written to the initiation queue
TYPE	Queue type
USAGE	Queue usage
XMITQ	Transmission queue name

Process attributes and their tags in an MCCLI XML file

Table 23 lists the tags of process attributes in an MCCLI XML file and their descriptions.

Table 23. Tags of process attributes and their descriptions

Tag in MCCLI XML file	Attribute name in WebSphere MQ
ALTDATE	The date on which the definition was last altered, in the form of yyyy-mm-dd
ALTTIM	The time at which the definition was last altered, in the form of hh.mm.ss
APPLICID	Application identifier
APPLTYPE	Application type
ENVRDATA	Environment data
DESCR	Optional plain text comment
PROCESS	Process name
QSGDISP	Specifies the disposition of the objects for which information is displayed
USERDATA	User data

Channel attributes and their tags in an MCCLI XML file

Table 24 lists the tags of channel attributes in an MCCLI XML file and their descriptions.

Table 24. Tags of channel attributes in an MCCLI XML file and their descriptions

Tag in MCCLI XML file	Description
AUTOSTART	Specifies whether an LU 6.2 responder process should be started for the channel
BATCHHB	The batch heartbeating value that is used
BATCHINT	Minimum batch duration
BATCHSZ	Batch size
CHANNEL	The name of the channel definition that is displayed
CHLTYPE	Channel type
CLWLPRTY	The priority of the channel for the purpose of cluster workload distribution
CLWLRANK	The rank of the channel for the purpose of cluster workload distribution
CLWLWGHT	The weighting of the channel for the purpose of the cluster workload distribution
COMPHDR	The list of head data compression techniques that are supported by the channel
COMPMSG	The list of message data compression techniques that are supported by the channel
CONVERT	Specifies whether sender should convert application usage data
CONNAME	Connection name
DESCR	Optional plain text comment
DISCINT	Disconnection interval
HBINT	Heartbeat interval
KAINT	KeepAlive timing for the channel
LOCLADDR	Local communications address for the channel
LONGRTY	Long retry count
LONGTMR	Long retry timer
MAXMSGL	Maximum message length for channel
MCATYPE	Specifies whether message channel agent runs as a separate process or a separate thread
MCANAME	Name of the message channel agent
MCAUSER	User ID of the message channel agent
MODENAME	LU 6.2 mode name
MREXIT	Name of the channel message retry exit
MRDATA	User data of the channel message retry exit
MRRTY	Channel message retry count

Table 24. Tags of channel attributes in an MCCLI XML file and their descriptions (continued)

Tag in MCCLI XML file	Description
MRTMR	Channel message retry time
MSGEXIT	Name of the channel message exit
MSGDATA	User data of the channel message exit
NPMSPEED	Nonpersistent message speed
NETPRTY	Priority for the network connection
PASSWORD	Password for initiating LU 6.2 session
PUTAUT	Put authority
RCVEXIT	Name of the channel receive exit
RCVDATA	User data of the channel receive exit
SEQWRAP	Sequence number wrap value
SCYEXIT	Name of the channel security exit
SCYDATA	User data of the channel security exit
SENDEXIT	Name of the channel send exit
SENDDATA	User data of the channel send exit
SHORTRTY	The maximum number of attempts that are made by a sender, server, or cluster-sender channel to connect to the remote queue manager
SHORTTMR	For short retry attempts, this is the maximum number of seconds to wait before reattempting connection to the remote queue manager
SSLCAUTH	Specifies whether SSL client authentication is required
SSLCIPH	Cipher specification for the SSL connection
SSLPEER	Filter for the Distinguished Name from the certificate of the peer queue manager or client at the other end of the channel
TPNAME	Name of the LU 6.2 transaction name
TRPTYPE	Transport type
USERID	User identifier for initiating LU 6.2 session
XMITQ	Name of the transmission queue

Listener attributes and their tags in an MCCLI XML file

Table 25 lists the tags of listener attributes in an MCCLI XML file and their descriptions.

Table 25. Tags of listener attributes and their descriptions

Tag in MCCLI XML file	Description
ADDR	IP address of the listener
ADAPTER	The adapter number on which NetBIOS listens

Table 25. Tags of listener attributes and their descriptions (continued)

Tag in MCCLI XML file	Description
BACKLOG	The number of concurrent connection requests that the listener supports
COMMANDS	The number of commands that the listener can use
CONTROL	Specifies how the listener is started and stopped
DESCR	Optional plain text comment
LOCLNAME	The NetBIOS local name that the listener uses
LISTENER	The name of the listener definition for which information is displayed
PORT	The port number for TCP/IP
SESSIONS	The number of sessions that the listener can use
SOCKET	SPX socket
TBNAMES	The number of names that the listener can use

Service attributes and their tags in an MCCLI XML file

Table 26 lists the tags of service attributes in an MCCLI XML file and their descriptions.

Table 26. Tags of service attributes in an MCCLI XML file and their descriptions

Tag in MCCLI XML file	Description
CONTROL	Specifies how the service is started and stopped
DESCR	Optional plain text comment
SERVICE	Name of the service definition for which information is displayed
STARTARG	Specifies the arguments that are passed to the user program at queue manager startup
STARTCMD	Specifies the name of the program that is to run
STOPCMD	Specifies the name of the executable program to run when the service is requested to stop
STOPARG	Specifies the arguments that are passed to the stop program when instructed to stop the service
STDOUT	Specifies the path of the file that the standard output of the service program is redirected to
STDERR	Specifies the path of the file that the standard error of the service program is redirected to

Table 26. Tags of service attributes in an MCCLI XML file and their descriptions (continued)

Tag in MCCLI XML file	Description
SERVTYPE	Specifies the mode in which the service is run

Namelist attributes and their tags in an MCCLI XML file

Table 27 lists the tags of namelist attributes in an MCCLI XML file and their descriptions.

Table 27. Tags of namelist attributes and their descriptions

Tag in MCCLI XML file	Description
DESCR	Optional plain text comment
NAMELIST	Name of the namelist that is displayed
NAMES	List of names
NLTYPE	Indicates the type of the namelist that is displayed

Authentication information attributes and their tags in an MCCLI XML file

Table 28 lists the tags of authentication information attributes in an MCCLI XML file and their descriptions.

Table 28. Tags of authentication information attributes and their descriptions

Tag in MCCLI XML file	Attribute description in WebSphere MQ
AUTHINFO	Name of the authentication information object that is displayed
AUTHTYPE	Type of the authentication information
CONNAME	The hostname, IPv4 dotted decimal address, or IPv6 hexadecimal notation of the host that the LDAP server is running on
DESCR	Optional plain text comment
LDAPPWD	Password that is associated with the Distinguished Name of the user on the LDAP server
LDAPUSER	Distinguished Name of the user on the LDAP server

Storage class attributes and their tags in an MCCLI XML file

Table 29 lists the tags of storage class attributes in an MCCLI XML file and their descriptions.

Table 29. Tags of storage class attributes and their descriptions

Tag in MCCLI XML file	Attribute description in WebSphere MQ
STGCLASS	Name of the storage class
DESCR	Optional plain text comment

Table 29. Tags of storage class attributes and their descriptions (continued)

Tag in MCCLI XML file	Attribute description in WebSphere MQ
PSID	The page set identifier that a storage class maps to
XCFGNAME	Name of the XCF group that WebSphere MQ is a member of
XCFMNAME	The XCF member name of the IMS system within the XCF group specified in XCFGNAME
PERFMEV	The application name that is used to authenticate IMS bridge pass tickets

Appendix F. Library for the WebSphere MQ Configuration agent

The following documents are available in the library for the WebSphere MQ Configuration agent:

- *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Installation and Setup Guide*

  Describes how to install WebSphere MQ Monitoring agent, WebSphere MQ Configuration agent, and WebSphere Message Broker Monitoring agent on Windows, UNIX, Linux, and i5/OS systems.
- *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Upgrade and Migration Guide*

  Provides information about how to upgrade or migrate from previous versions of WebSphere MQ Monitoring agent, WebSphere MQ Configuration agent, and WebSphere Message Broker Monitoring agent to version 7.3.
- *IBM Tivoli Composite Application Manager Configuration Agent for WebSphere MQ User's Guide*

  Provides instructions for using the features of WebSphere MQ Configuration agent.
- *IBM Tivoli Composite Application Manager Agents for WebSphere Messaging: Troubleshooting Guide*

  Provides problem determination and resolution information for the issues most commonly encountered when using WebSphere MQ Monitoring agent, WebSphere MQ Configuration agent, and WebSphere Message Broker Monitoring agent.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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 and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's user name for purposes of session management, authentication, and single sign-on configuration. These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Glossary

This glossary includes terms and definitions for ITCAM Agents for WebSphere Messaging.

The following cross-references are used in this glossary:

- See refers you from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- See also refers you to a related or contrasting term.

To view glossaries for other IBM products, go to www.ibm.com/software/globalization/terminology (opens in new window).

A

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access management
The process of controlling access to IT services, data, or other assets.

address space
The range of addresses available to a computer program or process. Address space can refer to physical storage, virtual storage, or both. See also buffer pool.

agent Software that is installed to monitor systems. An agent collects data about an operating system, a subsystem, or an application.

aggregation
The process of collecting, interpreting, and sorting data from various locations into a single file.

alert A message or other indication that signals an event or an impending event. See also event.

attribute

1. The application properties that are measured and reported on, such as the amount of memory that is used or a message ID. See also attribute group.
2. Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
A set of related attributes that can be combined in a view or a situation. See also attribute, situation, view.

audit A process that logs modifications to the database and plan.

B

batch

1. Pertaining to a group of jobs to be run on a computer sequentially with the same program with little or no operator action.
2. A group of records or data processing jobs brought together for processing or transmission.

batch job
A predefined group of processing actions submitted to the system to be performed with little or no interaction between the user and the system.

batch mode
The condition established so that batch processing can be performed.

BPM See business performance management.

broker
A set of execution processes that host one or more message flows. See also execution group, message flow.

buffer pool
An area of memory into which data pages are read and in which they are modified and held during processing. See also address space.

bundle
A packaged collection of software products that is purchased as one item and that has its own product identifier (PID).

business performance management (BPM)
The monitoring, management, and tuning

of business performance in real time through the analysis of business relevant information.

C

channel
A WebSphere MQ object that defines a communication link between two queue managers (message channel) or between a client and a queue manager (MQI channel). See also queue manager.

client A software program or computer that requests services from a server. See also host, server.

cluster

1. In WebSphere MQ, a group of two or more queue managers on one or more computers, providing automatic interconnection, and allowing queues to be advertised among them for load balancing and redundancy.
2. In Microsoft Cluster Server, a group of computers, connected together and configured in such a way that, if one fails, MSCS performs a failover, transferring the state data of applications from the failing computer to another computer in the cluster and reinitiating their operation there.

cluster queue manager
A queue manager that is a member of a cluster. A queue manager can be a member of more than one cluster.

component
A software item that is part of a software product, and might be separately identified, but is not individually licensed.

condition

1. An expression that consists of an agent attribute, an operator such as great than or equal to, and a value. It can be read as, "If - system condition - compared to - value - is true. See also situation.
2. A test of a situation or state that must be in place for a specific action to occur.

configuration
The manner in which the hardware and software of a system, subsystem, or network are organized and interconnected.

D

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

dead-letter queue (DLQ)
A queue to which a queue manager or application sends messages that cannot be delivered to their correct destination.

deployment
The process of installing and configuring a software application and all its components.

DLQ See dead-letter queue.

dynamic queue
A local queue created when a program opens a model queue object.

E

enterprise
The composite of all operational entities, functions, and resources that form the total business concern and that require an information system.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process. See also alert, situation.

execution group
A named process or set of processes within a broker in which message flows are executed. The broker is guaranteed to enforce some degree of isolation between message flows in distinct execution groups by ensuring that they execute in separate address spaces, or as unique processes. See also broker, message flow.

F

full repository
A complete set of information about every queue manager in a cluster. This set of information is called the repository or sometimes the full repository and is usually held by two of the queue managers in the cluster. See also partial repository.

function
Any instruction or set of related instructions that performs a specific operation.

H

host A computer that is connected to a network and that provides an access point to that network. The host can be a client, a server, or both a client and server simultaneously. See also client, server.

hot standby
A redundant server that, if the primary server or hub server fails, assumes the responsibilities of the failed server.

I

integration
The software development activity in which separate software components are combined into an executable whole.

L

launch-in-context
An operation in which a user starts a secondary application from a primary application to perform a specific task. Using the parameters, navigation instructions, and user credentials that are supplied by the primary application, the secondary application opens to the specific place in which to complete the task.

M

managed object
A resource that is subject to management as viewed from a systems management perspective. Examples of such resources are a connection, a scalable system, or a line.

managed system
A system that is being controlled by a given system management application.

manager
An entity that monitors or controls one or more managed objects by (a) receiving notifications regarding the objects and (b) requesting management operations to modify or query the objects.

message flow
A sequence of processing steps that execute in the broker when an input message is received. Message flows are defined in the workbench by including a number of message flow nodes, each of which represents a set of actions that define a processing step. The connections in the flow determine which processing steps are carried out, in which order, and under which conditions. See also broker, execution group, subflow.

middleware
Software that acts as an intermediate layer between applications or between client and server. It is used most often to support complex, distributed applications in heterogeneous environments.

module
A program unit that is discrete and identifiable with respect to compiling, combining with other units, and loading.

monitoring agent
See agent.

multi-instance queue manager
A queue manager that is configured to share the use of queue manager data with other queue manager instances. One instance of a running multi-instance queue manager is active, other instances are on standby ready to take over from the active instance. See also queue manager.

O

offering

1. A logical unit of software packaging and sharing that has a managed development and maintenance life cycle and customer visible attributes (offering features, product IDs, licenses, maintenance contracts, and so forth). An offering is a serviceable software asset that is orderable by an IBM customer. It can be a collection of common components, assemblies, and other offerings.
2. The element or integrated set of elements (hardware, software, services) designed to satisfy the wants and needs of current and/or prospective customers. A solution is the application of the offering in a specific customer environment. See also solution.

P

partial repository
A partial set of information about queue managers in a cluster. A partial repository is maintained by all cluster queue managers that do not host a full repository. See also full repository.

performance management

1. The discipline that encompasses capacity planning, collecting performance data, and tuning resources.
2. The management processes and systems needed to effectively deliver business services.

PID See product identifier.

platform
The combination of an operating system and hardware that makes up the operating environment in which a program runs.

policy A set of considerations that influence the behavior of a managed resource or a user.

product ID
See product identifier.

product identifier (PID, product ID)
A unique value that identifies an IBM software product. Every mainframe and distributed IBM software product has a PID.

Q

query In a Tivoli environment, a combination of statements that are used to search the configuration repository for systems that meet certain criteria. The query object is created within a query library.

queue An object that holds messages for message-queueing applications. A queue is owned and maintained by a queue manager.

queue manager
A component of a message queuing system that provides queuing services to applications. See also channel, multi-instance queue manager.

queue-sharing group
In WebSphere MQ for z/OS, a group of queue managers in the same sysplex that can access a single set of object definitions stored in the shared repository, and a single set of shared queues stored in the coupling facility.

R

registry
A repository that contains access and configuration information for users, systems, and software.

S

sampled event
An event that happens when a situation becomes true. Situations sample data at regular intervals. When the situation is true, it opens an event, which is closed automatically when the situation returns to false.

segment
A set of customers/buyers within a market who have common wants, needs, characteristics and buying behavior. These wants and needs are sufficiently homogeneous that a consistent set of strategies, marketing campaigns and sales tactics can be directed toward them.

server A software program or a computer that provides services to other software programs or other computers. See also client, host.

service request
A request from a user for help, information, advice, or access to an IT service.

severity level
A classification for an event that indicates its degree of severity. The predefined severity levels, in order of descending severity, are: fatal, critical, warning, minor, harmless, and unknown.

situation
A set of conditions that, when met, creates an event. See also attribute group, condition, event.

snapshot
A capture of data at a point time for performance analysis.

solution
A combination of products that addresses a particular customer problem or project.

started task
In MVS, a process that begins at system start and runs unattended. Started tasks are generally used for critical applications. The UNIX equivalent of a started task is a daemon.

state
An indication associated with an icon, color, and severity level assigned to a situation at a point in time. A situation can reflect one of the following states: critical, warning, or informational.

status
The true or false condition of a situation.

subflow
A sequence of processing steps, implemented using message flow nodes, that is designed to be embedded in a message flow or in another subflow. A subflow must include at least one Input or Output node. A subflow can be executed by a broker only as part of the message flow in which it is embedded, and therefore it cannot be deployed. See also message flow.

subnet
See subnetwork.

subnetwork (subnet)
A network that is divided into smaller independent subgroups, which still are interconnected.

subscription
In a Tivoli environment, the process of identifying the subscribers that the profiles are distributed to.

summarization
The process of aggregating events and then submitting the set of events with a much smaller number of summary events.

system
A computer and its associated devices and programs.

T

TCP/IP
See Transmission Control Protocol/Internet Protocol.

threshold
A customizable value for defining the acceptable tolerance limits (maximum, minimum, or reference limit) for an application resource or system resource. When the measured value of the resource is greater than the maximum value, less than the minimum value, or equal to the reference value, an exception or event is raised.

transaction
A unit of processing consisting of one or more application programs, affecting one or more objects, that is initiated by a single request.

Transmission Control Protocol/Internet Protocol (TCP/IP)
An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types.

transmission queue
A local queue on which prepared messages destined for a remote queue manager are temporarily stored.

U

upgrade
To install a new version or release of a product to replace an earlier version or release of the same product.

user profile
A description of a user that includes such information as user ID, user name, password, access authority, and other attributes that are obtained when the user logs on.

V

view A window pane, or frame, in a workspace. It may contain data from an agent in a chart or table, or it may contain a terminal session or notepad, for example. A view can be split into two separate, autonomous views. See also attribute group.

W

workspace

1. A window comprised of one or more views.
2. In Tivoli management applications, the working area of the user interface, excluding the Navigator pane, that displays one or more views pertaining to a particular activity. Predefined workspaces are provided with each Tivoli application, and systems administrators can create customized workspaces.

Index

Printed in USA

SC14-7525-01